New rules, wider reach: the extra-territorial scope of the GDPR

June 2016

This publication is part of a series of Briefings we are publishing on the EU General Data Protection Regulation ("GDPR") that will take effect on 25 May 2018.

Introduction

The GDPR marks a significant expansion of the territorial scope of the EU data protection regime, bringing a larger number of overseas businesses within its reach.

When determining whether activities fall within its geographical reach, the GDPR considers not only the location of the processing, as in the current EU Data Protection Directive (the "Directive"), but also the location of the individual whose data is being processed.

This should come as no surprise to practitioners and businesses – the ever-widening interpretation of the extra-territoriality of the Directive in recent case law had already begun to implement this expansion.

The formalised global reach of the GDPR calls into question the enforceability of the regime on non-EEA businesses suggesting that, despite increased fines and sanctioning powers, reputation may continue to be the key driver behind privacy compliance for market leaders outside the EU.

What changes does the GDPR introduce?

Directive	GDPR
Data controllers established outside the EEA but using equipment in the EEA. EU jurisprudence deems this to include servers and employees, even in some cases only one representative, as well as more traditional forms of equipment.	Data controllers or processors established outside the EU processing personal data in relation to: • the offering of goods or services to individuals in the EU (including free of charge), or • monitoring their behaviour (in the EU).

The wider extra-territorial reach of the GDPR comes as no surprise

The creation of a "level playing field" for businesses established inside and outside the EU through an expansion of territorial scope was a key and much publicised objective of the GDPR.

On the face of it, the GDPR's two-limbed test is a significant expansion of the territorial reach of EU data protection. However, EU courts had already made clear their view on the direction of travel of EU law: a broad interpretation of the Directive was necessary for the protection of individuals' rights.

Google Spain

Perhaps the most publicised and controversial instance of the Court of Justice of the European Union ("CJEU") stretching the territorial reach of the EU Directive was the 2014 Google Spain decision (Case C-131/12). A key element in the Court's decision that Google Inc.'s data processing activities were subject to Spanish data protection law was that Google Spain "orientates its activity towards the inhabitants of the Member State", in Google's case by positioning advertising directed at Spain alongside search results, and that the activities of Google Spain and Google US were "inextricably linked". The Court's decision appeared to interpret the existing regime in light of the draft GDPR.

What does "offering goods or services" mean?

Key to determining whether a non-EU business is offering goods/services to EU data subjects is the business's intention, and whether it is apparent that an offer to an EU-based data subject was "envisaged". The availability of a business's website to EU data subjects is not sufficient to establish an intention to offer. However, if the website is in an EU language which is not that of the controller's jurisdiction, is offering goods/services in an EU currency or, unsurprisingly, is explicitly targeting EU citizens, this could provide proof of intent and pull the business within scope.

These criteria for establishing intention reflect the CJEU's ruling in Weltimmo (Case C-230/14), which emphasised that if a company operates a service in the native language of a country (in this case a Slovakian property advertising service operating in Hungary) it could be held accountable to that country's data protection authority ("DPA").

What does "monitoring behaviour" in the EU mean?

The recitals to the GDPR make clear that where data subjects are "tracked on the internet" this will constitute monitoring and bring the relevant entity within scope. All websites that use tracking cookies and apps that track usage will be caught to the extent that the information they collect, in aggregate, renders an individual identifiable.

The use of cookies

Non-EU companies that carry out cookie profiling (i.e. by using persistent - as opposed to session only - cookies to track a user's overall online activity across websites) will most likely be processing personal data to monitor behaviour. This is not surprising given the 2014 finding in Google v Vidal-Hall (currently on appeal to the Supreme Court), that information on a user's browsing and internet usage could amount to personal data.

It will be interesting to see the extent to which businesses will continue such profiling or tracking of individuals given the enhanced transparency requirements under the GDPR and the fact that some research suggests that

behavioural advertising is disliked by over 90% of UK consumers.[1]

The use of cookies that do not collect personal data or that do not track or profile a user (such as session only cookies that regulate website functionality) is unlikely to be caught by the GDPR.

