EU Data Protection and the Conflict of Laws: The Usual "Bag of Tricks" or a Fight Against the Evasion of the Law?

By: Paul Lefebvre and Cecilia Lahaye

Admitted to the Bar in 1985, Paul Lefebvre is one of the twenty lawyers of the Belgian Supreme Court (Cour de cassation/Hof van Cassatie) and one of the four founding partners of the law firm Hanotiau & van den Berg, which was established 2001 and is widely recognized as leader in the field of commercial arbitration and litigation. Hanotiau & van den Berg won the Belgian Legal Award both in 2006 and 2007 in the field of ADR & Arbitration.

Cecilia Lahaye is an attorney at Van Olmen & Wynant (Brussels, Belgium), specializing in employment law. She has also worked as legal counsel to attorneys appointed to the Belgian Supreme Court, concentrating on labor and social security law.

UNTIL April 2016, the basic principles on the protection of personal data of EU citizens were laid down in Directive 95/46/EC, issued October 24, 1995.[1] This Directive served a

[1] 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

double purpose: to ensure the free flow of data from one Member State to another within the internal market; while safeguarding the individual's fundamental rights and freedoms including, notably, his right to privacy. Because differences in the level of protection of an individual's rights with regard to the processing of his data constitute obstacles to the free flow of data, and thus distort competition, the Directive sought to coordinate the divergent laws of the member States in order to remove these obstacles in a manner that provides for a high level of protection for all EU citizens. As a legal instrument, a directive is only binding upon each Member State with regards to the result to be achieved; it has no direct effect and cannot be invoked by private parties. Moreover, Member States are still left a margin to maneuver, which allows them to specify in their national law the general conditions governing the parameters of lawful of data processing, so the Directive acknowledges that new disparities may well arise.[2]

The new General Data Protection Regulation (GDPR), [3] adopted by the Council and the European Parliament in April 2016, brings data protection within the EU to a higher level by establishing a new and harmonized data protection framework across the EU. As a legal instrument, it is of a higher order than a directive because it establishes a single body of law that is directly applicable in the EU Member States. As of May 26, 2018, the GDPR will be directly effective in all EU Member States without the need for national implementing laws, as were required under the Directive.

The aim of the GDPR is to set up a digital single market, with the highest possible common standards for all citizens of the EU Member States, so that each individual remains in control of his or her personal data. This set of unified rules will not only warrant the consumer's trust but also provide businesses with a level playing field throughout the EU when setting up new businesses in the digital economy. At the core of the GDPR lies the rule: "one continent, one law." Companies based outside of the EU will have to apply the same rules when offering services in the EU and should only have to deal with one supervisory authority (a one-stop-shop system),

---

and on the free movement of such data, OJ L 281, 23/11/1995, pp. 31-50.

[2] Directive 95/46/EC, consideration (9).

[3] Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119, 4/5/2016, pp. 1-88. It enters into application May 25, 2018 after a two-year transition period.

leading to savings estimated at EUR 2.3 billion per year.[4]

Under the Directive, the legal issues of jurisdiction and applicable law were extremely controversial, giving rise to much case-law and doctrine. A new element introduced by the GDPR is its extra-territorial reach: it will not only apply to businesses established within the EU but also to businesses based outside the Union that offer goods and services to, or monitor individuals in, the Union. This article examines to what extent the principles developed by the case law of the Court of Justice of the European Union (CJEU) still apply under the GDPR and, if so, to what extent they can still be used as a source of inspiration in resolving these questions.

I. From a Patchwork of 27 National Rules to the 'One-Stop-Shop'

The framework established by the GDPR consolidates the "one-stop-shop" principle already set forth under the Directive; the aim of the GDPR is to ensure that businesses only need to deal with a single supervisory authority (SA) for all processing carried out in the Union, rather than having to deal with the SA of each of the Member States in which the business is active. However, this initial proposal was watered down, mostly following concerns from Member States over the inability of some smaller supervisory authorities to adequately regulate larger businesses, and that these larger businesses would therefore seek to establish themselves in their jurisdiction. Language barriers and local laws were also seen as an impediment to a true "one-stop-shop" system.

As a general rule, following the one-stop-shop rule, the GDPR provides that a business should be regulated by the SA where it has its main establishment, which will be called the "lead SA."[5] There are two exceptions to this rule: (i) a local SA will still have jurisdiction where processing is carried out by public

[4] Available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm, for the Council; http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm, for the European Commission and http://www.europarl.europa.eu/news/en/news-room/20151217IPR08112/new-eu-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat, for the European Parliament.

