International In-house Counsel Journal
Vol. 6, No. 23, Spring 2013, 1

EU Data Protection Directive: a thorn in the side of the US domestic online retailer

NADJA VAN DER VEER
Deputy General Counsel Global Collect Services B.V., GlobalCollect, The Netherlands

Abstract
Companies outside the European Union are sometimes confronted with having to comply with European legislation around data protection. This is especially the case in the event they make use of a Europe-based service provider. This does not only raise concern for said companies, it also potentially damages the business of European service providers in acquiring new businesses outside the EU. This paper discusses the particular issues arising out of a US based retailer making use of a European payment service provider in particular for the execution of its online payments. The European data protection directive did not anticipate on the effects of its broad interpretation of 'making use of equipment situated in the European Union', which leads to applicability of the law. The principles behind the directive are challenged and a solution is proposed to prevent situations where a non-European based retailer processing payments from non-European consumers via a European PSP has to comply with European data protection requirements.

Keywords: data protection, EU data protection directive, payment service provider.

1. Introduction

Suppose you are a US-based online seller, only selling goods or services to US-based consumers via a local website. For your online payment processing, you have chosen a Europe-based Payment Service Provider.[1] The Payment Service Provider ("PSP")[2] receives payment data from you, including personal data of consumers, in order to properly facilitate the payment process on your behalf and for you to receive the funds and deliver the sold good or service in the US. In short, this type of service provider acts as an intermediary between you and the financial institution where the American consumer holds a bank account or a credit card. You would think that European regulations around data protection do not apply to you as you are not based in Europe, you do not sell to consumers in Europe and therefore do not process consumers' personal data originating from Europe. However, the opposite is true.

The extraterritorial jurisdiction of the European data protection rules stems from the intent of the European legislator to protect data of all individuals wherever located. The broad interpretation of the article (that defines the rule of applicable law in the relevant directive) provides further legal basis for the regulation. This paper discusses the above in

[1] In my experience as Legal Counsel for an international payment service provider, I see many cases where non-EU online retailers (from either Latin America, USA or Asia-Pacific) process online payments via the company while not targeting EU consumers but rather selling to consumers residing in non-EU regions.
[2] Payment service providers are also referred to as Payment Institutes as defined under the EU Payment Services Directive 2007/64/EC.

more detail and examines other principles and rulings which could resolve the issues faced by the online retailer as described herein.

The main focus of this paper will be on US-based companies, although the same applies to online sellers located in other non-European regions (like Latin America and Asia-Pacific) processing via a PSP located in the European Union (EU) without selling their goods or services to European consumers. This type of company will hereinafter be referred to as the "US domestic retailer" and will be used as an example throughout the paper.

2. Applicability to the US domestic retailer

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 of 24 October 1995 (the "EU Directive") distinguishes a controller (one that determines the means and purpose of processing personal data) from a processor (one that processes such personal data on behalf of the controller). Under the EU Directive, the controller carries all liabilities and has to fulfil a number of obligations as provided for in the EU Directive, such as having a legal basis for processing, registering itself at the local authority and taking necessary data security measures. In the situation as described in the first paragraph, in principle and for purposes of this paper, the US domestic retailer would be the controller and the PSP the processor.[3]

The applicability of the EU Directive to non-EU based companies is laid down in consideration 20 and article 4 paragraph 1 sub c ("Article 4(c)")[4] and has a controversial basis for determining applicable law: "*…Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for…*", especially in cases where "equipment"[5] used for data processing is located in a EU Member State. Member State data protection laws apply when *"…the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.*" The currently supported definitions of "making use of equipment" triggers applicability of the EU Directive to the US domestic retailer as further discussed below.

