scripted

Volume 13, Issue 1, May 2016

Cross-Border Data Protection: Applicable Law and Territorial powers of National Data Protection Supervisors

Karen Mc Cullagh[*]

Abstract

This commentary analyses the European Court of Justice preliminary ruling in Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, on the interpretation of two important aspects of Directive 95/46/EC, namely the applicable law, and territorial reach of, national data protection authorities. The Court ruled that the data protection legislation of a member state may be applied by the national data protection authority to a foreign registered company which exercises, through stable arrangements, real and effective (albeit minimal) activity in that member state. This is a ruling that potentially increases compliance costs for entities operating across multiple European jurisdictions pending the introduction of the General Data Protection Regulation.

DOI: 10.2966/scrip.130116.95

[*] Lecturer, University of East Anglia, United Kingdom.

1. Introduction

Personal data processing is at the heart of the information economy. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*[1] (hereafter "the Directive") provides a general, comprehensive legislative framework that regulates the processing of personal data within the European Union. Disparities in the transposition of the Directive into member states' national laws has led to compliance uncertainty for internet-based entities such as Google and Facebook that operate on a transnational basis.

Such entities have exploited these disparities by "establishing" European headquarters in one member state (usually Ireland)[2] and sought to comply with the specific data protection requirements of that particular state only, whilst also having a "presence" in multiple other member states. They have then asserted that a national data protection authority in a member state in which they merely have a "presence" could not oblige them to comply with that country's national data protection law.

The European Court of Justice (hereafter "ECJ") recently considered the issue of "establishment" in Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*[3] (hereafter "*Weltimmo*"). After giving a brief description of the facts in the case, this commentary will analyse the legal issues that led the Court to its decision, and examine its significance for the territorial application of data protection law, and the powers of national data protection authorities. The discussion will confirm that entities operating on a pan-European basis can now be subject to the data protection laws of each country in which they have a presence (not just the one they are legally established in). It will conclude by considering the implications for the "one-stop-shop" contained in the EU's proposed General Data Protection Regulation.

2. The Facts

The plaintiff in the case, Weltimmo, is a company registered in Slovakia but it conducts its business in Hungary. To this end it operated a property dealing website under two domain names: ingatlanbazar.com and ingatlandepo.com. The website advertising the sale of properties in Hungary offered free advertising to Hungarian customers for a month. Many advertisers sent a request by email for the deletion of both their advertisements and their personal data after the free trial period ended but Weltimmo did not delete their data and charged the advertisers a fee for its services. When the fees were not paid Weltimmo forwarded the personal data of the advertisers to debt collection agencies without consent or notification. The Hungarian advertisers complained to *Nemzeti Adatvédelmi és Információszabadság hatóság* (the Hungarian Data Protection and Freedom of Information Authority) (hereafter "HDPA") that

---

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995.

[2] The decision to locate in Ireland is influenced by a number of factors including: low rates of corporation tax, liberal interpretation of the provisions of the data protection directive.

[3] *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (2015), ECLI:EU:C:2015:639.

Weltimmo's processing of their personal data breached Hungarian data protection law in failing to comply with notification and purpose limitation requirements and in processing and transferring personal data without a legal basis. The HDPA imposed a fine of HUF 10 million (approximately EUR 32 000) upon Weltimmo.

On appeal, before the Kúria (the Hungarian Supreme Court), the plaintiff challenged the fine arguing that Hungarian data protection law should not apply to it, a service provider established in a different member state, and contended that the HDPA should have referred the matter to the Slovakian Data Protection Authority.