[5] Article 56 (1) GDPR: ". . . the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60." Under EU law, an establishment refers to a place where business is deemed to be conducted, whether or not a separate legal entity. Thus the "main establishment" may be seen as somewhat analogous to what is referred to in United States law as a "principal place of business".

authorities or private bodies acting on the basis of the legal obligation or public functions;[6] and (ii) a local SA can ask the lead SA to be allowed to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. [7] If the lead SA decides to handle the complaint, it will cooperate closely with the local SA in accordance with the procedure set out in Article 60 of the GDPR. The lead SA would then be responsible for overseeing all supervisory and enforcement actions across other EU Member States.[8]

Hence, under Article 56 of the GDPR, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for any cross-border processing carried out by that controller or processor. The GDPR further develops the cooperation mechanisms[9] that the lead supervisory authority and the other relevant authorities should follow for the application of the GDPR.

Although the GDPR will only apply throughout the EU from May 25, 2018 onward, Member States already have a duty of loyalty and cooperation towards the EU and its objectives. The CJEU has stipulated in similar circumstances where new EU legislation is about to come into effect that "Member States to which [a] directive is addressed [should] refrain, during the period laid down therein for its implementation, from adopting measures liable seriously to compromise the result prescribed."[10]

Under the Directive, determining the applicable law was a three-step process: (1) first, one had to determine who is the controller of the data processes; (2) whether he has one or more establishments within the EU; and (3) if so, which of these establishments is "more closely linked" to the data processing at

[6] Article 55 (2) and Article 6 (1)(c) or (e) GDPR. This exception will only marginally, if at all, affect international businesses.

[7] Article 56 (2) and (3) GDPR.

[8] Article 60 GDPR. It is up to the lead SA to decide whether or not it will allow the local SA to handle a complaint. In all likelihood, the lead SA will be quite reluctant to relinquish its authority to the lead SA. Therefore, this exception will most probably not affect international businesses.

[9] This cooperation principle already existed under Directive 95/46/EC.

[10] Case C-129/96 *Inter-Environnement Wallonie ASBL v Région Wallone* [1997], para. 50. One could argue that this case law does not only apply Directives but also to Regulations. Although the Regulation is not yet applicable, the existing legislation should not be interpreted against the *ratio legis* of this future legislation.

hand than the others. This determination is a factual matter. It was for the Courts to examine and determine the exact scope of the activities of European subsidiaries of multinational corporations.

We will look at each of these steps and examine whether or not these principles still hold under the GDPR and/or if other steps need to be taken into consideration. This analysis will show that the GDPR does not substantially affect the determination of either the jurisdiction of the SA or the applicable law.

A. Step 1: Who Is the Data Controller?

Under Article 2(d) of Directive 95/46 "data controller" was defined as the natural persons or entities "which alone or jointly with others determines the purposes and means of the processing of personal data", i.e. the one who determines the "what", "why" and "how" of certain processing activities. [11] In determining the "*means*", not only the technical and organizational questions are relevant, (e.g. the question which hardware or software must be used) but also the substantive core questions that are only dealt with and answered by the data controller, such as "which data shall be processed?", "for how long shall it be processed?" and "who shall gain access to this data?" Of particular interest are the comments of the Article 29 Working Party on the initial draft Directive, which specify four essential criteria in identifying the controller: purpose, personal data, processing and third-party access to data.[12]

The core rule that the data protection rules apply to the processing of personal data by a controller or processor remains the same under the GDPR. Article 4 (7) of the GDPR retains the same definition of "controller" as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It adds that, where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. A new element under the GDPR is the provision that, unlike under the

[11] Terms used by the Article 29 Data Protection Working Party on the original draft Directive, i.e. a Group of national privacy supervisory organizations, established under Article 29 of the Directive, hence its name. The EDPB (European Data Protection Board) will replace Article 29 Working Party.

[12] Article 29 Data Protection Working Party, Opinion 1/2010 on the concept of controller and processor, at 32.

Directive, the actual processor of the personal data[13] will become directly liable for compliance with some parts of the Regulation.

In practice, where a multinational corporation has different entities within the European Union, the entity that qualifies as "controller" can be identified on the basis of the following questions:

1) Does this entity devote substantial resources (e.g. staff, financial means) to data protection compliance?
2) Does it determine the corporation's policies on data use within the Union, ensuring that new products are compliant with EU legislation?
3) Does it decide on the withdrawal of certain products, should they appear not to meet with the EU requirements?
4) Does this entity decide on a third party to be given access to the personal data that it holds and under what conditions?
5) Is there a contractual relationship between this entity and the data subject, allowing for the data subject to make enquiries about their data before this entity or, possibly, lodge claims and complaints before this entity?
6) Is this entity the focal point with regard to law enforcement and police investigations regarding personal data?
7) Does it engage with the local Data Protection Control Agency in order to ensure its compliance with both local as well as EU Data Protection legislation?

The fact that a subsidiary company is "controlled" by the parent company from a corporate law point of view, does not imply that the parent is to be considered as the controller in the sense of the GDPR.[14] Indeed, the company's corporate structure is irrelevant in determining who is to be considered as "controller" or "co-controller"[15] for the purpose of the GDPR.