3. Nationality or residence irrelevant: a regulatory overreach?

Apart from the broad definitions, which will be discussed later, certain conceptions upheld by the European legislator and the so-called Article 29 Working Party (an independent advisory body established under the EU Directive) have led to applicability of the EU Directive to the US domestic retailer. Geographical limits have not stopped the European legislator and the Working Party from determining applicability of EU law to a non-EU controller by applying the territoriality principle. Under this principle laws apply of that country where a person is based (or at that time situated) or that country where an act (to which a certain law applies) was conducted. The EU Directive considers that data processing systems must respect the fundamental rights and freedoms of human beings

[3] For the sake of this paper, the assumption is made that the PSP is the processor and not a (joint) controller. In practice, however, it is not that black and white and such determination is dependent upon many factors. This discussion falls outside the scope of this paper.

[4] This paper is limited to the issues around sub c of article 4 paragraph 1 only. No further detailed consideration is given to the rest of the specific article, for instance sub a on "establishment" within the EU to determine applicability of the EU Directive.

[5] In the Member State's national laws of implementation of the EU Directive, the word "means" is commonly used. This is in line with the broad interpretation of the wording.

(more specifically the right to privacy), whatever their nationality or residence. However, despite all what has been said about the extraterritorial effects of the EU Directive on non-Europe-based controllers, the possibility of non-European personal data being processed via an Europe-based PSP was in most cases not comprehended.

The Working Party has explicitly supported the view of the legislator on the irrelevancy of one's nationality or residence. However, the Working Party's statements are not consistent and quite confusing. In one of its working documents[6] for instance, in certain parts specific reference is made to the processing of European personal data (basically supporting the territoriality principle): "*…the Working Party is of the opinion that not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law*" and "*…the Working Party is committed to continue the dialogue with companies…from third countries who collect personal data in the European Union in order to promote adequate data protection standards for the data subjects*". But other phrases in the same document indicate otherwise: "*….it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive……harmonizes Member States laws on fundamental rights granted to all human beings irrespective of their nationality*." This could indicate that the basis of the EU Directive goes beyond the territoriality principle as the last quoted phrases would allow a state to exercise jurisdiction beyond its border. Furthermore, such statements about the irrelevance of nationality and the need for protection for all human beings, let the legislator and the Working Party suggest that other states do not provide sufficient protection for its own civilians.[7]

Under the EU Directive, the European legislator believes it is its responsibility to protect the privacy of both EU and non-EU residing consumers regardless the situation (seller being either European or not). I disagree with this view for the specific case of the US based retailer (in other cases – for instance criminal law related – such an extraterritorial position may be justified). Privacy of consumers is high on every sovereign state's agenda and one should not challenge the internal sovereignty of a state as the ultimate authority lies within its own borders to decide upon protection of its inhabitants (more particular the privacy rights of its citizens in this case). As stated by the UK data protection authority: "*It is hard to see the justification for applying the [EU] Directive to situations where a data controller is not established in any Member State but nevertheless uses equipment in a Member State for processing….If a collection of personal data is controlled and used in a non-EU jurisdiction regulation should be a matter for that jurisdiction regardless of where the data are actually processed.*"[8] The territoriality principle results in applicability of the EU Directive to the US domestic retailer which has not (and most likely could not have) been foreseen at the time of drafting the EU Directive. There should be a reserved approach in applying the territoriality principle as a basis to determine applicable law. In some cases the concept could lose its meaning *"…as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system.*"[9]

---

[6] Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, adopted on 30 May 2002, WP 56.

[7] While this may be an unintended consequence of the statements made, the Working Party specifically states that an individual should not be without protection without specifying whether such individual is European or not.

[8] For more information around states' recent actions around data protection, see also the introduction in the IICJ Article of Noris Ismail, "Data Transfer from the European Economic Area to the Association of Southeast Asian Nations; Strategic Considerations for In-house Counsel". D. Korff, consultant to the European Commission in his EC Study on Implementation of Data Protection Directive, July-September 2002, Annex 3: Report on the findings of the study, page 55.

[9] "Trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", by S.J. Kobrin, November 2002.

