Data Protection and Conflict-of-laws: A Challenging Relationship

*Maja Brkan**

The present article aims to address issues of applicable law in data protection litigation, dealing notably with the questions of possibility of agreements on applicable law, the questions of applicable law if the controller is situated within the EU and the questions of extraterritorial application of EU data protection law if the controller is established outside of the EU. In particular with regard to the issue of agreements on applicable data protection law, where general rules on applicable law with regard to contracts or torts are different than in data protection law, the issue will be addressed whether the provisions of general EU regulations on applicable law bear any significance for the field of data protection.

I. Introduction[1]

In data privacy litigation – as in any other litigation – the question which law applies to the dispute is one of the first questions requiring clarification in legal proceedings. The question of applicable law in the framework of data protection disputes has attracted quite some attention of the academic doctrine.[2] This doctrine mainly explores a very relevant, although rather technical, question of applicability of a law of a certain Member State to particular data protection dispute, as determined on the basis of Article 4(1) of the 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 (Data Protection Directive).[3] While this paper indeed seeks to contribute to this debate, it also argues that it is important to place this issue within a broader context of a relationship between the general EU conflict-of-law rules and the rules on data protection. Such juxtaposition of specific data protection rules on applicable law and more general conflict-of-law rules is important, on the one hand, from a more theoretical and systematic perspective of hierarchy of norms and relationship between them. On the other hand, clarifications in this regard are necessary also from a practical perspective, with a view of giving concrete answers to data controllers and data subjects on applicable law. Finally, it should be pointed out that the future General Data Protection Regulation (GDPR)[4] clarifies, to a certain extent, the issues of applicable law and that an analysis in the present paper would not be complete without going deeper into the questions raised by the new Regulation.

In light of the above, the purpose of this paper is threefold. First, in *Section II*, the paper aims to contribute to the existing debate by addressing the challenges connected to the determination of applicable law according to the current legislation (Data Protection Directive). Issues such as structure, legal nature and interpretative problems of Article 4(1) of this directive are analysed and the recent case law of the Court of Justice of the EU (CJEU) in this regard is dis-

* Maja Brkan, Assistant Professor, Faculty of Law, Maastricht University. For correspondence: <maja.brkan@maastrichtuniversity.nl >. The author would like to thank Hielke Hijmans, Joasia Luzak, Jorg Sladič and Dan Svantesson for helpful discussions/comments on this topic and two anonymous reviewers for their comments on an earlier draft of this paper. The usual disclaimer applies.

1 This article draws upon the paper Maja Brkan, 'The Relevance of European Data Protection Standards for US Businesses and Authorities' (6th International Conference on Society and Information Technologies: ICSIT 2015, Orlando, Florida, USA, 10-13 March 2015) published in the Conference Proceedings, 63-68.

2 See, for example, Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 International Data Privacy Law 28-46; Christopher Kuner, *European Data Protection Law* (OUP 2007), 114.

3 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.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) [2016] OJ L 119/1.

cussed. The purpose of this section is to provide with an explanation of data protection rules on applicable law currently in force and to point to some queries that have remained unclear in CJEU case law on these issues.

The core of the paper – *Section III* – seeks to clarify the relationship between general conflict-of-law rules and more specific data protection rules when it comes to the determination of applicable law. In particular with regard to the issue of agreements on applicable data protection law, where general rules on applicable law with regard to contracts or torts are different than in data protection law, it is of utmost importance to research the question whether the provisions of general EU rules on applicable law bear any significance for the field of data protection. For example, for the German users or Facebook, the Facebook's Terms of Service stipulate that the German law applies.[5] If you rent a car online with Europcar, the applicable law will be French law, submitting all privacy-related claims to this law, given that the Terms and Conditions do not distinguish between privacy claims and other disputes.[6] As data subjects and consumers, we are often submitted to a certain set of rules to which we, indeed, consent by agreeing with general terms and conditions, mostly because there is no *real* choice of law available which would give the data subject/consumer a say in determining the applicable law. However, are such agreements valid or should applicable law be determined pursuant to specialised data protection rules?

Furthermore, the paper aims, in *Section IV,* to discuss rules on applicable law in GDPR that will enter into force in 2018. This Regulation indeed unifies the law that should be applicable in all Member States and thus *prima facie* does not pose conflict-of-laws questions. However, Member States' laws can still diverge from this unified law when expressly allowed by the Regulation, and can therefore raise more general issues of conflict-of-laws. On the basis of which legislation should such conflicts be solved? For example, if a Member State imposes further limits on processing of health data as allowed by the GDPR[7], how should it the applicable law be determined? Can general conflict-of-law rules be relevant in this respect? To illustrate with another example: suppose that the general terms and conditions of a Chinese company selling its products online to its European customers determines Chinese law as applicable law – can the European data subjects still invoke the protection from GDPR?

Finally, concluding remarks in *Section V* seek to clarify the current and future rules on data protection in that a suggestion for an amendment of both Data Protection Directive and GDPR is put forward. Such amended rules aim at elucidating the relationship between data protection rules and general conflict-of-law rules and bring clarity notably with regard to agreements on applicable law as well as issues for which the GDPR allows for divergent provisions between Member States.

II. *De lege lata*: Applicable Law in Data Protection Directive

1. The Hurdles and Function of Article 4(1) of Data Protection Directive

Article 4(1) of the Data Protection Directive, which regulates questions of applicable law, is a complex provision raising many interpretative issues. In the light of quickly developing information technologies – and evidently the fact that the Directive was drafted in 1995 – this provision consequently occasionally does not clearly match the demands of today's information society. According to Article 4(1) of the Data Protection Directive, the law of a particular Member State transposing this directive applies if the controller is established in this Member State and data is processed in the context of its activities [subparagraph (a)].[8] If the controller does not have an establishment within the EU, the law of a particular Member State transposing the Data Protection Directive can apply either on the basis of public international law [subparagraph (b)] or if the controller makes use of equipment situated on the territory of this particular Member State [subparagraph (c)].

From the viewpoint of systematics of this provision, is apparent from its text that the first step in

5 The German Terms of Service which provide that, for German users, German law applies; see <https://www.facebook.com/terms/provisions/german/index.php> accessed 8 September 2016.

6 See art X of the Online Booking Terms and Conditions of Europcar, available at <https://www.europcar.com/terms-and-conditions/online-booking> accessed 8 September 2016.