B. Step 2: Does the Data Controller Have More Than One Establishment in the EU?

As its recitals confirm, Directive 95/46/EC was originally implemented to safeguard data privacy rights, while also allowing personal data "to flow freely from one

[13] E.g. a company's payroll agency or a cloud provider that offers data storage.

[14] See Lokke Moerel, *Back to basics: when does EU data protection law apply?,* in INTERNATIONAL DATA PRIVACY LAW, 8 (Oxford, 2011) (explaining that even a "branch office can also qualify as a controller. The fact that a branch is not a separate legal entity is not a decisive factor […].").

[15] *Cf. supra* note. 4.

Member State to another" to promote "the establishment and functioning of an **internal market** in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured."[16] Directive 95/46/EC was thus intended to "ensure a high level of protection" of the right to privacy in the EU,[17] as well as to "address differences in the levels of protection of […] the right to privacy" that were "an obstacle to the pursuit of a number of economic activities at Community level."[18] Directive 95/46/EC sought to achieve "the **equivalent protection** resulting from the approximation of national laws" so that "the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to […] the right to privacy."[19] This intention is made clear in the European Commission's preparatory discussions for Directive 95/46/EC,[20] and scholars have also emphasized the strong Internal Market component of Directive 95/46/EC.[21]

Unsurprisingly then, the applicable law provisions in Directive 95/46/EC seek (i) to avoid the circumvention of European data protection rules and (ii) to prevent an overlap of multiple rules applying to a particular processing activity that would impede the functioning of the EU Internal Single Market.[22] Article 4(1)(a) of Directive 95/46/EC accordingly reads:

> "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

[16] Directive 95/46/EC Recital (3).
[17] Directive 96/46/EC Recital (10).
[18] Directive 95/46/EC Recital (7).
[19] Directive 95/46/EC Recital (9) and Article 1.
[20] COM92 (422) Final – SYN 287, 15 October 1992, at 13. Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 15 October 1992, available at http://aei.pitt.edu/10375/1/10375.pdf.
[21] *See* M-H. Boulanger, C. de Terwangne, T. Léonard, S. Louveaux, D. Moreau, Y. Poullet, *La protection des données à caractère personnel en droit communautaire*, 40 JOURNAL DES TRIBUNAUX DROIT EUROPÉEN (Larcier, 1997).
[22] *See* COM(90) final – SYN 287 and 288, 13 September 1990, at 22 and COM(92) 422 final – SYN 287, 15 October 1992, at 13. The Article 29 Working Party has opined that the application of choice of law rules "should prevent the simultaneous application of more national laws to the same processing activity." Opinion 8/2010 on applicable law, 16 December 2010, at 10.

> 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."

Moreover, the Article 29 Working Party, [23] the Advocates General in the *Weltimmo* and *Amazon* cases,[24] as well as national courts, [25] all have acknowledged that the prevention of overlapping applicable laws is one of the key purposes of Directive 95/46/EC.

Article 4(1)(a) (and the national laws that give effect to it) must accordingly be applied in a way that prevents the multiple and overlapping application of data protection rules by different Member States to the same data processing activity. Any contrary interpretation would violate Article 56 TFEU and the Internal Market objective of Directive 95/46/EC, based on CJEU case law. [26] Moreover, an undue overlap of national laws would create the exact situation that Directive 95/46/EC was designed to avoid: "differences in the level of protections of […] the right to privacy […] constitut[ing] an obstacle to the pursuit of […] economic activities at the community level"[27] that are "vital to the internal market."[28]

Article 4(1)(a) only applies when a data controller has at least one establishment within the EU. Specifically, Article 4(1)(a) indicates that a Member State's law applies if "processing is carried out **in the context** of the activities **of an establishment of the controller** on the territory of the Member State [. . .]" (emphasis added). The key issue is therefore what is meant by data processing "carried out in the context of the activities of an establishment of the controller." This requirement will obviously be satisfied as soon as an EU establishment is the data controller for the data at issue.

---

[23] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 16 December 2010, at 5: "rules on applicable law also determine the scope of data protection law within the EU/EEA, so as to avoid possible conflicts between and overlapping of the national laws of the EU/EEA Member States implementing the Directive."

[24] CJEU, 1 October 2015, no C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*) Opinion of the AG of 25 June 2015, at para. 23, which refers to Article 4 of Directive 95/46/EC as establishing a rule on conflict of laws, which necessarily means that certain laws will apply to the exclusion of others. *See also* CJEU 28 July 2016, no. C-191/15, ECLI:EU:C:2016:612 (VKI v. Amazon EU) Opinion of the AG of 2 June 2016, at paras. 112 and 125.