4. Connection with the European Union

In its working document of May 2002,[10] the Working Party discussed the rule on applicable law and the processing of personal data by a non-EU controller via the internet. In this document, the Working Party provides several examples of other regulations with extraterritorial effect (such as competition law and consumer protection) to explicitly argue that extraterritorial application may be necessary to protect the rights and interests of EU civilians and that it is justified to apply to data protection. One should bear in mind that all of the provided examples[11] explicitly involve a non-European-based company either providing access to its website to European citizens or doing business within the EU, and therefore rendering the case of the US domestic retailer not directly applicable. There is at least a "community dimension" in the scenarios described; a targeting of individuals residing in the EU. I do not object to extraterritorial effects of a certain law if there is a close connection with the specific country, especially while having the Rome I Convention 1980 in mind, which is supportive of the concept that there should be a close connection with the country in order for a national law to apply.[12] In addition, the close connection requirement of determining applicability of national law is applied by the European Commission and more sovereign states in other cases.[13] Nevertheless, the designation of "equipment" in Article 4(c) effectively means that even a limited (or no) connection with the European Union leads to applicability of the EU Directive. Rather than using a serious or close connection standard as a basis for triggering applicability, the EU Directive focuses on a clear connection, which is broadly defined to cover almost every link, regardless of how irrelevant it may be.

The Working Party has given no consideration to the current applicability of the EU Directive to the US domestic retailer, even where no such connection exists apart from the EU-based "equipment". In my view, the mere use of an EU service provider does not constitute a close connection, but rather a limited one. Taking into consideration the facts of the underlying case as described in the first paragraph, it can even be argued that, despite the use of the EU service provider, there is no connection with the European Union.

Assessing whether the European legislator actually intended, for purposes of application of the EU Directive, to include the activities like those carried out by the US domestic retailer, leads to the following interesting observation: the original draft proposal of the EU Directive actually referred to "the location of the data file" rather than to "equipment". The "location of the data file" standard entails some sort of physical requirement. Nevertheless, changes were made to prevent situations where no protection was provided to data subjects and to avoid possible circumvention of law. According to the leading commentary on the EU Directive, Article 4(c) aims to avoid situations where controllers move corporate seat (while conducting activities in the EU) to circumvent European data protection requirements.[14] The Working Party has also indicated that the objective behind Article 4(c) is to prevent individuals from having no protection solely

[10] Ibid 6.
[11] Ibid 9, p. 3-4.
[12] The private international law principle of closest connection with a country determines applicability of that country's national law in case of conflict of laws. In the Netherlands for instance, see article 8 book 10 Dutch Civil Code (Private International Law) – Close connection of a case with a state.
[13] See for instance the EU Directives on consumer protection (Directive 97/7/EC on distance selling, Directive 93/13 on unfair terms in consumer contracts) and Directive 99/44 on certain aspects of the sale of consumer goods and associated guarantee) and the Australian anti-bribery regulations which could also apply to US based companies.
[14] Dammann and Simitis (n 105), page 129.

because of the fact that the controller is not established within the EU.[15] Nevertheless, in my view, the Working Party has taken a much more far-reaching stand than intended and justified by the commentary aforementioned.

5. Understanding the meaning of equipment

The single noun "equipment", its broad interpretation and the limited exemption (as discussed below) have tremendous consequences for the US domestic retailer who will have to endure significant costs and efforts to ensure compliance with the EU Directive (which are not similar to US data protection regulations that might already apply to it).