7 See art 9(4) of the GDPR.

8 According to this same article, if the controller is established in several Member States, each of the establishments of this controller has to comply with the obligations laid down by the national law applicable.

determination of applicable law is to determine whether data controller is *established* within the EU or not. It is submitted that in an online environment and in time where data (mostly) freely crosses borders, the answer to this question might not always be entirely clear, even though the CJEU already had an opportunity to pronounce itself on this issue.[9] If the controller is established within the EU, Article 4(1)(a) – which seems to be formulated very broadly – will be used to determine the law of which Member State will be applicable to the case. Given its broad formulation, this paragraph quite evidently raises some interpretative issues. For example, even though the notion of 'establishment' has been, to a certain extent, clarified in the case law,[10] it still remains unclear how broad the 'context' of activities of a controller should be interpreted. The degree of involvement of the establishment and the nature of its activities are factors that should be taken into account in this regard.[11] In view of its broad nature, paragraph (1)(a) will be the pertinent provision to determine applicable law in most of disputes relating to data protection. The goal of such a broad formulation is to prevent avoidance, by data controllers, to be submitted to EU data protection rules by transferring data processing to third countries.[12]

If the data controller is *not* established within the EU, either paragraph 1(b) or 1(c) will be relevant. Paragraph 1(b) is, contrary to its counterpart 1(a), not very often used in practice. It is relevant in rare cases, such as for example for embassies of EU Member States in third countries which normally use data protection laws from their domestic Member States.[13] This is a case where data protection law of a particular Member State applies on the basis of public international law.

With regard to paragraph 1(c), the criterion of making use of 'equipment' seems particularly confusing, since it is not clear how broad the notion of 'equipment' should be interpreted. Does in entail (only) hardware or (also) software? Is it the equipment aimed at processing of data or can other equipment also be relevant? To solve this conundrum, it should be referred to other language versions of the Directive that use a more neutral term 'means' (*moyen, Mittel, strumenti*). From the perspective of textual interpretation, Article 29 Working Party[14] understands 'equipment' as 'means' which is indeed a broader concept that would normally encompass both hardware and software. Looking at the article through teleological interpretation, it should logically encompass 'means' used for or relating to processing of personal data, such as geo-location services and cloud computing,[15] and not just any means lacking this purpose.

It stems from the above that Article 4 of Data Protection Directive seems to have a double function. On the one hand, this article determines when the law of one of the Member States will be applicable *as opposed to the law of a third country.* On the other hand, this article determines *the law of which Member State* will be applicable within the European Union. The article as a whole can therefore be considered as a conflict-of-law rule.[16]

a. The CJEU's Approach Towards Questions of Applicable Law

The CJEU had the opportunity to decide on matters relating to applicable law only in a handful of cases. A landmark case in this regard is the *Google Spain and Google* case[17], in which the CJEU interpreted, for the first time, Article 4(1)(a) of the Data Protection Directive. As already mentioned, this provision requires the application of national law of a certain Member State transposing the directive if 'the pro-

9 Case C-131/12 *Google Spain and Google* (CJEU, 13 May 2014) ECLI:EU:C:2014:317. For a comprehensive analysis of the case, see Herke Kranenborg, 'Google and the Right to Be Forgotten' (2015) 1 EDPL 70.

10 ibid.

11 See Article 29 Working Party (A29 WP), 'Opinion 8/2010 on applicable law' (16 December 2010) 836-02/10/EN WP 179, 14.

12 Kuner, *European Data Protection Law* (n 2) 111.

13 See A29 WP, Opinion 8/2010 on applicable law (n 11) 18.

14 ibid 21.

15 ibid.

16 ibid 9; Kuner, *European Data Protection Law* (n 2) 112.

17 *Google Spain and Google* (n 9). The majority of academic literature comments upon this case from the perspective of the right to be forgotten and puts the issues of applicable law less in the forefront; see for example Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761–777; Hannah Crowther, 'Google v Spain: is there now a 'right to be forgotten'?' (2014) 11 Journal of Intellectual Property Law & Practice 892-893; Joseph Jones, 'Control-alter-delete: the 'right to be forgotten'' (2014) European Intellectual Property Review 595-601; Merav Griguer, 'Conditions et modalités d'exercice du droit à l'oubli numérique - ou les apports de l'arrêt CJUE, 13 mai 2014, C-131/12' (2014) 24 La Semaine Juridique Entreprise et Affaires 1326; Guillaume Busseuil, 'Arrêt Google: du droit à l'oubli de la neutralité du moteur de recherché' (2014) 24 La Semaine Juridique - entreprise et affaires 51-54.

cessing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'. The CJEU, asked to interpret several notions from this article – notably the notion of 'establishment' and the question when such an establishment 'processes' personal data 'in the context' of its activities – came to the conclusion that the conditions of this article are fulfilled "when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State"[18]. Whereas this decision, following the opinion of Advocate General Jääskinen[19], might well be appropriate for the factual constellation specific for the *Google Spain and Google* case, it is doubtful whether, from a more general perspective, it can be the only plausible and the most appropriate interpretation of this provision.

It is submitted that is not entirely convincing that the application of data protection legislation should be dependent on the business model that the search engine uses to generate its revenues.[20] It is questionable whether selling of advertising space is a criterion that should be taken into account at all, given the fact that the main (and only) criterion that the Data Protection Directive builds upon is the processing of personal data. It is true, however, that both activities form part of the same business model and that it is precisely the selling of advertising space that financially enables the activity of processing of personal data.

What is however left unanswered is the question whether such an interpretation of Article 4(1)(a) of Data Protection Directive would allow for this provision to include also search engines that are built upon different, non-profit, business models[21]. It seems that such search engines, that process personal data, would equally need to be covered by this provision. Such a solution does, however, not stem readily from the reasoning of the CJEU that affirms that the activities of Google in California (operator of the search engine) and of its subsidiary in Spain (selling advertising space) are 'inextricably linked' in the sense that the latter activity renders the 'search engine at issue economically profitable' and that it is therefore 'the means enabling those activities to be performed'[22]. In the case of the absence of this link, would the conditions from Article 4(1)(a) still be fulfilled? It seems that this would not be the case and that such a situation could potentially be covered by subparagraph (c) of the same article, requiring that the controller 'makes use of equipment' on the territory of a particular Member State.

Therefore, it is not entirely clear from the *Google Spain and Google* judgment whether processing of personal data by an operator selling advertising space is the *only* possibility covered by this article or whether this is only *one of* examples that can be covered by this provision. The problem with former interpretation lies in the circumstance that it depends to a too high degree on a business model on which the search engine is built upon. In fact, such an interpretation only covers certain business models – more precisely, it encompasses only those search engines that use the sale of advertising space to finance its search activities.

Furthermore, it is important to stress that the solution adopted by the CJEU comes curiously close to the one regarding the interpretation of Article 17 of Regulation 1215/2012[23] (before Article 15 of Regulation 44/2001[24]) in the joint cases *Pammer and Hotel Alpenhof*[25] and the subsequent case-law, *Mühlleitner*[26] and *Emrek*.[27] The CJEU namely adds as one of the conditions of the application of Article 4(1)(a) of Data Protection Directive the circumstance that the subsidiary of the search engine 'orientates' its activity towards the inhabitants of the Member State in

18 *Google Spain and Google* (n 9) para 60.