[25] *For example, see Hamburg Judgment*, nr 7 ii and iii.

[26] CJEU, 4 December 1986, no C-205/84 ECLI:EU:C:1986:463 (*Commission v. Council*).

[27] Directive 95/46/EC Recital (7).

[28] Directive 95/46/EC Recital (8); *see also* Directive 95/46/EC Recital (3).

The very same principles—providing the highest possible standard of protection to data subjects while ensuring the free flow of data within the union—lie at the core of the General Data Protection Regulation. Article 3 states that the "Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union *…".*

However, what is new is the extraterritorial scope of the GDPR, as it applies: "regardless of whether the processing takes place in the Union or not" and that "this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

> *(a)* the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
> *(b)* the monitoring of their behavior as far as their behavior takes place within the Union*."*

Although Article 3 of the GDPR operates in the same way as the equivalent Article 4 in the Directive, it does so where a controller is established either inside or outside of the EU.

Article 4(1)(a) of the Directive only applies when a data controller has at least one establishment within the EU. Specifically, Article 4(1)(a) indicates that a Member State's law applies if "processing is carried out **in the context** of the activities **of an establishment of the controller** on the territory of the Member State [. . .]" (emphasis added).

C. Step 3: Which Establishment Has the Closest Link to the Data Processes?

Under the Directive, if both or several establishments meet the requirement of acting as the data controller, the applicable law will then be determined by which establishment is "most closely connected to the data processing." Indeed, in order to ensure the internal market objective of free movement of personal data,[29] only one national law should apply to cross border data processing within the EU. This interpretation has been supported in the following court cases:

i. In *Weltimmo*, the EU Advocate-General indicated that "Article 4(1)(a) of the directive is the provision

[29] Directive 95/46 – Recital 3.

which determines the applicable law in so far as it is a rule governing conflict between the laws of the different Member States." [30] This conclusion was implicitly embraced by the CJEU in the same case, when it indicated that "any processing of personal data in the European Union must be carried out in accordance with the law of **one** of the Member States and that processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State" (emphasis added).[31] Thus, Directive 95/46/EC was intended not to lead to the application of multiple data protection laws of different Member States.

ii. In *Facebook v Hamburg DPA*, [32] the Hamburg Administrative Court embraced the Advocate-General's interpretation in *Weltimmo*, indicating that "the conflict-of-laws rule of Directive 95/46/EC is intended to avoid not just lapses in protection but also instances of overlap between individual states' legal orders if the responsible entity has establishments in several member states" and that "[i]t was to be avoided that multiple national legal orders apply to the same instance of data processing."

iii. Accordingly, the Hamburg Administrative Court confirmed that, where there are two potentially applicable establishments within the EU for the purposes of Article 4(1)(a), the applicable law will be determined by which establishment is "most closely linked" to the disputed data processing: "the applicable law should be that of the country that hosts the establishment whose activities are most closely linked to the processing data in dispute", which the Hamburg Court correctly determined to be Irish law, concluding that "if

[30] *See* Advocate General, *Weltimmo*, at para. 23.

[31] *See* CJEU, *Weltimmo*, at para. 26.

[32] *See* Hamburg Verwaltungsgericht, 3 March 2016, E4482/15, http://justiz.hamburg.de/contentblob/5359282/c0489 0044471740ab40b6d17dbd2d985/data/15e4482-15.pdf;jsessionid=A26A8798A876B8DDE8A7038638CEC293.liveWorker2; hereafter "the Hamburg Judgement"- all quotes are non-official translations from German.

> it is learned in the process that [Facebook GmBH] processes personally identifiable data not primarily as part of its own activities but as part of the activities of another establishment [Facebook Ireland], the data-protection provisions of such member state as may host the establishment in question apply."
>
> The test requires a detailed analysis of the factual role played by the establishments within the EU: "In the event that data-processing activities are undertaken "in the context of the activities" of establishments in several member states, one will have to refer to the very activities of which such processing formed part (cf. CJEU, opinion dated 25 June 2015, C-230/14, juris, margin no. 40 – *Weltimmo*), and the location of such permanent establishment as may be at the center of the data-processing activities counts *(cf. Schreibauer, in: Auernhammer*, BDSG, 4th edition 2014, preamble ad § 11 TMG, margin no. 25, ad § 1 para. 5 sentence 1 BDSG)." The Court must therefore "delineate the activities of each individual establishment. And if it is learned in the process that one of them processes personally identifiable data not primarily as part of its own activities but as part of the activities of another establishment, the data-protection provisions of such member state as may host the establishment in question apply."
>
> The Hamburg Administrative Court expressly confirmed that the "most closely linked" test was required by the Internal Market rules and principles to "avoid […] a scenario in which the providers of cross-border tele media services, for example, must observe a multitude of different member-state data protection Acts with respect to the same instance of data processing."[33]

[33] *See also* Recitals (8) and (9) of Directive 95/46/EC, in particular: "Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy."