As previously stated, by processing via a European PSP, the US domestic retailer falls under the definition of "making use of equipment". The Working Party refers back to the Collins English dictionary to define "equipment": *"...a set of tools or devices assembled for a specific purpose.*" "Making use" only requires (i) some activity, (ii) the intention to process personal data and (iii) the power of disposal - which does not necessarily have to be ownership. For our US domestic retailer, these definitions are not helpful. The PSP clearly offers a set of tools for the specific purpose of processing and the US domestic retailer clearly intends to process personal data and will carry out technical processing via the PSP.[16] While Article 4(c) does provide for an exemption ("…unless these means are only used for the transfer of personal data through the EU"), this carve-out is interpreted very narrowly and only concerns internet service providers, postal service providers and telecommunications carriers that merely transmit, route, switch or cache information. It is debatable as to whether this Article 4(c) was drafted more *"...for a world of physical, inanimate objects rather than for the internet age.*"[17]

If you take a closer look at the core service offered by a PSP, you will see that it offers software (a payment platform) to online sellers. It is this software that currently falls under the scope of "equipment". But is considering the use of third-party software as making use of "equipment" justified? The EU Directive contains no provision concerning use of the internet and no criteria are laid down for deciding whether operations of certain service providers that use the internet, like PSPs, should be deemed to be "equipment" (it just is).[18] If Article 4(c) would be interpreted to include these scenarios, going back to the example, would this not mean that the use of local payment methods of banks situated in the EU also constitutes "making use of equipment"? A PSP has to forward the transaction data (including personal data) to a bank or other type of financial institution for the actual execution of the payment; these parties act as sub-processors. This sub-processing bank could also be regarded as "equipment" and the US domestic retailer would have to comply simultaneously with the law of every EU Member State where such bank is located.[19] This is an impossible burden and the consequences thereof are incomprehensible and probably unintended. In addition, the above discussed meaning of "equipment" results in a scenario where all online sellers doing business with a European

---

[15] The Working Party indicated that an individual "*…should not be without protection as regards processing taking place within his country…*" and companies might "*…locate their establishment outside the EU in order to bypass the application of EU law.*"

[16] Reference is made to the similar conclusion made for EEA data centres by Kuan Han et al in "Data protection jurisdiction and cloud computing – when are cloud users and providers subject to EU Data Protection Law? The cloud of unknowing, part 3", Queen Mary University of London, School of Law, Legal Studies Research Paper No 84/2011, by W. Kuan Hon, J. Hörnle and C. Millard.

[17] "European data protection law – corporate compliance and regulation, 2nd edition, by C. Kuner, p. 123.

[18] As also indicated by the European Court of Justice in the "Bodil Lindqvist" case, Ibid 22, consideration 67, more specifically related to Chapter IV (transfer to third countries) of the EU Directive.

[19] A similar assessment is made by Kuner with regard to the view of the Working Party that cookies constitute "equipment" and would also result in location of the data subject be decisive in determining applicable law. Ibid 14, p. 125.

PSP, regardless of their location and their consumer targeting, will have to adhere to the EU Directive. In the current situation, "*rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced.*"[20] The European Court of Justice already indicated in 2003 that, given the state of the internet when the EU Directive was passed, certain provisions could no longer be assumed to be applicable for "newly developed" situations.[21] As stated by the European Court of Justice in the above referenced case, "*The special regime provided for by Chapter IV of the directive [in this case "by the Article 4(c)"] would thus necessarily become a regime of general application, as regards operations on the internet.*" Software is not the physical object which the legislative history and the explanatory memorandum initially meant with "equipment".

In 2000, the Working Party issued a working document[22] recognizing the issues around electronic commerce on the internet and indicated that it should be analyzed on a case-by-case basis. Despite this, the Working Party stresses that the aforementioned analysis "*…should, however, bear in mind that the provisions of Directive … clearly apply to processing operations carried out using equipment wholly or partly located in the territory of the EU, even when the data controller is located outside the Community.*" The Working Party also confirmed that outsourcing activities (notably by processors) carried out in the EU territory on behalf of a non-European controller may be considered as "equipment."[23] Fortunately, a few years later, the Working Party realized the impact of such a broad interpretation and the undesirable consequences to the US domestic retailer.[24] Nevertheless, it did recommend retaining the wording in some form to prevent avoidance of the EU Directive in cases where there is a relevant infrastructure in the European Union.[25]

I argue that the current concept of "equipment" is outdated and should be further clarified given the current characteristics of the world. Major technological developments and globalization have brought a whole new definition to processing of (personal) data. Compared to 1995, when the EU Directive came into effect, the access to and the use of the internet has increased explosively. Furthermore, the use of non-domestic service providers and cross-border data flows has become more standard. In my opinion, the rule on applicability of law is constructed on the basis of improper and broadly defined wording, too excessive to meet its purpose.