19 Case C-131/12 *Google Spain and Google* ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para 68.

20 In more general terms, John W Kropf, 'Google Spain SL v. Agencia Española de Protección de Datos (AEPD)' (2014) 108 The American Journal of International Law 507, wonders whether 'other search engines with fewer ties to the European Union be able to determine with any certainty that they are subject to application of the Directive'.

21 As an example of non-profit search engine is Benelab (*http://bene.co/* accessed 2 February 2015) that donates revenues generated from the Internet searches.

22 *Google Spain and Google* (n 9) para 56.

23 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L 351/1.

24 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L 12/1.

25 Case C-585/08 *Pammer and Hotel Alpenhof* (CJEU, 7 December 2010) ECLI:EU:C:2010:740.

26 Case C-190/11 *Mühlleitner* (CJEU, 6 September 2012) ECLI:EU:C:2012:542.

27 Case C-218/12 *Emrek* (CJEU, 17 October 2013) ECLI:EU:C:2013:494.

which it is established. It is true that the Working Party 29 considered the 'targeting' of individuals in the EU as a potential additional criterion when the controller does not have an establishment in the EU in order to provide for a sufficient link with EU territory.[28] However, adding this criterion through an interpretation of Article 4(1)(a) of Data Protection Directive without a legislative revision of this provision seems problematic.[29] Not only because this criterion does not appear in the text of the article itself and hence cannot be established on the basis of a textual interpretation of this article, but also because this criterion does not seem to stem either from a teleological interpretation of this provision or from the usual meaning from the term 'orientating'.

It seems that this element, in a way, neutralises the circumstance that the controller has a subsidiary in a certain Member State. While it is certainly possible to imagine circumstances in which a controller would have a subsidiary in a given Member State and *not* orientate its activity towards the inhabitants of this Member State, it seems that such examples would be rather rare in practice. It should be recalled that the criterion of 'orientating' of an activity makes most sense if there is a cross-border element to such 'orientating'.[30] A cross-border element is also present in the notion of 'directing of activities' as used by Article 17 of Regulation 1215/2012. In any event, it would seem reasonable that this criterion is used as a subsidiary criterion and not as a primary one in the framework of the interpretation of Article 4(1)(a) of the Data Protection Directive. That is confirmed also in the recent case *Verein für Konsumenteninformation*,[31] where it is shown that the criterion of processing data in the context of the activities of an establishment is the core criterion for determination of applicable law.

It is true, however, that the decision of the CJEU in *Google Spain* can also be understood in the light of the preliminary questions asked by the national court. In fact, the answer given by the CJEU in paragraph 45 of the judgment to the question regarding applicable law is a mirror image of one of the three possible interpretations put forward by the national court. It could therefore be claimed that the CJEU only affirmatively replied to a premise already given to it by the national court. The question was not asked in abstract, but with regard to a concrete situation and on the basis of the concrete description of a situation given by the national court.

Another question that needs to be addressed is whether the interpretation given by the CJEU would be the same if a company from a third country has a subsidiary in one or several EU Member States that process personal data within the EU. In the German case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*,[32] the German administrative court of Schleswig-Holstein held that German law was not applicable to processing of data of its German users because the German subsidiary of Facebook did not actually process the data, but was only active in the field of marketing[33]. Since it was the Irish subsidiary of Facebook that processed personal data of its European users, it was the Irish law that was exclusively applicable.[34] The case was appealed by Facebook to the German Federal administrative court (*Bundesverwaltungsgericht*) and this court made a reference for a preliminary ruling to the CJEU.[35]

It can be argued that a decision allowing only for applicability of the law of the country where data is actually processed is not in accordance with the CJEU decision in *Google Spain and Google* and that the circumstance that the German subsidiary of Facebook exercises marketing activity should be sufficient for German law to be applicable.[36] Such rea-

28 See A29 WP, Opinion 8/2010 on applicable law (n 11) 31.

29 Moerel (n 2) 44, for example, proposes a legislative revision of art 4(1)(a) and (c) of Data Protection Directive that could provide that the national laws apply 'to the processing of personal data in the context of the activities of the controller on or directed at the territory of the Member State'.

30 In the sense that an internet service provider, established in one Member State, orientates its activity towards the inhabitants of *another* Member State. It is true, however, that a cross-border element can also be established if a controller established in a third country orientates (through its subsidiary) its activity towards the EU.

31 Case C-191/15 *Verein für Konsumenteninformation* (CJEU, 28 July 2016) ECLI:EU:C:2016:612.

32 Case 8 B 60/12 *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany*.

33 ibid 6.

34 ibid 7 and 9.

35 See case BVerwG 1 C 28.14, communication for the press 'EuGH soll datenschutzrechtliche Verantwortlichkeit für die beim Aufruf einer Facebook-Fanpage erhobenen Nutzerdaten klären' (25 February 2016) <http://www.bverwg.de/presse/pressemitteilungen/pressemitteilung.php?jahr=2016&nr=11> accessed 5 April 2016.

36 It is to be noted that the German case law itself is not consistent regarding this issue. Apart from the cases that deny the applicability of German law, there are also cases that confirm this application or even those that leave the issue opened; see Heinrich Amadeus Wolff and Stefan Brink, Beck'scher Online-Kommentar Datenschutzrecht, 15. Edition (Beck 2016), para 31.

soning, however, seems to entirely disregard different functions of the two European subsidiaries of Facebook: the German one to perform marketing and the Irish one to perform processing. In *Google Spain* case, there was no EU subsidiary that would process personal data and the CJEU, wanting to apply EU law to Google, allowed for such an applicability through the link with Google's Spanish subsidiary.

Therefore, it is submitted that the criteria for determining applicable law should differ depending on whether a company from a third country has a subsidiary in the EU that processes personal data of its EU users or not. It can be argued that, for such a company, it would be enough to have a marketing subsidiary in one of the EU Member States for the law of this Member State to apply, whereas, in case of an existence of another EU subsidiary processing personal data, this would not suffice. However, it could further be reasoned that an EU subsidiary that processes personal data is actually an *establishment* within the meaning of Article 4(1)(a) of the Data Protection Directive and that, therefore, the law of this Member State should be applicable to this establishment.[37] The CJEU's decision will clarify these queries.

Some other cases in the CJEU jurisprudence are relevant for the determination of applicable law in data protection matters. In the case *Weltimmo*, the CJEU had to decide whether Hungarian or Slovakian law was applicable to a real estate agent who had a registered business in Slovakia, but aimed at selling, through advertisement on a website in Hungarian language, properties situated in Hungary.[38] The CJEU decided that Hungarian law could be applied to the case,[39] provided that the agent (the controller) "exercises, through stable arrangements in the territory of that Member State, a real and effective activity ... in the context of which that processing is carried out".[40] It is very interesting to observe how the CJEU approached the interpretation of the notion of 'establishment' from Article 4(1)(a) of the Data Protection Directive. The Court specifically noted that the 'establishment' within the meaning of this article could mean that a company is established in a different Member State then the one in which it is registered which is particularly important for companies doing business over Internet.[41] This means that the definition of this concept is factual-based rather than basing itself on a formal legal approach. In practice, it can also mean that a company can be 'established' within the meaning of Data Protection Directive, in different Member States.

