Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 2 >>> FEBRUARY 2016

Data Protection

Art. 29 Party Opinion Update Provides Guidance on the Application of EU Privacy Law to Non-EU Companies

Rafi Azim-Khan, Partner & Head Data Privacy, and Steven Farmer, Counsel Pillsbury Winthrop Shaw Pittman

The Article 29 Working Party (WP29) has published an update to Opinion 8/2010[1] on "applicable law in light of the Court of Justice of the European Union's (CJEU) judgment in Google Spain" (the Opinion), which seeks to provide clarity on the application of European Union data protection law to non-EU businesses.

Although the update to the Opinion is dated December 2015, it was released to the public in January this year, over a year after the judgment in *Google Spain*[2] .

This update seeks to address the territorial scope of the Data Protection Directive (95/46/EC) (the Directive), focusing on the criteria for the applicability of EU law under Article 4 of the Directive with regard to establishment in a Member State.

The update also looks at whether or not controllers

[1] WP29 Opinion 8/2010 on applicable law (WP 179)

[2] CJEU judgment of 13 May 2014 in case C-131/12, *Google Spain SL* and *Google Inc. v AEPD and Gonzalez* .

with EU headquarters are required to comply with the laws in all Member States where they are deemed to have establishments, or just the laws of the Member State in which they are headquartered.

The update is welcome guidance, particularly for organisations based outside the EU that have a European footprint or that otherwise target EU customers. The question of whether EU data protection law applies to such businesses is, of course, of vital importance, dictating the compliance efforts required.

However, the impact of the update (and the Opinion) is arguably limited in light of sweeping, broader changes expected under the new General Data Protection Regulation (GDPR) which are set to significantly reshape the rules regarding the application of EU data protection law to non-EU businesses further.

Google Spain

By way of reminder, in the *Google Spain* case, the CJEU ruled on three questions concerning the interpretation of the Directive with regard to the data processing activities of Google Inc. as a search engine provider, its status as a data controller and the existence and scope of the right to be forgotten.

Crucially for the purposes of the update to the Opinion, the CJEU held that a non-EU search engine operator (Google Inc.) was a data controller in respect of processing activities it carried out and that processing by it which was "inextricably linked to" its Spanish establishment's activities (i.e. the activities of its Spanish subsidiary) was carried out "in the context of that establishment" under Article 4 of the Directive, making Google Inc. a non-EU controller, subject to EU law.

By way of reminder, Article 4(1)(a) of the Directive provides that a Member State shall apply its data protection laws where processing of personal data arises "in the context of the activities of an establishment of the controller on the territory of the Member State." It further provides that "when the same controller is established on the territory of several Member States, he must. . . ensure that each of these establishments complies with. . . the national law applicable."

The Working Party considers that an additional element should be added to the criteria which may trigger national and EU law applicability: an "inextricable link" between an activity in the Member State and the data processing.

Following this decision, the WP29 issued separate guidance on how national data protection authorities (DPAs) intended to implement the judgment[3], focusing on the search de-listing aspect of the judgment (in particular, publishing a list of common criteria which the DPAs will apply to handle any complaints they receive from data subjects following refusals of de-listing by search engines). However, this latest update explores two main issues relating to the concept of establishment under Article 4 of the Directive in light of the CJEU decision, not initially dealt with in the Opinion in detail i.e.:

- the extent of the territorial reach of the Directive for non-EU data controllers with a "relevant" establishment in the EU. At what point is the application of EU data protection law triggered? and
- Do EU-headquartered data controllers need only to comply with one Member State's national law, or additionally, with the laws of other EU Member States where they have a "relevant" establishment?

Territorial Reach of the Directive

The WP29 notes that Article 4(1)(a) of the Directive applies where processing is carried out "in the context of the activities of an establishment" of a data controller in a Member State.

It notes that "establishment" is broadly interpreted and arises where even a minimal, but still real and effective activity is exercised by a data controller in a Member State (as recently held by the CJEU in *Weltimmo*[4] (15 WDPR 33, 7/23/15).