6. Reform of EU data protection: just take it all out!

The European Commission is reconsidering the legal framework of data protection within the EU and, on January 25, 2012, it proposed a reform thereof via a regulation (the "Proposal"). This Proposal is intended to tackle the challenges of globalization and the revolution of technology. It will still take a considerable amount of time before the new regulation will be ready for enactment (just past the first reading phase), and it will take another two years after publication to become applicable (article 91 paragraph 2 of the Proposal). So we still have to endure the current EU Directive for a while. The issues as described herein therefore continue to be of relevance for quite a long time.

---

[20] Ibid 15, p. 125.

[21] Ibid 15, p. 81 and the "Bodil Lindqvist" case C-101/01 (2003) ECR 1-12971. The EU Court of Justice concluded that the data transfer restrictions of article 25 EU Directive were not intended to apply as a general rule to the entire internet without the data controller taking a positive step to actively transfer personal data outside the EU, in this case placing it on a website.

[22] "Privacy on the Internet - An integrated EU Approach to On-line Data Protection", 21 November 2000, p. 71.

[23] Opinion 8/2010 on applicable law, adopted on 16 December 2010, WP 179.

[24] Ibid 14.

[25] Ibid 15 and 18.

It is noteworthy that the European Commission (so far) did not follow the recommendations given by the Working Party related to the issues around the rule of applicable law.[26] Rather than adjusting the definition and interpretation, any reference to "use of equipment" within the EU territory has been removed entirely and the territorial scope has been adjusted in article 3 (which replaces Article 4(c) under the EU Directive). Under the Proposal, EU data protection rules apply in cases where the non-EU controller targets EU individuals via the offering of goods or the monitoring of their behaviour. A more substantive link between the processing of personal data and applicable EU legislation is required, as also proposed by the Working Party (but in another execution form). I support the new proposed wording of article 3 of the Proposal[27] as it reflects a close connection with the EU. It seems that the European legislator also realized that the underlying principle of territoriality was no longer sustainable in the electronically interconnected world we are in and that basis should be found more in the protective principle field.

That having been said, as of this date it remains the case that non-EU-based companies are torn between obtaining regulatory compliance and concerns about the involved costs and efforts needed. Obviously, it is a major source of irritation for the US domestic retailer, provided that it is even aware of the applicability of the EU Directive, which, in most of the cases, it is not. And why should it be? It is not targeting EU consumers, it does not undertake active local advertising and it has no local sales people soliciting for business in the EU. If the company would be aware of the regulatory consequences of entering into a relationship with an Europe-based payment service provider at the very beginning, it might even be possible that it would reconsider and rather obtain the services from a non-European payment service provider. In sum, the EU Directive does not only affect foreign companies, it also has a potentially negative impact on European companies trying to win world-wide businesses and therefore risking the continuous growth of the entire European market.

7. A closer look at US Safe Harbor Principles

For the purpose of US companies receiving personal data from the EU, the Safe Harbor Privacy Principles have been issued by the US Department of Commerce (and accepted by the European Commission). This was done in order to meet the concerns around the EU-required "adequacy standard" on personal data transfers from the EU to a third-country[28] and the aim thereof was to facilitate said transfers from the EU to the US without thereby compromising the protection of the personal data. Said Principles[29] "*…cannot be used as a substitute for national provisions implementing the directive that apply to the processing of personal data in the Member States.*" The Principles do not affect a company's entire data processing operations, but merely apply to data transferred after they have entered the safe harbor (i.e. the US). I question why it should not include entire data processing.[30] The US Trade Information Center's statements above are

[26] Ibid 14. The Working Party proposed development of the criteria of targeting the public and the criteria of equipment/means.