IP addresses

Although cookies are a common method of obtaining information on users' online behaviour, individuals can be tracked or monitored in other ways, such as through the sharing of IP addresses. Many website owners keep logs of the dynamic IP addresses that have visited their website.

Such IP addresses may well amount to personal data, especially where the user's internet access provider has data that, in combination with the IP address, can identify the user.

This was the opinion of the Attorney General ("AG") in Breyer v. Federal Republic of Germany (C-582/14), which is pending before the CJEU. Although not legally binding, AG opinions are often followed by the CJEU.

Implications for overseas businesses

What does this mean for overseas businesses whose websites are visited by individuals located in the EU (whether or not they are EU residents)? Are these website owners 'tracking' the individuals whose IP addresses they collect and thus subject to the GDPR? In practice, it is unlikely that website owners based outside the EU would restrict access to their services by individuals in the EU. This would not only likely be detrimental to business but would trigger a consequential decrease in functionality of the relevant website. The sensible interpretation of the GDPR would be that it does not intend to capture such incidental collection.

This is supported by the GDPR recitals which explain that tracking individuals on the internet includes the use of data processing techniques to profile an individual, and then taking decisions concerning them or analysing or predicting their personal "preferences, behaviours and attitudes". The inclusion of this example would suggest that an element of intentional or active tracking is required for the GDPR to apply to non-EU businesses.

In practice, a DPA would need to be fairly ambitious to take on a foreign controller or processor only incidentally collecting the personal data of individuals located in the EU, when that data is not actively used to profile those individuals or monitor their behaviour.

For now, however, it is still unclear exactly how detailed the tracking of a data subject must be in order to trigger the application of the GDPR.

---

[1] Frederik Zuiderveen Borgesius, "Consent to Behavioural Targeting in European Law – What are the Policy Implications of Insights from Behavioural Economics?", 2013, http://poseidon01.ssrn.com

Examples of the wider application of the GDPR

Scenario	Directive applies	GDPR applies
US company without any EU subsidiaries offering free social media services via a website hosted in the US to individuals in the EU	x	✓
Singaporean hotel booking business using cookies to track past customers' (including EU-based customers) browsing in order to target specific hotel adverts to them	x	✓
Chinese flower delivery company allowing data subjects in the EU to make orders for fulfilment only in China	x	✓
Australian retailer with a website for orders/deliveries. The website is accessible to individuals in the EU in English. The currency is the Australian dollar and the address fields only allow Australian addresses	x	x

Enforcing the GDPR outside the EU

Although the powers of DPAs to sanction data protection breaches have been considerably broadened – and the quantum of fines raised to 4% of annual global turnover - there remain significant doubts regarding the enforceability of the regime on businesses established outside the EU. If breaches by such entities are found to be unenforceable, this could bring into question the credibility of the EU regime.

Individuals' claims

The GDPR states that all data subjects have the right to an effective judicial remedy. However, the mechanism for overseas enforcement is currently unclear and it is likely that, under the GDPR, individuals will continue leveraging DPA findings to seek permission from national courts to serve proceedings in non-EU jurisdictions.

Regulator enforcement action

While some parallels may be drawn to enforcement by other regulators against overseas entities, this remains an area fraught with uncertainty. The GDPR requires an extremely limited nexus to the EU in order to apply, increasing the practical difficulties of enforcement.

As a comparable, in the UK financial services sector, UK regulators may have limited enforcement powers where the nexus to the UK is weak (e.g. a breach is committed by a non-UK entity without a place of business in the UK). Even where those powers do exist we would generally expect the UK regulators to seek to co-ordinate with overseas regulators in taking any enforcement action.

For example, where an EEA financial services firm passports its services into the UK, the policy of the Financial Conduct Authority ("FCA") when exercising its intervention powers is to co-operate with the firm's home state regulator as appropriate.