On appeal, the Hamburg Higher Administrative Court concluded that the Hamburg DPA had not presented sufficient evidence or case law to overturn the judgment of the first instance Hamburg Administrative Court.[34]

iv. More recently, in the *Amazon EU* case of 28 July 2016, another EU Advocate-General supported the same interpretation as its homologue in the *Weltimmo* case, acknowledging the following:

"[O]nly the law of the Member State of the establishment in the context of whose activities that operation is carried out will be applied." […] "[I]t must be determined which, among several national laws transposing the directive, is intended to govern the data processing operations provided for in the terms at issue. This means identifying the establishment in the context of whose activities those operations are most directly involved."[35]

In its final Judgment, the CJEU implicitly accepted the view that only one law may apply to a cross-border data processing activity within the EU. In multiple instances, [36] the CJEU referred to the sections of the Advocate-General's Opinion that supported this outcome. Furthermore, the CJEU never referred to the possibility that more than one law could apply to the same data processing activity:

"Article 4(1)(a) of Directive 95/46 must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is

---

[34] Court Reference 5 Bs 40/16; https://openjur.de/u/897676.print; It is noted that the Hamburg Higher Administrative Court rejected the appeal of the Hamburg DPA on other grounds than those used by the Hamburg Court in first instance.

[35] http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d0f130d69092727f2ea24ce796228ff8c97d7836.e34KaxiLc3eQc40LaxqMbN4Pax0Ne0?doclang=EN&text=&pageIndex=0&docid=182286&cid=846036; Case C-191/15; See Opinion of the Advocate-General in *Amazon EU*, at para. 112 and 125; http://curia.europa.eu/juris/document/document.jsf?text=&docid=179322&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=846476.

[36] *See Amazon EU*, at paras. 76 and 80 as regards the views on the application of Directive 95/46/EC.

> governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State."[37]
>
> The CJEU continued by indicating that it was for the national judge to determine whether the data processing at issue was taking place in the context of the activities of an Amazon entity other than Amazon Luxembourg, but that "if the referring court were to conclude that the establishment in the context of which Amazon EU carries out the processing of that data is situated in Germany, it would be for German law [and not Luxembourgish law] to govern the processing."[38]

This finding also accords with the fundamental principles of free movement of services across the EU and avoids the risk of undue overlap and hindrance of the efficient operation of the Internal Market. In this context, the foregoing court judgments and opinions are consistent with the Opinion 8/2010 of the Article 29 Working Party, which confirms that "[t]he purpose of clear criteria for determining the applicable law is to avoid both circumvention of Member States' national rules, and overlap of those rules" and that "[a]pplication of the criteria should prevent the simultaneous application of more national laws to the same processing activity."[39] The Article 29 Working Party did not edit these statements in the Update[40] of Opinion 8/2010 on applicable law in light of the CJEU judgement in *Google Spain*, issued on December 16, 2015.[41]

If the link between the data processing at issue is manifestly greater with one establishment than with another, the first one should take prevalence as the one that holds the key data controlling role, i.e. the "most closely linked to the data-processing activities in dispute." Only the law of that

---

[37] *See Amazon EU*, at para. 81.

[38] *See Amazon EU*, at para. 80.

[39] *See* Opinion 8/2010 on Applicable Law, of 16 December 2015 at pp. 9-10.

[40] As the Update is the result of a Working Group that reunites the supervising authorities most fiercely opposing the '*one law principle*', this update has to be considered most cautiously if at all: it extrapolates the *Google Spain* case law to all possible situations of data processing thereby making abstraction of the circumvention aspects characterizing this case.

[41] *See* Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in *Google Spain*.

establishment would govern the data processing at hand.

The *Google Spain, Weltimmo* and *Amazon* judgments cannot be invoked to justify that more than one SA would have jurisdiction over a same processing activity and that more than one law would be applicable.

(i) *Google Spain*

In its decision of 13 May 2014 in the case of *Google Spain*, the CJEU found that, where the data processing is not carried out under the control of an establishment within the EU, the "in the context of" requirement will nevertheless be fulfilled if there is an "inextricable link" between the activities of a non-EU establishment carrying out the data processing activities and the activities of the EU establishment. In reaching this conclusion, the CJEU gave specific regard to the fact that the data controller (Google, Inc., an entity domiciled in the USA) was not otherwise established in another Member State and was seeking to circumvent the protections of Directive 95/46/EC.[42] The CJEU accordingly held that the commercial and marketing activities of Google Spain with regard to advertising space were "inextricably linked" to the data processing occurring in the operation of Google, Inc.'s search engine, and the "in the context of" requirement was therefore met.[43]

The CJEU adopted an expansive definition of "in the context of" in *Google Spain*, to establish a "link" between the activities of Google, Inc. and Google Spain, because, without such a link, the Google platform operated from outside the EU would have been able to circumvent the European data protection regime entirely. Thus, the issue at hand in *Google Spain* was whether any EU law applied to the processing of data within the EU by Google Inc. (located in United States), in circumstances where Google Inc. had deliberately sought to evade EU data protection regulation by seeking to ensure that there was no establishment within the EU linked to Google, Inc.'s processing of data. The approach followed by the European Court of

[42] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d6490bc8978c37487996c1fdff9a2e3c1f.e34KaxiLc3eQc40LaxqMbN4Pax0Ne0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=846861; *see* paragraph 58: "…It cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure…".