[27] "This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour."

[28] Chapter IV of the EU Directive provides for the following principle to be adhered to: "…transfer to a third country…may take place only if,……, the third country in question ensures an adequate level of protection."

[29] US Trade Information Centre, http://export.gov/safeharbor/eu/eg_main_018475.asp

[30] For the purpose of this paper, the serious criticism on the controversial Safe Harbor Principles will not be considered. The Safe Harbor Agreement is currently in place for a specific purpose and even though detailed reconsideration might be required, the extension of the Principles to the flow into the EU is worth

supported by the Working Party, but contrary to this, on another topic the Working Party has articulated that applicability of the EU Directive relates to a company's whole processing rather than just a part thereof.[31] This would even affect the data processing of a US domestic retailer via a US based PSP! This feels like some form of cherry-picking, where in one case the entire data processing is affected and in another case it is not. I believe that one should take a certain stand in a topic (in this case, with regard to data protection rules applying to entire data processing) and such position should be analogously applied for all other matters related to that topic (so that safeguards provided by US Safe Harbor cover entire data processing from and into the EU). It should be either one way or the other, not a bit of both.

Safe Harbor-certified companies are deemed to provide adequate privacy protection and data flows originating out of the EU to the US can take place.[32] The Safe Harbor Framework attempts to provide protection for personal information deemed adequate by the EU. If this is considered adequate protection and there is no compromising situation whatsoever, why would it not also be sufficient for data flowing into the EU and not have a broader effect to such company's entire data processing?

As for the specific case of the US domestic retailer, I would defend that any voluntarily certification by a US company (processing US personal data via EU based "equipment") under the Safe Harbor Privacy Principles should be considered a proper substitute to waive national provisions of the Member State where the "equipment" is located. If the Principles are considered sufficient for sending data out of the EU, they should also be considered sufficient for processing data in the EU that does not affect EU citizens. Actually, the aim of the Principles is the reassurance of Europeans that their privacy will be protected. I would support a waiver of all obligations the US controller would have under national law (of where the equipment is situated) without necessarily ruling out applicability of such national law. In no way will the objectives of the EU Directive be detrimentally affected by the aforementioned waiver and European privacy will remain protected. Such waiver would be in line with the decision of the French data protection authority as discussed below (for non-EEA companies using French service providers). Whether from a practical point of view this would be feasible and whether the US domestic retailer is willing to adhere to these Principles is a different topic, but it would help them in obtaining regulatory compliance with the EU Directive.

8. Provisional solution

The French data protection authority (CNIL) did – in a way – already contemplate a manner to address the concerns. Even though under strict conditions,[33] the CNIL has indicated that the EU Directive is too burdensome for non-EEA persons using French service providers. CNIL has allowed certain waivers from local data protection formalities for processing by French service providers for non-EU controllers of certain types of personal data (payroll, customers and prospects data) for limited purposes.[34] The French have acknowledged that the formalities to be followed for non-EU companies are too onerous. However, unlike what is being contemplated in this paper, the CNIL does not entirely rule out French law from becoming applicable, but alternatively provides

considering. Any changes thereto or replacing schemes could cover the entire data processing likewise as proposed herein.

[31] Ibid 14.

[32] Ibid 17 (n 105), p. 14.

[33] A PSP will not meet the conditions set by the CNIL as no reference is made to consumer data only, the limited purpose does not apply and there may not be any other data recipients (a PSP has to forward the data to a bank for clearing and settlement).

[34] Ibid 14 and CNIL decision "Délibération n° 2011-023 du 20 janvier 2011".

exemptions to certain formalities that normally should be followed. I believe this has been a good way forward, but does not entirely solve the issues faced by the US domestic retailer.

