THE CJEU'S *WELTIMMO* DATA PRIVACY RULING

Lost in the Data Privacy Turmoil, Yet So Very Important

Case C-230/14 *Weltimmo*, EU:C:2015:639

Dan Jerker B. Svantesson*

§1. INTRODUCTION

On 1 October 2015, the Court of Justice of the European Union (CJEU) handed down its judgment in the dispute between Weltimmo s. r. o. (Weltimmo) and the Hungarian data protection authority (*Nemzeti Adatvédelmi és Információszabadság Hatóság*).[1] The decision is of the greatest importance in the context of jurisdiction and applicable law, but it has been largely overshadowed by other developments – not least by the CJEU's decision of 6 October 2015 invalidating the Safe Harbour scheme.[2] Despite lacking time in the limelight the long-term implications of the *Weltimmo* decision may be at least as far-reaching as those of the Safe Harbour decision.

§2. PROCEDURAL BACKGROUND

Weltimmo is a company that runs a property dealing website. The company is registered in Slovakia but the company website is focused on Hungarian properties. The business model that brought Weltimmo to the attention of the Hungarian data protection authority

* Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Visiting Professor, Faculty of Law, Masaryk University (Czech Republic). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

1 Case C-230/14 *Weltimmo*, EU:C:2015:639.

2 Case C-362/14 *Schrems*, EU:C:2015:650.

involved offering advertisers one month free of charge and then charging a fee. Despite many advertisers sending requests for the deletion of both their advertisement and their personal data at the end of the free period, Weltimmo did not delete the relevant data and charged those advertisers for the unwanted services. When the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers concerned to debt collection agencies.[3]

The advertisers complained to the Hungarian data protection authority, which fined Weltimmo HUF 10 million (approximately € 32,000). Weltimmo responded by bringing the matter before the Budapest administrative and labour court (*Fővárosi Közigazgatási és Munkaügyi Bíróság*), and the matter eventually made its way to the CJEU, via the Hungarian Supreme Court (*Kúria*).[4]

§3. THE QUESTIONS BEFORE THE CJEU

The Hungarian Supreme Court referred 8 questions to the CJEU. The Hungarian Supreme Court's first 6 questions related to whether Articles 4(1)(a) and 28(1) of Directive 95/46[5] must be interpreted as permitting the data protection authority of a Member State to apply its national data protection law to a data controller whose company is registered in another Member State as in the main proceedings. In the context of this, the Hungarian Supreme Court asked whether it is significant that the Member State concerned is the Member State: (a) at which the activity of the controller of the personal data is directed; (b) where the properties concerned are situated; (c) from which the data of the owners of those properties are forwarded; (d) of which those owners are nationals; and (e) in which the owners of that company live.[6]

As for the seventh question, the Hungarian Supreme Court asked about the correct interpretation of Article 28(1), (3) and (6) of Directive 95/46 in the event that the law applicable to the processing of the personal data is the law of another Member State rather than Hungarian law – would the data protection authority then be able to exercise only the powers provided for by Article 28(3) of the Directive, in accordance with the law of that other Member State? This was important because it meant they would not be able to impose penalties.[7]

The eighth and final question related to the interpretation of the term '*adatfeldolgozás*' (technical manipulation of data) used in the Hungarian implementation of Directive

3 Case C-230/14 *Weltimmo*, para. 9.
4 Ibid., para. 10–14.
5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.
6 Case C-230/14 *Weltimmo*, para. 19.
7 Ibid., para. 43.

95/46. The discussion of that matter was of limited importance and will therefore not be dealt with in this short case note.

§4. THE FIRST SIX QUESTIONS – ARTICLE 4(1) OF DIRECTIVE 95/46 AND THE APPLICABLE LAW

While the Hungarian Supreme Court referred to both Article 4(1) and Article 28(1) of Directive 95/46 in relation to questions 1 to 6, the CJEU (like the Advocate General before it) took the view that the only provision of importance in the context of questions 1 to 6 is Article 4(1) of Directive 95/46.[8] Specifically, Article 4(1)(a) reads as follows:

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> > (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