[43] *See* Case C-131/12 *Google v AEPD* [2014] ECLI:EU:C:2014:317, at para. 56.

Justice is therefore in line with the intended effect of Directive 95/46/EC at the moment it was drafted: the broader wording "in the context of which [i.e. the place of establishment of an establishment of the controller] the processing activities take place" was specifically chosen so as to prevent circumvention of the Directive.[44]

As noted by the CJEU, "it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the [data protection] obligations and guarantees laid down by Directive 95/46 […]".[45] It was for this reason that the CJEU found in concreto that "the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in **a third State** but has **an establishment in a Member State**, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine" (emphasis added).[46]

This interpretation was followed by the Hamburg Administrative Court, which confirmed that the extensive interpretation of the words "in the context of the activities" used in Article 4(1)(a) of Directive 95/46/EC by the CJEU in the *Google Spain* and *Weltimmo* cases was not justified outside a case of circumvention of EU data protection laws, and that, where there are multiple establishments within the EU, the correct test is which establishment is "most closely linked to the data-processing activities in dispute".

The Hamburg Court also confirmed that the CJEU in *Google Spain* "was tasked with the adjudication of a case that differs markedly from the present one: […] the data-processing activities in dispute there were controlled by an entity not domiciled within the geographic scope of Directive 95/46/EC." Accordingly, "there was reason to fear that the personal data of the affected Union citizens were being processed in violation of the standards of Directive 95/46/EC". Therefore, the CJEU intended "to allow Union law to apply […] in order to avoid that a person's protection granted in accordance with the directive is withheld or circumvented." Thus, the Hamburg Judgment concluded that "the case constellations are not comparable" as the controller in the German case (as well as in the Belgian case) "has an establishment in an EU member state" so that "there is no reason for concern that the Union citizens affected by the processing of data in question could

[44] *See id.* at paras. 175-195, comparing the different versions of Directive 95/46.

[45] *See id.* at paras. 58 and 68.

[46] *See id.* at para. 55.

be denied the protection of Directive 95/46/EC".[47]

In contrast, where the processing is carried out under the control of an establishment within the EU, the data protection regime plainly applies to the data processing in question. Thus, as confirmed by the Hamburg Judgments, if one assumes that the controller has more than one establishment in two or more Member States, only the law of the Member State hosting the establishment that is "most closely linked" to the data processing at issue will apply.

The reasoning of the CJEU in *Google Spain* is accordingly limited to preventing legal circumvention where a foreign data controller with an EU establishment would escape regulation altogether unless a broad interpretation of the "in the context of" requirement was adopted. [48] Indeed, the CJEU's references to its decision in *L'Oréal v. eBay*, a case where eBay was arguing the inapplicability of the e-Commerce Directive 2000/31/EC to the case at issue given the operation of the eBay.com website from the U.S., underline that the CJEU's clear intention was to thwart Google Inc.'s attempt to circumvent EU data protection requirements.[49] Only with a view to avoiding such law evasion, the CJEU clearly opted for a broad interpretation of the terms "*in the context of*" in article 4(1)(a) of Directive 95/46 and "*inextricably linked*". However, this line of reasoning would not apply as a general rule, since it would lead to the applicability of more than one Member State's law on data protection, thus elevating new obstacles to the free flow of data that the Directive seeks to ensure.

The *Google Spain* decision is further not applicable where there are two (or more) applicable establishments within the EU for the purposes of Article 4(1)(a), because such application would violate the principles of the Single Market enshrined in Directive 95/46/EC.

(ii) *Weltimmo*

The CJEU's decision in *Weltimmo* is similarly driven by the need to curb an attempt to

[47] The Hamburg Judgment goes on by quoting the updated opinion of the Article 29 Working Party that also "concedes that Directive 95/46/EC would guarantee the relatively high level of protection afforded for affected parties in a constellation of this kind" at 6.

[48] The CJEU's reference to "third State" in Paragraphs 55 of *Google Spain* parallels Directive 95/46's use of the term in "third country" in Recital 20 to refer to a data controller established in a non-Member State.