The WP29 highlights as a key point in the update that even if a Member State establishment is not involved in any direct way in the processing of data (by a non-EU data controller), its activities may still bring the processing within EU law, as long as an "inextricable link" between the local establishment's activities and the processing exists, regardless of where that processing takes place.

It considers that an additional element should be added to the criteria which may trigger national and EU law applicability: an "inextricable link" between an activity in the Member State and the data processing.

By way of illustration, the WP29 provides examples of how EU law might be triggered depending on the facts and the role played by the local establishment, including: (i) offering free services within the EU (financed by use of data collected); (ii) offering membership or subscription services in the EU; and (iii) seeking donations in the EU.

Nevertheless, the WP29 is careful not to apply the "inextricable link" test too broadly, emphasising the importance of a case-by-case analysis.

It notes that an "inextricable link" will not arise for every non-EU entity that has operations in the EU. The mere fact that two entities are part of the same corporate group is not sufficient to establish such a link, for example—there must be an actual connection between

[3] Guidelines on the implementation of the Court of Justice of the European Union judgment on *Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* c-131/121 (WP225) (26 Nov. 2014)

[4] C-230/14 *Weltimmo s.r.o v. NAIH*

   ISSN 1473-3579

the business activities performed by a subsidiary established in the EU and the data processing carried out by the non-EU entity.

Multiple EU Establishments—Which EU Law Applies?

The update goes on to consider the question of which law applies where an organisation has several establishments in various Member States, but where only one (for example, its EU headquarters) is a data controller in relation to the processing in question (and where the others do not necessarily play a role in the processing).

It notes that where there is an establishment in any EU country, an assessment must be carried out on a case-by-case basis as to whether any particular processing activity is carried out in the context of the activities of that establishment. If processing is carried out in the context of an establishment, there will be a need to comply with the laws of that Member State.

In summary, therefore, as the update notes, regardless of where data processing takes place, "where a company has establishments in several EU Member States which promote and sell advertisement space, raise revenues or carry out other activities and it can be established that these activities and the data processing are '*inextricably linked*,' the national laws of each such establishments will apply."

The update reiterates, therefore, that as things stand non-EU businesses with a pan-European footprint may indeed need to comply with up to 28 different data protection laws at any one point.

The net result following the *Google Spain* case, the Opinion and the Working Part update, is that many non-European Union businesses that have operations in the EU could potentially find themselves subject to EU data protection law

---

Comment

The WP29 update confirms that the *Google Spain* judgment provides useful clarification on two aspects.

First, the judgment makes it clear that the scope of current EU law extends to processing carried out by non-EU entities with a "relevant" establishment whose activities in the EU are "inextricably linked" to the processing of data, even where the applicability of EU law would not have been triggered based on more traditional criteria.

Second, where there is an "inextricable link," there may be several national laws applicable to the activities of a controller having multiple establishments in various Member States.

The net result following *Google Spain*, the Opinion and this latest update, is that many non-EU businesses that have operations in the EU could potentially find themselves subject to EU data protection law, resulting in a compliance headache which many non-EU based organisations may not have expected (particularly where they have multiple EU establishments).

The impact of this WP29 guidance is, however, arguably short-lived in light of the GDPR which is set to redefine the rules regarding the application of EU data protection law to non-EU businesses—making the test even broader than it already is.

In particular, under the GDPR, any business that is based outside the EU, but either: (i) offers goods or services in the EU; or (ii) tracks the behaviour of EU residents, will be subject to the requirements of EU privacy law.

All these developments point toward the increasingly strong extraterritorial application of EU data protection law which non-EU businesses cannot ignore.

Businesses based outside the EU, but doing business in the EU or otherwise targeting the EU, should therefore take note of the fact that the law is moving in this data subject-centered direction, and focus compliance efforts accordingly.

To turn a blind eye or otherwise ignore these developments could ultimately subject a company to fines comparable to those currently levied in antitrust matters (i.e. the GDPR cites fines of up to 4 percent of global turnover).

  WDPR ISSN 1473-3579