Article 4(1) of Directive 95/46 is complex and often misunderstood, or perhaps not sufficiently understood. Indeed, Bygrave has pointed to this Article as 'arguably the most controversial, misunderstood and mysterious of the Directive's provisions'.[9] In light of this, it is both noteworthy and praiseworthy that Advocate General Cruz Villalón devoted some time to clarifying the complex operation of this contested provision – clarification that was needed despite the Article 29 Working Party's opinion on applicable law.[10] Writing about Article 4(1) of Directive 95/46 in general, Advocate General Cruz Villalón states that '[t]his [Article 4(1)] contains different criteria for determining whether the national law, adopted to implement the Directive, is applicable. Through this, the actual Directive's geographical scope is determined indirectly (in that it stipulates that the national rules are applicable).'[11] This is surely a correct interpretation of the role of Article 4(1) of Directive 95/46, and as I pointed out in 2013, where we view the function of Article 4(1) of the Directive in this way, its *modus operandi* has obvious parallels in, for example, the correlation between subject-matter jurisdiction and applicable law under the US *Lanham Act* dealing with trademark cases.[12]

---

8 Ibid., para. 23.

9 L. Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014), p. 199.

10 Article 29 Working Party, Opinion 8/2010 on applicable law, WP 179.

11 Opinion of Advocate General Cruz Villalón in Case C-230/14 *Weltimmo*, EU:C:2015:627, para. 21, (author's translation of Swedish version – English translation not available at time of writing).

12 See further, D. Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013), p. 96–97.

At any rate, turning to Article 4(1)(a) of Directive 95/46 specifically, Advocate General Cruz Villalón points to its dual functions:

> On the one hand, it [Article 4(1)(a)] makes possible the application of Union law, through the legislation in one of the member states, when the processing of data is merely performed in the context of the activities of an establishment in that member state, even if the processing of the data actually takes place in a third state (which was the case in the Google Spain and Google case). On the other hand, this provision works as a rule governing the applicable law as between member states (which is the question in the present case). In the latter case, Article 4(1)(a) is the provision of the Directive that determines applicable law, in that it is a choice of law rule as *between* the different member states' legislations.[13]

This is also sensible and the Advocate General's clear reasoning enables a better understanding of this complex provision and its multiple functions.

Looking at Article 4(1)(a) of Directive 95/46 in more detail, it is now well established that, in applying this provision, the Court will take a 'consequence focused' approach;[14] that is, rather than restricting itself to a blind adherence to the exact wording of the Directive, it seeks to identify the consequences of the various possible interpretations.[15]

Further, the CJEU stated that '[t]he EU legislature thus prescribed a particularly broad territorial scope of Directive 95/46, which it registered in Article 4 thereof'.[16] There are two comments that should be made about this. First, it is refreshing to see an EU body acknowledging that the scope of the Directive is particularly broad. Second, at least from a pedantic point of view, it would, however, be appropriate to expressly acknowledge that the mentioned 'particularly broad territorial scope' in fact is so broad as to be 'extraterritorial'.

At any rate, the key question addressed in the context of Article 4(1)(a) of Directive 95/46 was the meaning of 'an establishment'. In that context, several facts of the case were seen to be of relevance. First of all, although the owner resides in Hungary, Weltimmo is registered in Slovakia and is therefore established there under Slovakian company law. However, Weltimmo carried out no activity in Slovakia and had representatives in Hungary. Weltimmo had opened a bank account in Hungary and had a post box there for its daily business affairs. The property website was written exclusively in Hungarian and dealt only with properties in Hungary. In light of all this, it is clear that Weltimmo

---

13 Opinion of Advocate General Cruz Villalón in Case C-230/14 *Weltimmo*, para. 23, (author's translation of Swedish version – English translation not available at time of writing; internal footnote omitted).

14 See further, D. Svantesson, 'What is "Law", if "the Law" is Not Something That "Is"? A Modest Contribution to a Major Question', 26 *Ratio Juris* (2013), p. 456.

15 'In the light of the objective pursued by Directive 95/46, consisting in ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, the words "in the context of the activities of an establishment" cannot be interpreted restrictively (see, to that effect, judgment in *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 53).' (Case C-230/14 *Weltimmo*, para. 25).

16 Ibid., para. 27.

had a substantial connection to Hungary and that Hungary had a legitimate interest in the matter. Thus, it was unsurprising that the Court held that Weltimmo pursued a real and effective activity in Hungary.

In this context, the Court stressed the need for a flexible definition of the concept of 'establishment', rather than a formalistic approach whereby undertakings are established solely in the place where they are registered. The CJEU concluded that in assessing whether a data controller has an establishment (within the meaning of Directive 95/46) in a Member State other than its country of registration, attention should be given to (a) the degree of stability of the arrangements and to (b) the effective exercise of activities in that Member State. This, the Court emphasized, must – not least for undertakings offering services exclusively over the internet – be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.