Increased co-operation between DPAs has long been encouraged and the GDPR formalises this trend by explicitly setting out co-operation

obligations between DPAs, including a consistency mechanism. Co-operation agreements, as seen in the financial services sector between national or regional data protection bodies, could also provide a possible path to enforcement.

Similarly, in the context of the market abuse regime, whose broad extra-territorial application is being extended further by the Market Abuse Regulation, the FCA has enforced fines against overseas persons on a number of occasions, notably in the 2012 Greenlight/Einhorn case where US persons were sanctioned for insider dealing in Punch shares, a company listed on a UK market. However, in most cases co-operation with local regulators is essential.

In the data protection sphere, Google's prompt compliance with the Google Spain decision, albeit a narrow interpretation of that decision, could suggest that companies will be loath to risk the reputational damage incurred from refusing to comply with a data protection enforcement notice, rendering the practical difficulties of enforcement irrelevant.

However, although this may be the case for larger, consumer focussed companies, enforcement issues are likely to be of greater concern as regards smaller, non-consumer businesses.

Are representatives part of the solution?

The GDPR requires overseas data controllers or processors falling within its scope (and whose processing is not occasional) to designate a representative based in an EU Member State who will act as the point of contact for the relevant DPA, and who are also subject to certain record-keeping requirements.

Scope of representatives' role

Under the Directive, the scope of the nominated representatives' role is unclear, consequently the degree of responsibility ascribed to such representatives varies across Member States.

In Greece, the representatives are subject to sanctions alongside the data controller, whilst in the UK representatives fulfil a largely administrative role.

The recitals to the GDPR state that "the designated representative should be subjected to enforcement actions in case of non-compliance by the controller", which may be the intended solution to some of the enforcement difficulties identified above. However, the GDPR fails to include an appropriate enforcement mechanism within the text itself, merely stating that the designation of a representative shall be "without prejudice" to the liability of the controller.

When is a representative required?

The GDPR does clarify that a nominated representative is only required in the Member State of the controller's or processor's "main establishment" whereas currently, national data protection laws could require data controllers established outside the EU to nominate a representative in each Member State in which they are conducting processing activities.

The "main establishment" of a data controller or processor is defined as its place of "central administration", unless decisions regarding the purpose and means of processing are taken elsewhere. Overseas businesses with a number of establishments in the EU taking decisions regarding the purpose and means of processing, or with no clear EU establishment, are likely to encounter practical difficulties in designating a single "main establishment".

If overseas businesses wish to be strategic in their choice of "main establishment", they could consider electing a representative in a preferred Member State. However, they should be monitoring the Verein für Konsumenteninformation v Amazon EU Sàrl case (C -191/15, currently unavailable in English) to assess the extent to which this approach will work. The AG has recently issued his opinion in that case, arguing that despite Amazon's attempts

to streamline its data protection compliance to ensure the laws of Luxembourg apply, neither the laws of Luxembourg nor the laws of Austria (where the consumer was based) do apply. Rather, it could be that the laws of Germany apply, where Amazon has an establishment whose website targets Austrian customers.

Conclusion

A significant number of businesses previously operating outside the scope of the Directive will be caught by the GDPR. However, the wide scope of the GDPR should come as no surprise given the direction of travel of EU jurisprudence during the last few years. Overseas businesses that were not previously caught by the Directive should now be in the process of assessing whether their activities will bring them within the scope of the GDPR.

The GDPR will require substantial changes to processes and procedures for businesses that are already complying with the current regime, but the road to compliance for those previously falling outside scope is likely to be significantly steeper.

If you have any queries on this Briefing or if you would like to discuss any aspect of the GDPR or any data protection or privacy issue, please do not hesitate to contact Rob Sumroy, Rebecca Cousin or your usual Slaughter and May advisor.

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

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

Cindy Knott
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com

Lucia Bird
T +44 (0)20 7090 5368
E lucia.bird@slaughterandmay.com