[49] *See Google Spain,* ECLI:EU:C:2014:317, at para.s 53 and 58. In *L'Oréal v. Ebay*, the CJEU interpreted trademark laws very expansively to protect the rights of trade mark owners from violations by companies established outside the EU in order to evade such regulations.

circumvent European data protection law, which took the form of repeatedly switching the data controller's registered "office from one State to another" within Europe.[50] The case was particularly egregious (if not fraudulent) because the website owner offered potential advertisers one month of free advertising to encourage them to sign up to the service, but then disregarded all requests to cancel the contract after a month and billed them for advertising thereafter.[51]

Weltimmo was structured to evade EU data protection law. Weltimmo's business activities took place in Hungary, [52] but the company was registered in Slovakia. Weltimmo "did not carry out any activity at the place where it has its registered office," [53] and, "on several occasions, Weltimmo moved that registered office from one State to another."[54] Weltimmo would then use the constantly shifting location of its registered office to escape any form of data protection scrutiny.[55]

The CJEU first indicated that "any processing of personal data in the European Union must be carried out in accordance with the law of one of the Member States and that processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State" [56] thereby implicitly acknowledging that Directive 95/46/EC is not meant to lead to the application of multiple data protection laws of different Member States. It then took a dim view of Weltimmo's attempts to circumvent the effective application of European data protection law,[57] and interpreted the definition of "establishment" expansively, [58] because it was the only way to prevent Weltimmo from dishonestly evading EU regulation.[59]

As in *Google Spain*, there was no need to consider whether any other establishment within the EU had a stronger inextricable link, because there was no other establishment within the EU with any link to the data processing in question. As Advocate General Villalón observed, the question whether the processing of data occurred "within the framework of the activities of an establishment" was not at issue given the obvious role played by the establishment in relation to the data processing.[60]

As the Hamburg Judgment has also noted, in *Weltimmo*: "the court

[50] *Weltimmo*, ¶ 16.
[51] *Weltimmo*, ¶ 9.
[52] *Weltimmo*, ¶ 32-33.
[53] *Weltimmo*, ¶ 16.
[54] *Id*.
[55] *Weltimmo* ¶¶ 11-12.
[56] *Weltimmo*, ¶¶ 26 (emphasis added).
[57] The location of Weltimmo's servers was "not settled" when the CJEU handed down its decision. *Weltimmo*, ¶ 18.
[58] *Weltimmo* ¶¶ 28-33.
[59] *Weltimmo* ¶ 38.
[60] Advocate General *Weltimmo* ¶ 26.

primarily looked into the question whether the controller within the meaning of Directive 95/46/EC was established in Hungary for purposes of data-protection law even though it was listed with a Slovakian register (. . .) and only the location of the establishment was in dispute there, as opposed to whether the data-processing at issue had been undertaken as part of such establishment's activities [. . .] the court's decision was likely made in light of the fact that the Slovakian authorities faced dismal prospects in going after the undertaking on grounds of data-protection law. Apparently, it was safe to assume that Weltimmo repeatedly moved its principal place of business from one country to another and did not engage in any activities at its registered offices in Slovakia (. . .)." The Hamburg Judgment noted, on the other hand, that "[t]he risk of the Plaintiff [Facebook Ireland] evading any meaningful control by the Irish data-protection authorities neither has been asserted nor is apparent."[61]

Thus, neither *Google Spain* nor *Weltimmo* provide any guidance on how the phrase "in the context of" should be interpreted where there is a data controller within an EU Member State which is responsible for the processing of the data in question.

Outside the specific context of attempts to circumvent European data protection law, the only questions to be answered when determining the applicable law are (1) whether another EU Member State's law enacting Directive 95/46/EC already applies to the same data processing activity; and (2) if so, which law should prevail. The answer to each of these questions is unaffected by the CJEU decisions in either *Google Spain* or *Weltimmo*.

As in *Google Spain*, the CJEU opted for a broad interpretation of the term "establishment" in order to fight the circumvention of the Hungarian law (and competence of the Hungarian supervising authority) due to the Slovakian sham construction.

(iii) The *Amazon* case

This case concerns the distinct matter of e-commerce. Amazon Luxembourg is part of an international mail order group. The Luxemburg company addresses consumers via a website with a domain name with the extension "*.de*", but also aimed at consumers residing in Austria, with whom it concludes electronic sales contracts. An Austrian consumer's organization challenged the validity of the general conditions of Amazon Luxembourg.

[61] *See* note 32, consideration (ee), p. 25.

One of the questions raised by the Austrian Supreme Court was whether or not the processing of data by an undertaking active in e-commerce is governed by the law of the Member State to which that undertaking directs its activities. In this context, three laws come into account: the Luxembourg law of the Luxembourg establishment, the German law of the domain name extension and German consumers, or the Austrian law of the Austrian consumers.