The above proposed expansion of applicability of the Safe Harbor principles might help US based companies, but not all non-European based retailers. Also, the US domestic retailer would rather want no applicability of law then applicability but with waivers. While waiting for the new Proposal to take effect, as an interim solution, a lot can be achieved in terms of better interpretation of current arrangements under the EU Directive.

A solution that can be implemented in the short-term is to limit the long reach of the term "equipment" by altering its current interpretation. This view is supported by applying the findings of the European Court of Justice (ECJ) in the Bodil Lindqvist case (elaborated above). This is also supported by Christopher Kuner,[35] although he did not (yet) consider the specific case of the US domestic retailer. These ECJ findings support the argument that the rules of Article 4(c) should not be applied to activities that could result in EU data protection law being extended indiscriminately to the entire Internet, unless the non-EU data controller has taken some positive steps to target EU individuals. In the particular case of the US domestic retailer, as already set out, the EU data protection law is broadened to all non-EU controllers using a PSP. The entire client portfolio of the PSP would have to adhere to the EU data protection rules, without any exception.

The activities as referenced by the ECJ would be - in the described case of the US domestic retailer - the making use of software. These activities should in principle not result in concluding that the EU Directive applies. The rule of Article 4(c) would then only be applied in the event that the non-EU controller takes positive steps to target persons residing in the EU (quoting the ECJ), which is in support of the protective principle and fully in line with the anticipated reform of the data protection framework (the Proposal). As a consequence, the original goals of Article 4(c) of the EU Directive would be restored, namely to prevent controllers from willingly evading application of EU law by relocating in a non-EU country, and ensuring that data subjects in the EU are not left without protection.[36]

Analogously applying the ECJ Bodil Lindqvist findings would effectively mean that the use of software situated in the EU – in this case a PSP – would not trigger applicability of the EU Directive as it is not considered to categorize as "making use of equipment", save the cases where EU consumer targeting takes place. The US domestic retailer would be relieved from having to comply with the European data protection requirements and could freely choose to work with European based service providers without regulatory implications. This would also help other service providers, for instance Europe-based SaaS companies providing cloud computing services.

***

Nadja van der Veer is Deputy General Counsel at GlobalCollect. She has been working for the company for almost six years, right after having obtained her law degree at the University of Amsterdam and having studied a semester at the American University of Cairo. She has grown together with the company and now fulfills the role of deputy and acts as sounding board of the General Counsel and the Board. Next to day-to-day operational activities, her focus in this role goes out to reviewing of and advising on (inter)national legislation to a worldwide service provider like GlobalCollect and drafting

[35] Ibid 15, p. 124. He discussed the undesirable application of the EU Directive due to access by EU citizens of foreign websites using cookies being regarded by the Working Party as "making use of equipment situated on EU territory".

[36] Ibid 15, p. 126.

business policies to allow the company to take decisions in line with applicable laws, such as AML, Sanctions and Anti-Bribery. Next to that, Nadja is closely involved in (i) several business expansion initiatives to advise upon regulatory and other legal impacts and (ii) process reviews to advise upon, determine and implement improvements into the legal department and throughout the company.

GlobalCollect is the world's premier Payment Service Provider of local e-payment solutions for international Customer Not-Present (CNP) channels such as internet, mail and telephone orders, and specializes in a wide range of industries such as travel, ticketing, telecommunications, retail, publishing, portals, online gaming, and digital content. While most providers limit their services to a technical link with payment acquirers, GlobalCollect is a full service partner consulting clients on how to increase transaction volumes, expand distribution channels, and reduce costs by streamlining back office processes. Through a single-interface online payment platform, we offer access to an unrivalled portfolio of local and international payment methods in over 170 countries and 170 currencies, including all major credit and debit cards, direct debits, bank transfers, real-time bank transfers, eWallets, cash at outlets, prepaid methods, checks, and invoices. For more information please visit: www.globalcollect.com.