Finally, the case *Rease and Wullems* on the interpretation of the notion of 'making use of equipment' in Article 4(1)(c) of Data Protection Directive[42] was radiated because the referring court, Dutch Council of State, unfortunately withdrew the reference for preliminary ruling.[43]

III. Data Protection Directive v Rome I and II Regulations: A Relationship of Tension?

1. Conceptualising the Problem

Aside from the analysis above, showing that Article 4(1) of the Data Protection Directive in itself opens the possibility of different and ambiguous interpretations, it is equally necessary to take a closer look on the relationship between this provision and the general conflict-of-law rules. The doctrine dealing with issues of applicable law in the framework of EU data protection provides for a thorough analysis of Article 4 of Data Protection Directive, without first addressing the issue of the relationship between the general EU conflict-of-law rules and the Data Protection Directive.[44] The EU conflict-of-law regulations that are relevant for the present analysis are the Regulation on the law applicable to contractual obligations (Rome I Regulation)[45] and the Regulation on

37 Such reasoning could also be supported by the Recital 18 of the Data Protection Directive, according to which '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'.

38 Case C-230/14 *Weltimmo* (CJEU, 1 October 2015) ECLI:EU:C:2015:639, paras 9-13.

39 ibid para 39.

40 ibid para 41.

41 ibid para 29.

42 See Application in case C-192/15 *Rease and Wullems*, [2015] OJ C 236/26.

43 See Order in case C-192/15 *Rease and Wullems*, ECLI:EU:C:2015:861, [2016] OJ C 78/11.

44 See, for example, Kuner, *European Data Protection Law* (n 2) 111-112. Rome I and II Regulations are also not mentioned in A29 WP, Opinion 8/2010 on applicable law (n 11).

45 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L 177/6.

the law applicable to non-contractual obligations[46] (Rome II Regulation).[47] While Rome I Regulation remains neutral as to the applicable law in data protection matters, the Rome II Regulation clearly stipulates that it does not apply to 'non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation'.[48]

When assessing potential conflicts between Article 4(1) of Data Protection Directive and the general conflict-of-law rules, it should not be of importance which sub-paragraph of this provision is at stake. In other words, the question of which set of rules apply should not be dependent on the question which paragraph of Article 4 could potentially be relevant for the case. It is a conflict between two sets of rules that calls for a determination which set prevails.

A few examples can clarify open questions relating to relationship between these two types of legal sources. Imagine, for example, a distribution contract between a company producing soft drinks in Poland and a distributor established in Luxembourg. The Luxembourgish distributor is collecting data about its buyers and transferring it to Poland where this data is processed (classified, processed in view of targeted advertising, profiling etc). Under the general conflict-of-law rules (Rome I Regulation) the distribution contract would be governed by Luxembourgish law.[49] However, under Article 4(1)(a) of the Data Protection Directive, data protection issues included in such a contract should be assessed under Polish legislation because the processing takes place in Poland. Which law would be eventually of relevance for data protection breaches by this company?

To provide another example: an online EU-wide agent for immovable property, established in Finland, sells houses throughout the EU, including the Netherlands. According to the general rules on applicable law for this contract, if a house is situated in the Netherlands, the Dutch law would apply to the contract for sale.[50] However, the data protection rules would point to the use of Finnish data protection law on the basis of Article 4(1)(a) of Data Protection Directive. Can data protection breaches be assessed on the basis of different rules as other contractual breaches?

a. Theoretical Analysis

It is submitted that the analysis of the rules of both Rome Regulations as well as the relevant provisions of the Data Protection Directive allow for two potential conclusions with regard to the relationship between the two sets of legal documents.

b. Separate Scopes of Application

The first possibility is to argue that Article 4(1) of the Data Protection Directive lies entirely outside the scope of application of both Rome I and II Regulations, thus leaving no possibility of overlap between their respective scopes of application or integration of the former provision into the system of the two regulations. In this regard, it is to be noted that both the Rome I and II Regulations expressly stipulate that they do not apply to 'administrative matters', but only to 'civil and commercial matters'.[51] Data protection is, however, rather difficult to conceptualise, since it falls into 'the grey area between public and private'.[52] Nevertheless, it could be argued that this field falls both under 'administrative matters' given that regulatory remedies such as administrative fines can be imposed for breaches, as well as under 'civil matters' insofar as data subjects might bring claims for contractual and tortious breaches. Therefore, only the civil data protection claims will raise issues of potential overlap with traditional conflict-of-law rules. Within this framework, the core of the analysis of applicability of both Rome regula-

46 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199/40.

47 This article does however not take into account Rome III Regulation (See Council Regulation (EU) No 1259/2010 of 20 December 2010 implementing enhanced cooperation in the area of the law applicable to divorce and legal separation [2010] OJ L 343/10) and Rome IV Regulation (Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L 201/107) as the matters that they regulate – divorce and succession – seem somewhat less relevant for the field of data protection.

48 See art 1(2)(g) of Rome II Regulation.

49 See art 4(1)(f) of Rome I Regulation.

50 See art 4(1)(c) of Rome I Regulation.

51 See art 1 of both Rome I and II Regulations.

52 Jan-Jaap Kuipers, 'Bridging the Gap. The Impact of the EU on the Law Applicable to Contractual Obligations' (2012) 76 RabelsZ 573. See also Lee Bygrave, 'Determining applicable law pursuant to European Data Protection Legislation' (2000) 16 Computer Law and Security Report 252; Christopher Kuner, 'Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)' (2010) 18 International Journal of Law and Information Technology 178.

tions to the field of data protection will therefore be the question whether those civil claims in data protection can fall under the notion of 'civil matters' within the meaning of the two regulations – an issue that will have to be determined on a case by case basis. Therefore, from the perspective of this argument, there is no clear principled answer as to whether Rome I and II Regulations apply to data protection matters.

In addition, Rome II Regulation expressly excludes from its scope 'non-contractual obligations arising out of violations of privacy'.[53] In this regard, it is equally not evident whether, for the purposes of Rome II Regulation, violations of privacy include also violations of data protection, notably due to the fact that neither the textual nor historical[54] interpretation of this provision seem to include data protection issues in its scope. The issue of whether data protection and privacy are two separate rights or whether data protection forms part of privacy is *per se* a rather contested issue.[55] On the one hand, the Charter's distinct provisions for data protection (Article 8) and privacy (Article 7) demonstrate that those two rights need to be seen as having a separate scope of application. The CJEU in its recent case-law vindicates this approach by using both fundamental rights in the analysis.[56] As argued in the doctrine, privacy has to be distinguished from data protection at least to a certain extent.[57] While these two rights might indeed partially overlap, privacy seems to be a broader concept that encompasses also other issues than just personal data, and not all personal data necessarily fall into the sphere of privacy.[58] On the other hand, it can also be argued that the two rights are so intertwined that it is close to impossible to separate them. This approach would also be consistent with the approach taken in the Data Protection Directive which itself uses the term the 'right to privacy with respect to the processing of personal data'.[59] Moreover, the CJEU, which repeatedly used this term in its case-law,[60] very often considers both rights together.[61] Such an approach of the CJEU, referring both to the right to privacy and the right to protection of personal data[62], is an indication that the two rights are inextricably intertwined.