Pointing to the Directive's objective of ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, the CJEU stated that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question and; that the concept of 'establishment' extends to any real and effective activity – even a minimal one – exercised through stable arrangements.[17]

Furthermore, pointing to the judgments in *Lindqvist*[18] and *Google Spain and Google*,[19] the Court held that '[t]here is no doubt that that processing takes place in the context of the activities, as described in paragraph 32 of this judgment, which Weltimmo pursues in Hungary.'[20]

In summarizing its conclusions on questions 1 to 6, the Court expressed the following:

> Article 4(1)(a) of Directive 95/46 must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity – even a minimal one – in the context of which that processing is carried out;[21]

The Court also noted that:

> in order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing

17 Ibid., para. 29.
18 Case C-101/01 *Lindqvist*, para. 25.
19 Case C 131/12 *Google Spain and Google*, EU:C:2014:317, para. 26.
20 Ibid., para. 38.
21 Ibid., para. 41.

> takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned.[22]

Finally, the Court observed that 'by contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.'[23]

A. *WELTIMMO* AND THE 'TARGETING' APPROACH

The Court's application of Article 4(1)(a) of Directive 95/46 fits well with the approach adopted in the corresponding Article 3 of the forthcoming General Data Protection Regulation (GDPR),[24] which in turn draws from the approach adopted in the context of consumer protection in the Brussels I *bis* Regulation.[25] The decision is a clear and undeniable win for the 'targeting' thinking that is becoming more and more prevalent within EU law; that is, by looking at a range of factors such as the top-level domain name used, the currency or currencies in which payments are specified, and the language used, we are meant to determine whether or not the website in question has 'targeted' a particular Member State.

'Targeting enthusiasts' will no doubt tout this as a validation of the superiority of the targeting approach; after all, such an approach evidently worked very well in the *Weltimmo* decision. However, despite the success targeting had on this occasion, we would do well to remember that it is difficult to imagine a more straight forward fact scenario than that presented in *Weltimmo*. Indeed, I would go as far as to say that any jurisdictional filtering method that fails to reach a sensible outcome in a fact pattern such as that in *Weltimmo* may safely be disposed of in the nearest rubbish bin. In other words, the fact that the targeting approach worked so well in *Weltimmo* says very little about its general merits and suitability. Thus, the concerns I have expressed elsewhere about the targeting approach being applied as a jurisdictional filter in the data privacy setting remain.[26]

---

22 Ibid.

23 Ibid.

24 Agreement on the Regulation was reached between the Council, European Parliament and European Commission on the 15th December 2015 (see: Council Press Release of 18 December 2015, www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/). See further, C. Burton et al., 'The Final European Union General Data Protection Regulation', *Wilson Sonsini Goodrich & Rosati Website* (2016), www.wsgr.com/publications/pdfsearch/bloombergbna-0116.pdf.

25 Council Regulation (EC) No. 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L 351/1.

26 D. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation', 5 *International Data Privacy Law* (2015), p. 226–234.

§5. THE SEVENTH QUESTION – ARTICLE 28 OF DIRECTIVE 95/46 AND JURISDICTION

As noted above, the seventh question related to what measures would be at the Hungarian data protection authority's disposal if the answer to questions 1 to 6 were that Hungarian law is not applicable. While the CJEU's approach to questions 1 to 6 renders this question virtually superfluous as far as the *Weltimmo* case is concerned, it is still a matter of great importance.

Article 28(1), (3), (4) and (6) of Directive 95/46 are central in this context. Article 28(1) of Directive 95/46 reads as follows:

> 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.
> These authorities shall act with complete independence in exercising the functions entrusted to them.

Article 28(3) of Directive 95/46 outlines the powers with which each authority is endowed, including investigative powers, powers of intervention and the power to engage in legal proceedings.

Article 28(4) of Directive 95/46 adds that the authorities shall hear the claims lodged with them and that the person the claim concerns must be informed of the claim's outcome.

Finally, Article 28(6) of Directive 95/46 states that:

> 6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.
> The[27] supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

The complexities associated with applying this to situations such as those of the *Weltimmo* case had been anticipated, for example by the Article 29 Working Party, which is the advisory body to the Commission on matters concerning data protection. At any rate, having discussed this provision, and drawing upon the reasoning of Advocate General Cruz Villalón, the CJEU concluded that the answer to the seventh question is that:

> where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law

[27] See Article 29 Working Party, Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC (2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex3_en.pdf, p. 2.

> applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.[28]

A. *WELTIMMO* AND 'INVESTIGATIVE JURISDICTION'

It is illuminating to analyse the Court's conclusion in relation to the seventh question from the perspective of the categories of jurisdiction we can see in international law. Elsewhere, I have expressed the view that the 3 types of jurisdiction (adjudicative jurisdiction, legislative jurisdiction and enforcement jurisdiction), traditionally discussed in international law, can usefully be supplemented by a fourth category – what we can call 'investigative jurisdiction'.[29] In that context, it is interesting to note how the CJEU stresses that:

> [W]hen a supervisory authority receives a complaint, in accordance with Article 28(4) of Directive 95/46, that authority may exercise its investigative powers irrespective of the applicable law and before even knowing which national law is applicable to the processing in question. However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State.[30]

Thus, the data protection authorities' investigative power, of such central importance for the seventh question, does not fit well within any of the traditional categories since it is clear that a data protection authority may have the jurisdiction to investigate a matter but still lack the power to impose penalties.[31] This supports my claim that the traditional international law approach of grouping investigations within enforcement jurisdiction is unsound.

§6. CONCLUDING REMARKS

The *Weltimmo* decision can be seen to encourage data protection authorities (DPAs) to investigate foreign data controllers themselves rather than to rely on the collaboration

---

28 Case C-230/14 *Weltimmo*, para. 60.

29 See further, D. Svantesson, 'Will data privacy change the law?', *OUP Blog* (2015), http://blog.oup.com/2015/05/investigative-jurisdiction-law/.

30 Case C-230/14 *Weltimmo*, para. 57.

31 For a similar reasoning, also in the data privacy setting see the Canadian decision in *Lawson v. Accusearch Inc dba Abika.com* [2007] 4 FCR 314.

between DPAs catered for under Directive 95/46. At the same time, the decision can be seen to reaffirm the importance of cooperation between DPAs in the context of cross-border enforcement.[32]

At any rate, the most obvious impact of the *Weltimmo* decision is that it continues the trend started in the *Google Spain* decision of lowering the bar, or indeed changing the focal point, in the assessment of what amounts to an 'establishment' under Directive 95/46. This can perhaps be seen as a natural adjustment given how e-commerce is developing, and this type of adjustment is not specific to the data privacy context. Nevertheless, it arguably amounts to a step away from the more simplistic, indeed overly simplistic, 'country-of-origin' thinking for online business such as that expressed – somewhat flippantly – in the 2000 E-commerce Directive;[33] after all, the goal of simplicity and predictability is seriously undermined where the location of 'establishment' is not easily ascertainable.

This, in turn, sends the signal that those multinationals that have assumed that they need only take account of the law of the country of their incorporation must reassess their practices. The same can be said for those businesses that specifically target data subjects in countries other than the country of their incorporation; they can no longer assume that they need only consider the law of the country of their incorporation. This change will likely add to the overall cost of compliance. However, the playing field will change again once the GDPR takes effect since the 'one-stop-shop' of the original 2012 proposal has survived the Trilogue negotiations, be as it may in a 'weaker and more complex'[34] form. Under this structure '[t]he DPA of the main establishment of a company in the EU will take the lead in supervising the company's compliance across the EU in accordance with the cooperation procedure'.[35] Importantly:

> the criterion for determining where a company has its 'main establishment' will be the location of the company's central administration in the EU (Article 4 (13)). The 'central administration' of a controller relates to the 'effective and real exercise of management activities' that determine the main decisions regarding the purposes and means of processing through 'stable arrangements.'[36]

---

32 M. Kawecki and D. Kloza, 'Weltimmo, Schrems and the reinforcement of cooperation between European data protection authorities', *Phaedra* (2015), www.phaedra-project.eu/weltimmo-schrems-reinforcement/.

33 Directive (EC) 2000/31 of the European Parliament and Council, 8 June 2000, on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, [2000] OJ L 178/1. See in particular Article 3 of Directive 2000/31.

34 C. Burton et al., 'The Final European Union General Data Protection Regulation', *Wilson Sonsini Goodrich & Rosati Website* (2016), www.wsgr.com/publications/pdfsearch/bloombergbna-0116.pdf, p. 12.

35 Ibid., p. 11.

36 Ibid.

Unsurprisingly, this approach corresponds well to the CJEU's approach in *Weltimmo*, or of course *vice versa*.

The proper place that the *Weltimmo* decision will hold within the data privacy framework of the EU, and indeed more broadly within the EU's legal framework, remains to be seen. However, as is hopefully clear from this brief case note, the decision undeniably:

1. addresses a topic of great significance;
2. provides valuable insights into the application of the current Directive 95/46; and
3. provides valuable insights into the CJEU's thinking on data privacy more broadly and undoubtedly sends signals as to how it will approach matters arising under the forthcoming GDPR.

I have a feeling that the impact of the *Weltimmo* decision will be felt long after people have forgotten about Max Schrems and the 2015 Safe Harbour decision. The future will tell.