The Kúria was unsure to how to answer the competence question because it was unclear as to the legal effects of two Articles of Directive 95/46/EC: Article 4 (concerning the territorial scope of domestic data protection laws) and Article 28 (concerning the role of the domestic supervisory authority). Accordingly, it referred a number of questions to the ECJ, including the following:

> Can Article 4(1)(a) of the data protection directive, read in conjunction with recitals 18 to 20 of its preamble and Articles 1(2) and 28(1) thereof, be interpreted as meaning that the Hungarian Data Protection and Freedom of Information Authority may not apply Hungarian law on data protection, to an operator of a property dealing website established only in another Member State, even if it also advertises Hungarian property whose owners transfer the data relating to such property from Hungarian territory to a facility (server) for data storage and data processing belonging to the operator of the website?[4]

3. Opinion of Advocate-General Cruz Villalón

On 25th June 2015, the Advocate-General delivered his opinion[5] in which he stated that the effects of Articles 4 and 28 are such that a supervisory authority in a member state cannot assert jurisdiction over a data controller which is not "established" in that member state.[6] When determining whether a data controller is 'established' in a member state, the focus should be on the *de facto* rather than the *de jure* position, and answering this question is likely to require a focus on where the business' human and technical resources are located.[7] He further opined that other factors such as the nationality of the data subjects, the domicile of the company owners or the targeting of citizens within a particular member state, are less relevant and only indirectly helpful in deciding where a data controller is established.[8]

4. European Court of Justice preliminary ruling

---

[4] OJ C 245, 28.7.2014, at 5–6.

[5] *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (2015), ECLI:EU:C:2015: 426.

[6] *Ibid*, para 42.

[7] *Ibid*, para 72(1).

[8] *Ibid*.

In a preliminary ruling issued on 1st October 2015,[9] the ECJ broadly followed the approach of the Advocate-General. It began its analysis of the applicable law by considering Article 4(1)(a) of the Directive which provides that the national law of a member state will apply to processing that is: "carried out in the context of the activities of an establishment of the controller on the territory of the Member State." It referred with approval to the decision in Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*[10] (hereafter "*Google Spain*"),[11] in which the ECJ had adopted a broad approach to the applicable legal rules to defeat Google's arguments that it was not subject to EU data protection law at all. In the instant case, the Court confirmed that the concept of establishment should also be interpreted broadly and flexibly where there is a question as to which member state's law should apply. The Court said that a two-fold approach should be adopted: firstly, it should determine whether a data controller is established in a member state and, secondly, consider whether the processing of personal data occurred in the context of that establishment.

In the October 2015 preliminary ruling, the ECJ referred to Recital 19 in the preamble to the Directive to reject a formalist approach ("legal personality, is not the determining factor"), finding that Weltimmo's registration as a company with a legal personality in Slovakia was not a conclusive factor when determining establishment.[12] Rather, establishment should be determined on a de facto basis by considering both the "effective exercise of its activities" and the "degree of stability" of Weltimmo's activities in Hungary.[13] The Court determined that "effective exercise of activities" should be considered in light of the "specific nature of the economic activities and the provision of the services concerned."[14] It held that even a "minimal" real and effective activity (here, the running of a property dealing website with advertisements for Hungarian properties subject to a fee that was written in Hungarian and directed at Hungarian citizens) could suffice to trigger the "establishment" test and render that member state's data protection law applicable.[15] It ruled that the referring court could consider factors such as Weltimmo having a representative in Hungary who was responsible for debt recovery and had represented Weltimmo in Court, a Hungarian bank account and a Hungarian postal address, as relevant evidence of a considerable "degree of stability."[16]

Thereafter, the Court confirmed its findings from *Google Spain* that Article 4(1)(a) of Directive does not require the processing of the personal data in question to be carried out *by* the establishment concerned, only requiring processing "in the context of the

---

[9] *Weltimmo*, note 3 above.

[10] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014), ECLI:EU:C:2014:317.

[11] *Ibid*, para 53.

[12] *Weltimmo*, note 3 above, para 28.

[13] *Ibid*, para 29.

[14] *Ibid*.

[15] *Ibid*, para 31.