Amid different understandings of the relation between two fundamental rights, the fundamental question for the purposes of this paper is which of the two viewpoints should be relied upon for the purposes of interpretation of Rome II Regulation. Even though the author believes that, for fundamental rights purposes, the two rights should be distinguished (at least to the extent that this is possible), from the perspective of teleological and systemic interpretation of Rome II Regulation, it seems more sensible to adopt the latter approach.[63] If privacy was excluded from the Regulation's scope of application and data protection was not, this would cause enormous difficulties in determination of applicable law for tortious privacy/data protection breaches. For example, if a provider of a health app disclosed data subject's health data and his/her opinions about

53 See art 1(g) of Rome II Regulation.

54 During the legislative process, the European parliament modified the wording of this provision to include violations 'resulting from the handling of personal data', but this modification was not retained in the final version of the Regulation. See, in this regard, Andrew Dickinson, *The Rome II Regulation: The Law Applicable to Non-Contractual Obligations* (OUP 2008), 240.

55 Compare Orla Lynskey, 'Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 574; Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 266.

56 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and Others* (CJEU, 8 April 2014) ECLI:EU:C:2014:238, para 32 et seq.

57 See in this sense Maria Tzanou, 'Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures' (2013) 17 Journal of Internet Law, 26 et seq, 569-597, 569-597 who stresses, at p 597, that it "is time to recognize the merits of a truly independent right to data protection". See also Juliane Kokott and Christoph Sobotta, 'The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', in Hielke Hijmans and Herke Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust?* (Intersentia 2014), 83-95; Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', *Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013 https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/SpeechArticle/SA2014* accessed 1 May 2015.

58 Tzanou (n 57) 26.

59 See art 1(1) of the Data Protection Directive.

60 For a recent case in this regard, see, for example Joined Cases C-141/12 and C-372/12 *YS and Others* (CJEU, 17 July 2014) ECLI:EU:C:2014:2081.

61 See for example Case C-293/12 *Digital Rights Ireland and Seitlinger and Others* (n 56) where the CJEU, in paras 32 et seq, addressed the interference with both arts 7 and 8 of the Charter. See also Case C-92/09 *Volker und Markus Schecke and Eifert* para 47, where the CJEU affirms that the right to the protection of personal data from art 8 of the Charter 'is closely connected with the right to respect of private life expressed in Article 7 of the Charter'.

62 See *Google Spain and Google* (n 9) paras 38, 80.

63 Compare Dickinson (n 54) 240.

his/her health state, it would be rather arduous to draw the line between the claim relating to privacy (for which Rome II would not apply) and data protection (for which Rome II would apply).

Such reasoning thus leads to the conclusion that not only the issues of privacy, but also the issues relating to data protection should be excluded from the scope of application of the Rome II Regulation.[64] Moreover, a study on applicable law in privacy and data protection matters confirms this view by pointing out that the conflict-of-law rule in Data Protection Directive does not follow the general rule for applicable law in non-contractual responsibility, which is the place where the harmful event was committed.[65] In consequence, this means that, for any tortious claims, arising for data protection and/or privacy, data protection rules on applicable law would apply, to the exclusion of Rome II Regulation.

c. The *lex specialis* Argument

While the relationship between data protection rules and Rome II Regulation might be clarified by the analysis above, there is however less lucidity when it comes to the relation with Rome I Regulation. Thus, the second possibility is to see the two sets of legal sources (Rome I Regulation and Data Protection Directive) as being in a *lex generalis – lex specialis* relationship. It is submitted that this is indeed the reasoning that should be adopted with regard to the relationship between the two sets of legal rules. Rome I Regulation expressly allows for the inclusion of conflict-of-law rules with regard to 'particular matters' into other EU law instruments. As it stems from its Article 23, such conflict-of-law rules relating to particular matters shall not be prejudiced by either of these regulations, thereby expressly allowing for specialised conflict-of-law provisions.[66] Article 4(1) of the Data Protection Directive should be seen as such a special provision, since regulates the matter in particular field and, for that field, determines how to solve the conundrum relating to applicable law.

The case *Verein für Konsumenteninformation*,[67] a preliminary reference from an Austrian court, arguably confirms the correctness of the *lex specialis* argument. One of the questions that the national court puts forward is determining applicable law on the basis of Article 4(1)(a) of the Data Protection Directive in a factual context where a company concludes contracts with consumers in other Member States in the framework of electronic commerce and these contracts contain a clause with an agreement on applicable law of the seat of the company.[68] The Advocate General, without going into the analysis of whether the Rome I Regulation could apply for data protection issues in the case, immediately proceeded with interpretation of Article 4(1)(a) of the Data Protection Directive,[69] concluding that the law of only one Member State – the one of establishment of data controller – should be applicable to data processing issues in the case. Implicitly speaking, since the case also relates to the interpretation of Rome Regulations, the Advocate General would have first analysed the relation between Data Protection Directive and these regulations should the former not be *lex specialis* in relation to the latter. The CJEU seems to have confirmed this argument. In its judgment, it pointed out that it is the establishment of the controller that is relevant for determination of applicable law without going into the analysis of relationship between the Directive and Rome Regulations.[70]

However, while the case might – implicitly – address the question of which set of rules is applicable, it does not raise the question whether the *lex specialis* rule applies towards the entire Rome I Regulation or only towards certain provisions of this Regulation. It is therefore questionable whether some provisions of Rome I Regulation could still be relevant

64 Another argument in favour the position that art 1(g) of Rome II Regulation includes also violations of data protection laws can be inferred from a systematic interpretation of this regulation. According to its art 30(2), the Commission had to prepare a study covering not only the issues of 'the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality', but also conflict-of-law issues regarding the Data Protection Directive. It seems to result from this study, completed in 2009, that this article covers also data protection issues. See Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality, JLS/2007/C4/028, Final Report, 61 et seq.

65 'Comparative study on the situation in the 27 Member States' (n 64) 68.

66 See also Recital 40 of Rome I Regulation. It is however interesting to note that, whereas this recitals makes a specific reference to the Directive on electronic commerce (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1), it does not mention art 4 of the Data Protection Directive.

67 *Verein für Konsumenteninformation* (n 31).

68 ibid question 4(b).

69 See case C-191/15 *Verein für Konsumenteninformation* ECLI:EU:C:2016:388, Opinion of Advocate General Saugmandsgaard Øe, paras 106 et seq.