The Advocate General insisted on this peculiar character of the Amazon case:

> "I doubt, however, whether that approach [the approach by the CJEU in the *Google Spain* case that read Article 4(1)(a) of the Directive 95/46 broadly] can be applied to the present case. Apart from other factual differences, that case differs from the present case in that it was a matter of assessing, in that case, whether the processing of data concerned was covered by the framework for protection established by Directive 95/46 (through the Spanish law transposing it). It was, in my view, from that perspective that the Court interpreted broadly the second condition laid down in Article 4(1)(a) of that directive in order to prevent such processing from escaping the obligations and guarantees provided for in the directive."[62]

The Advocate General concluded in crystal clear terms to the applicability of one single law: "in the present case, on the other hand, it must be determined which, among several national laws transposing the directive, is intended to govern the data processing operations provided for in the terms at issue. This means identifying the establishment in the context of whose activities those operations are most directly involved."[63]

The Advocate General excluded the Austrian law of the customers whose data were processed: "However, it appears to me at first sight, subject to verification by the referring court, that the operations provided for in clauses 6, 9 and 11 of Amazon EU's general terms and conditions are not directly linked to any after-sales service provided by Amazon EU in Austria."[64]

[62] *See* Opinion of the Advocate General, § 123-124.
[63] *See* Opinion of the Advocate General, § 125.
[64] *See* Opinion of the Advocate General, § 125.

The CJEU followed the point of view of its Advocate General on the principle that only one law is applicable, *i.e.* the law of the establishment where the data processing in question takes place : "It is for the national court to determine, in the light of that case-law and taking account of all the relevant circumstances of the case at issue in the main proceedings, whether Amazon EU carries out the data processing in question in the context of the activities of an establishment situated in a Member State other than Luxembourg".

Here, the CJEU made no reference whatsoever in its *Amazon EU* ruling – which dealt with an intra-EU situation – to the *Google Spain* judgment. In contrast, the CJEU referred twice to the Advocate-General's Opinion in *Amazon EU,* [65] who overtly supported the view that only one data protection law of an EU Member State should apply to cross-border data processing within the EU.

The CJEU case law is firmly established as follows: (i) only one law is applicable to the same data processing activity; and (ii) that law is the one of the establishment which is most closely connected with the processing activity. National courts must establish on the basis of the facts presented to them which establishment has the key data controlling role, by determining the purpose and means of the processing activities. By "means" one should not only look at the technical and organizational issues (e.g. which hardware or software must be used) but also the questions that only the data controller decides upon, such as "which data shall be processed", for how long, who will gain access to this data etc. [66]

D. No Fourth Step in Case of the Existence of a Joint Control

The person or entity in charge of processing data can opt for a system of "joint control."

Although this option already existed under the Directive 95/46, the concept is further elaborated by the GDPR. Article 26 of the GDPR states as follows: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations

[65] *See* CJEU, *Amazon EU*, at paras. 76 and 80.

[66] Of particular note are the comments of the Article 29 Working Party on the initial draft Directive, which specify **four essential criteria** in identifying the controller: purpose, personal data, processing and, key to this case, third-party access to data (Opinion 1/2010 on the concept of controller and processor, at 32).

under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects."

From both the structure and the terms of Article 26, it would appear that "joint control" is a choice exercised by the controller (or by the person controlling the controller). It is a status that cannot be imposed by the SA or by the Court "unless (…), and insofar" there is, as provided for by Article 26.1, specific EU or national legislation in that respect.[67]

Except in the case of specific national legislation on this matter, there shall only be "joint control", if two or more controllers enter into an "arrangement" in the sense of Article 26.2, reflecting "the respective roles and relationships of the joint controllers vis-à-vis the data subjects" and which "essence (…) shall be made available to the data subject".

Even if the person or entities involved opt for joint control, this does not affect the situation of the main data controller, as identified following the three steps as explained above, who remains solely under the supervision of his SA. A joint control only offers an additional possibility to the data subject who "may exercise his or her rights under this Regulation in respect of and against each of the controllers." This structural and textual interpretation is confirmed by the purpose of the GDPR which, as already stressed above, is to adhere to the "one-stop-shop" principle.

II. Conclusion

The main objective of the GDPR is to ensure the free flow of data between Member States, while offering the highest level of protection of personal data of European Citizens, in an ever-growing digital environment. These goals are to be reached by harmonizing data protection rules within the EU borders. On May 25, 2018, the GDPR will become applicable throughout the EU and the Directive will cease to exist. However, the extensive case law on jurisdiction and the applicable law as developed with regard to the Directive will continue to maintain its relevance, as it is based on the same core values that underpin the

[67] "The respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects".

GDPR. In that respect, the same rules on conflict of law will continue to prove valuable and help to prevent avoidance of EU Data Protection Law where its citizens' rights are at stake.