[16] *Ibid*, para 33.

activities" of the establishment.[17] It reaffirmed the position taken in both *Bodil Lindqvist v Åklagarkammaren i Jönköping*[18] and *Google Spain*[19] that uploading personal data to a webpage amounted to processing. In the present case, in the Court's view, the fact that Weltimmo's websites published personal data of the owners of the properties and in some cases used the data for invoicing purposes constituted processing in the context of the activities Weltimmo pursues in Hungary. The Court confirmed that nationality of the persons concerned by such processing is irrelevant.[20]

Additionally, the Court considered the territorial scope and power of data protection authorities by referring to the provisions in Article 28 of the Directive. It determined that when a supervisory authority receives a complaint it may exercise its investigative powers under Article 28(4) "irrespective of the applicable law and before even knowing which national law is applicable to the processing in question."[21] The Court went on to say that the effect of Article 28(6) and Articles 28(1) and (3) is that a data protection authority cannot enforce the applicable data protection law and impose sanctions against a controller that is not established in its jurisdiction. In such a case, the data protection authority would need to seek the cooperation of the data protection authority of the country in which the controller is established which may carry out investigations on the instructions of the referring supervisory authority.[22]

Thus, the Hungarian Kúria has been advised that Hungarian data protection law may be deemed to apply if the facts alleged are subsequently substantiated by it. If so, then the fine stands, but if the referring court finds that Weltimmo is not "established" in Hungary, the HDPA can still ask the Slovakian supervisory authority to impose the fine.

5. Analysis and Implications

Following *Weltimmo*, it is clear that the nationality of a data subject is not relevant when determining whether data protection laws apply. However, it is difficult to work out what weight to give to each of the relevant factors to be considered. It is not clear whether, in the case of an internet-based entity, an online presence targeting citizens of a particular member state will, by itself, mean the entity is established in that member state for data protection purposes, or whether a physical presence is always required (e.g. use of a local representative or bank account and PO box), as the ruling does not refer to the relevant factors as cumulative conditions. Nevertheless, the words "landmark" and "significant"[23] have been used to describe the potential impact of this

---

[17] *Ibid*, paras 35-41.

[18] *Bodil Lindqvist v Åklagarkammaren i Jönköping* (2003), C-101/01, EU:C:2003:596, para 25.

[19] *Google Spain*, note 10 above, para 26.

[20] *Weltimmo*, note 3 above, para 41.

[21] *Ibid*, para 57.

[22] *Ibid*, paras 57-60.

[23] S Gibbs "Landmark ECJ data protection ruling could impact Facebook and Google" (2015) available at http://www.theguardian.com/technology/2015/oct/02/landmark-ecj-data-protection-ruling-facebook-google-weltimmo (accessed 2 Apr 2016).

decision, as it confirms that there is no one-stop shop in respect of data protection: a business with operations in more than one member state may be subject to compliance requirements in each member state they operate in if they exercise, through stable arrangements, real and effective (albeit minimal) activity in that member state. It points to significant data protection compliance implications for internet based entities such as Google or Facebook who, prior to this ruling, had deliberately "established" their European operations in one country, such as Ireland, where data protection laws and practices are more liberal and arguably more business friendly. Following this ruling they will have to revise their compliance strategy as they will not be able to conclusively assert that they are subject to regulation only within that country. Instead, they will have to gain regulatory approval in each country in which they are de facto "established," and be subject to supervision by multiple data protection authorities, generating significant compliance costs.

Of course, when the General Data Protection Regulation[24] takes effect, as expected, in 2018, it will resolve many of these issues. Citizens will be able to complain to their national data protection authority (a one-stop shop approach), which will then work with the supervisory authority in the country where the company is headquartered to ensure the rights of data subjects are protected whilst personal data is being processed.

In summary, *Weltimmo* contributes to a growing body of jurisprudence on data protection. It confirms that data protection is no longer (if it ever was) a discrete, technical area; it is a significant compliance issue, and national regulators are increasingly determined to use their enforcement teeth. Businesses operating on a pan-European basis should review their data protection compliance strategy to ensure it is at the heart of their business operations.

[24] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), COM (2012) 11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 2 Apr 2016).