70 *Verein für Konsumenteninformation* (n 31) paras 72-81.

within the framework of data protection rules. It is submitted that the argument of *lex specialis* implies that Article 4(1) of the Data Protection Directive cannot be placed entirely outside of the system of Rome I and II Regulations. Whereas Article 4(1) could be a *lex specialis* with regard to the general or specific rules on applicable law in these regulations,[71] it is not entirely clear whether this is also the case with regard to the article regarding overriding mandatory provisions.[72] Nor does Article 4(1) of the Data Protection Directive expressly exclude the possibility of agreements on applicable law in data protection matters. This, in turn, raises the question whether Article 4(1) of the Data Protection Directive precludes the possibility of parties agreeing on applicable law in the field of data protection.

d. The Controversies around Agreements on Applicable Data Protection Law

The current doctrine and practice[73] is divided regarding the question whether the parties to a contract can freely choose data protection law that is applicable for processing of data and for data protection breaches in a framework of this contract.[74] Certain authors advocate the thesis that the parties to a contract have the freedom to make such a choice, arguing that Rome I Regulation does not (expressly) preclude the agreements regarding applicable data protection law.[75] Another argument in favour of such an approach is that data protection provisions cannot be seen as overriding mandatory provisions and that the contractual parties can, in no event, be deprived of their freedom of choice regarding applicable law. Other authors are of the opinion that Member States' data protection laws should be qualified as overriding mandatory provisions that do not allow for an agreement on applicable law between the parties.[76] Overriding mandatory provisions are, according to Article 9(1) of the Rome I Regulation, provisions that are regarded as 'crucial by a country for safeguarding its public interests'[77]. Overriding mandatory provisions[78] are those that are applicable regardless of the law that would be applicable on the basis of Rome I Regulation and regardless of the law that the parties have chosen.[79]

It is submitted that the latter view should prevail: data protection provisions should be seen as overriding mandatory provisions from which deviation in the sense of an agreement on applicable law is not possible. First, as it stems from the case-law of the CJEU, starting with *Ingmar*[80], not only provisions of Member States' law, but also provisions of EU law itself can be qualified as such provisions. In *Ingmar*[81], confirmed notably by *Honyvem Informazioni Commerciali*[82], *Semen*[83] and *Unamar*[84], the CJEU held

71 arts 3-8 of the Rome I Regulation and arts 4-9 of the Rome II Regulation.

72 art 9 of the Rome I Regulation and art 16 of the Rome II Regulation.

73 See, for example, the judgment of LG Berlin, 6 March 2012, Az 16 O 551/10 (allowing for such an agreement on applicable data protection law); as well as the judgment in the Case 8 B 60/12, *Facebook Ireland Ltd v Independent Data Protection Authority of Schleswig-Holstein, Germany* (not allowing for such an agreement).

74 A similar issue can arise also in the framework of the Rome II Regulation regarding the question whether art 16 of this Regulation regarding overriding mandatory provisions can be applicable in the field of data protection.

75 See, for example, Niko Härting, 'Rechtswahlklauseln in Datenschutzbestimmungen – Was ist zu beachten?' (2013) <http://www.cr-online.de/blog/2013/07/25/rechtswahlklauseln-in-datenschutzbestimmungen-was-ist-zu-beachten/> accessed 1 May 2015. Compare also Sven Polenz, 'Die Datenverarbeitung durch und via Facebook auf dem Prüfstand' (2012) Verbraucher und Recht 208-209, commenting upon the judgment of LG Berlin, 6 March 2012, Az 16 O 551/10.

76 See, for example, Carlo Piltz, 'Rechtswahlfreiheit im Datenschutzrecht? „Diese Erklärung unterliegt deutschem Recht"' (2012) K&R 640-645.

77 It is to be noted that different Member States interpret the scope of this notion differently, notably as to the question whether it covers only the overriding interests of the state or also of a weaker contractual party. See in this regard Kuipers (n 52) 569.

78 This notion should be distinguished from the notion of 'provisions which cannot be derogated from by agreement', used in other provisions of this regulation. In fact, apart from the notion of 'overriding mandatory provisions', Rome I Regulation contains also the notion 'rules that cannot be derogated from by agreement' in arts 3(3), 3(4), 6(2) and 8. As expressly stipulated in the Recital 37 of the Rome I Regulation, the former concept should be construed more restrictively than the latter. On the parallelism and distinction between the two concepts, see Alexander J Bělohlávek, *Rome Convention. Rome I Regulation. Commentary*, Vol 2 (Juris 2010), 1478-1480.

79 Bělohlávek (n 78) 1478.

80 Case C-381/98 *Ingmar GB* (CJEU, 9 November 2000) ECLI:EU:C:2000:605.

81 ibid para 21.

82 Case C-465/04 *Honyvem Informazioni Commerciali* (CJEU, 23 March 2006) ECLI:EU:C:2006:199, para 22.

83 Case C-348/07 *Semen* (CJEU, 26 March 2009) ECLI:EU:C:2009:195, para 17.

84 Case C-184/12 *Unamar* (CJEU, 17 October 2013) ECLI:EU:C:2013:663, para 40.

that the provision of the Directive on self-employed commercial agents[85] on the protection of the commercial agent after termination of the contract is mandatory in nature. Although not all EU law provisions have a character of overriding mandatory provisions, it can be claimed that, if those CJEU rulings are applied per analogy to the Data Protection Directive, its Article 4(1) could have a mandatory character.

Second, a textual argument in favour of designating data protection provisions as being overriding and mandatory can be inferred from Recital 18 of the Data Protection Directive which provides that the processing of personal data in the Union '*must* be carried out in accordance with the law of one of the Member States' and that the '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'[86].

Third, in order for a provision to be qualified as an overriding mandatory provision, the norm has to have the purpose of pursuing public interest.[87] To the extent that data protection contains administrative law provisions and relates to administrative enforcement, it undoubtedly pursues public interest objectives. However, in the framework of civil claims – in which the question of existence of mandatory provisions arises – such public interest might be more difficult to demonstrate. Nevertheless, two arguments need to be probed in order to prove the public interest nature of data protection provisions in general.

On the one hand, it is submitted that the public interest of the provisions of Data Protection Directive could be demonstrated by the circumstance that the directive pursues internal market objectives by ensuring free movement of personal data.[88] Whereas the adoption of legislation on the basis of the provision relating to the internal market undeniably demonstrates public interest of this legislation, it is not clear whether this suffices for a legal instrument to contain mandatory provisions within the meaning of Article 9 of the Rome I Regulation. Such reasoning would imply that all EU legislation in civil and commercial matters based on Article 114 TFEU has, by that very fact, the nature of an overriding mandatory provision. Given the fact that the Treaties do not provide for a specific legal base for adopting legislation in civil matters and that such legislation will be based on Article 114 TFEU, it might be a bit far-reaching to treat all the legislation adopted on the basis of this article as mandatory within the meaning of Article 9(1) of the Rome I Regulation.

On the other hand, a stronger argument in favour of public interest of data protection provisions is that, insofar these provisions aim to safeguard fundamental rights of data subject in civil claims, they can be seen as pursuing public interest objectives. Fundamental rights represent rudimentary values of society whose public interest can hardly be denied. Furthermore, it is apparent from earlier case-law such as *Viking Line*[89] and *Laval*[90] that fundamental rights indeed fall within the category of overriding reasons of public interest (at least within the framework of free movement of goods). Moreover, Data Protection Directive is a legal instrument that 'gives specific expression' to a fundamental right to data protection,[91] and it stems from the CJEU's case-law that data subject's rights from the Directive are inextricably linked to fundamental rights to data protection and privacy.[92] Hence, given the strong presence of fundamental rights element, it is submitted that data protection provisions should be seen as overriding mandatory provisions within the meaning of Article 9(1) of the Rome I Regulation.

Yet, this theoretical solution did mostly not yet find its way into practice. Agreements on applicable law are firmly rooted in practice, without their validity or legitimacy being challenged and, most importantly, without treating data protections issues separately from other contractual issues. As an already

85 Council Directive 86/653/EEC of 18 December 1986 on the coordination of the laws of the Member States relating to self-employed commercial agents [1986] OJ L 382/17.

86 Emphasis added. This argument is pointed out by Carlo Piltz, 'Rechtswahlfreiheit im Datenschutzrecht?' (2013) <http://www.delegedata.de/2013/07/rechtswahlfreiheit-im-datenschutzrecht/> accessed 27 February 2015.

87 Bělohlávek (n 77) 1474; Karsten Thorn, in Thomas Rauscher (ed), *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR. Kommentar. Rom I-VO. Rom II-VO* (sellier 2011) 425 et seq.

88 Piltz, 'Rechtswahlfreiheit im Datenshutzrecht? „Diese Erklärung unterliegt deutschem Recht"' (n 76) 643.

89 Case C-438/05 *International Transport Workers' Federation and Finnish Seamen's Union v Viking Line* (CJEU, 11 December 2007) EU:C:2007:772, para 77.

90 Case C-341/05 *Laval un Partneri* (CJEU, 18 December 2008) ECLI:EU:C:2007:809, para 103.

91 E Muir, 'The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges' (2014) 51(1) Common Market Law Review 226.

92 Case C-362/14 *Schrems* (CJEU, 16 October 2015) ECLI:EU:C:2015:650; *Google Spain and Google* (n 9).

mentioned, renting a car with Europcar would submit you to French law[93] or opening an e-mail with www.yahoo.co.uk automatically submits you to the application of Irish law.[94]

An exception mentioning overriding mandatory provisions in data protection framework and, in the same vein, showing the controversy regarding agreements on applicable data protection law is the German case *Facebook v Independent Data Protection Authority of Schleswig-Holstein*.[95] According to this decision, the General terms and conditions of Facebook contained a clause according to which, for German users, German law applies. The German court pointed out that, according to Rome I Regulation, it is in principle possible to make an agreement on applicable law for the contract, but not on data protection law, since the provisions on data protection fall within the concept of overriding mandatory provisions within the meaning of Article 9 of the Rome I Regulation, making it impossible for the parties to make an agreement on applicable law in this regard.[96] The reasoning of the German court can be fitted more the fundamental rights perspective. It can be argued that, given the fact that data protection constitutes a fundamental right which is concretised through the Data Protection Directive, it is not possible to deviate from this fundamental right or the rules adopted for its implementation.[97] Unfortunately, when the German Federal administrative court (*Bundesverwaltungsgericht*), deciding on appeal in this case, asked questions for preliminary ruling to the CJEU, it did unfortunately not address the issue of whether data protection provisions can be seen as overriding mandatory requirements.[98]

On another note, it is dubious how Rome I, regulating applicable law for contracts in civil and commercial matters, could apply at all in the German *Facebook* case, despite the fact that the case has been decided by an administrative court in a dispute between a Data Protection Authority (DPA) and Facebook and that the content of the claim was to set aside an administrative decision of a DPA. Nevertheless, the German court still considered that the Rome I Regulation could be relevant. The reason for that seems to be that the relationship between Facebook and its users – the two contractual parties that agreed on the application of German data protection law for the purposes of this contract –, is in nature a civil-law relationship to which the Rome I Regulation applies.[99] Moreover, it is important to stress that a civil law agreement on applicable law between contractual parties could, in no circumstance, alter the possibility to enforce a data breach through the administrative enforcement authorities (DPAs) which could potentially be an additional reason to see Article 4(1) as an overriding mandatory provision.

Finally, the case *Verein für Konsumenteninformation*,[100] a preliminary reference from an Austrian court, regrettably does not address the issue whether the provisions on data protection law could constitute overriding mandatory provisions, but only a question whether, from a consumer protection perspective, an agreement on applicable law could be seen as an unfair contractual clause. It is to be agreed with the CJEU that a general clause on applicable law in consumer contracts should be regarded as unfair if the consumer is not informed about the possibility to invoke overriding mandatory provisions.[101] If a parallel is drawn between consumer protection law and data protection law – notably from the perspective that, in contractual relationships, both sets of rules aim to protect the weaker party of a contract – it could equally be argued that the data subject should be given the possibility to invoke overriding mandatory provisions in case of agreements on data protection law. It is submitted that the status of data subject should be assimilated to the status of consumer in that both seem to be in a weaker position than their contractual counterpart, business or data controller respectively. Given that similarity, agreements on applicable data protection law could, per analogy, equally be considered as unfair contractual clauses if

93 See art X of the Online Booking Terms and Conditions of Europcar, available at <https://www.europcar.com/terms-and-conditions/online-booking> accessed on 23 June 2016.

94 See art 25(3) of Yahoo Terms of Service, available at <https://policies.yahoo.com/ie/en/yahoo/terms/utos/index.htm> accessed 23 June 2016.

95 *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany*. For a comment of the decision, see for example Carlo Piltz, '*Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany* – Facebook is not subject to German data protection law' (2013) 3 International Data Privacy Law 210-212.

96 ibid 4-5.

97 Compare also Kuipers (n 52) 75.

98 See 'EuGH soll datenschutzrechtliche Verantwortlichkeit für die beim Aufruf einer Facebook-Fanpage erhobenen Nutzerdaten klären' (n 35).

99 *Facebook Ireland Ltd. v Independent Data Protection Authority of Schleswig-Holstein, Germany*, 4.

100 *Verein für Konsumenteninformation* (n 31).

101 ibid para 71.

they do not allow to the data subject to invoke the applicable data protection law as an overriding mandatory provision.

IV. *De lege ferenda*: Territorial Application of the General Data Protection Regulation

1. Applicability of GDPR within the EU

The GDPR[102] contains a provision determining its territorial scope of application. Similarly as the current Data Protection Directive, the GDPR distinguishes between situations where the controller is established in the EU and where it is not.

If the controller has an establishment in the EU, the regulation applies, according to its Article 3(1), 'to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.' This paragraph of Article 3 contains two important elements.

On the one hand, it can be seen that the first part of the rule for territorial application of EU data protection legislation partially remained the same as in Data Protection Directive: processing of data in the context of the activities of a controller or processor, established in the Union. Therefore, with regard to this issue, the legal questions concerning the interpretation of this provision also remain the same, in particular the meaning of the phrase 'in the context of the activities' and 'establishment'. It should be noted that – just as in Data Protection Directive[103] – the notion of establishment is defined in Recital 19 GDPR as 'the effective and real exercise of activity through stable arrangements'. Therefore, it seems that the reasoning of the CJEU in the case *Google Spain* – where the CJEU found the effective and real exercise of the Spanish subsidiary of Google – will be pertinent also with regard to GDPR. The CJEU in *Weltimmo* equally used this criterion in order to affirmatively answer the question whether a company registered in Hungary had an establishment in Slovakia.[104] In this regard, it is important to note that the criterion of 'establishment' is interpreted on a factual basis and is largely unrelated to the place where the company or its subsidiary is registered. The interpretative balance regarding this criterion tilts more towards the place where the goods and services are offered and therefore comes closer to the place of residence of data subject then the actual seat of the company or its subsidiary.

On the other hand, the second part of the criterion from Article 3(1) – 'regardless of whether the processing takes place in the Union' broadens the applicability of GDPR much further than the current regime.[105] As was explained above, the place of processing or an activity closely related to processing is currently an important factor for determination of applicable law. With GDPR, the place of processing becomes an unimportant criterion for such determination. Rightly so, given the fact that data can be processed anywhere in the world, in particular from a technical perspective (eg servers being located in a different country then the headquarters of a company). Placing the second part of Article 3(1) in the context of the entire provision, it can be established that the criterion of processing is still important in that it still has to be done 'in the context of the activities of an establishment of a controller or a processor'. However, that processing can be done in a third country, not within the EU, as long as the establishment of the controller is within the EU. Therefore, the issue that the CJEU encountered in *Google Spain* – where the actual processing of data was taking place in California – will not be problematic anymore after the entry into force of the GDPR.

The GDPR therefore no longer contains a conflict-of-laws provision determining the applicable law of a particular Member State for the processing of personal data, since the regulation itself unifies the legal regime on processing of data. Nevertheless, the conflict-of-law issues within the EU could – to a certain extent – still be relevant within the scope of the GDPR.

Questions of applicable law might be relevant if the Member States, despite the Regulation, maintain in force divergent provisions on issues not addressed in detail by the regulation. For example, Article 77 of the proposed Data Protection Regulation gives the

102 Regulation 2016/679 (n 4).

103 See Recital 19 of Data Protection Directive.

104 ibid paras 39-41.

105 See Carol A F Umhoefer and Caroline Chancé, ' Europe: The Applicability Of EU Data Protection Laws To Non-EU Businesses', DLA Piper LLP (2016) <http://www.lexology.com/library/detail.aspx?g=95e11bfd-2931-44da-ac29-371614c516bd> accessed 6 April 2016.

data subject the right to claim damages in case of an unlawful processing of data. However, different Member States can have more or less favourable civil law rules on causal link or quantification of damage. Since the regulation does not specify which law is applicable in case of absence of specific unified rules, such cases might lead to forum shopping in favour of regimes of certain Member States. The conundrum on applicable law would, in such cases, be solved on the basis of general conflict-of-law rules. However, the problem with this approach is that only Rome I Regulation could be applicable and not Rome II Regulation, since the latter excludes from its scope issues related to privacy, as explained above. In tortious claims, it therefore seems that the national conflict-of-laws of the court deciding on the issue would be pertinent to determine the applicable law.

Furthermore, conflict-of-law rules will also be necessary whenever the GDPR gives to the Member States power to deviate from its provisions or to supplement them. For example, Member States may add specific requirements with regard to the lawfulness of processing,[106] lower the age of child's consent[107] or further limit processing of genetic, biometric or health data.[108] From the GDPR, it is unclear in what instances the law of a particular Member State will apply. The application of general conflict-of-law rules remedies this situation. In case of tortious claims, the applicable law will be determined on the basis of national legislation of Member State where the claim is decided. With regard to claims arising from breach of contract, the applicable law will be determined on the basis of Rome I Regulation.

For example, if the Member State A provides that the age for a child's consent is 14 years (instead of 16 years as provided by the GDPR)[109] and a child from that Member State opens an e-mail account with a provider established in Member State B, it is submitted that the legislation of Member State A should apply regarding child's consent because the child should be able to rely on his/her rights provided by domestic legislation. Such reasoning relies on Article 6(1) of the Rome I Regulation pursuant to which the law of the country of consumer's habitual residence applies for any type of consumer contract – which encompasses the contract between the child and the e-mail provider. Regarding stricter conditions on processing of genetic, biometric or health data, the data subject could equally invoke the law of his/her Member State if he is regarded as a consumer towards the data controller. If, however, the data controller is seen as providing services to the data subjects, it is the law of the establishment of the controller that will be applicable.[110] It is submitted that the use of Rome I Regulation in case of differences in Member States' data protection legislation is appropriate since it guarantees the balance of interests between the data subject and data controller.

Finally, conflict-of-law related questions might be relevant regarding the (im)possibility to enter into an agreement on applicable data protection law of a particular Member State. Apart from the argument that GDPR, just as Data Protection Directive, contains overriding mandatory provisions, it is submitted that, after the entry into force of the regulation, such agreements will no longer be practically possible, since the GDPR will, as a unifying legislation, replace the national legislation on data protection, except on points expressly allowed by the GDPR to be deviated from. Agreeing on applicable law of a particular Member State would therefore be tantamount to agreeing on the application of the GDPR itself. If the contractual parties agree on the application of a law of a Member State for an issue not covered by the GDPR or where Member States can diverge, it is the rules of Rome I Regulation that will solve this conflict-of-laws issue.

2. Applicability of GDPR Outside the EU: Towards Extraterritorial Application?

a. Article 3(2)(a) and Agreements on Applicable Law

The second and the third paragraph of Article 3 of GDPR deal with a situation where a controller does not have an establishment in the Union. According to Article 3(2)(a) of GDPR, such a controller has to comply with the rules established in the regulation if his activities relate to the offering of goods or services to data subjects in the Union.[111] It is not entire-

106 See art 6(2) of the GDPR.

107 See art 8(1) of the GDPR.

108 See art 9(4) of the GDPR.

109 See art 8(1) of the GDPR.

110 See art 4(1)(b) of the Rome I Regulation.

111 See art 3(2)(a) of the GDPR.

ly clear what 'offering of goods or services' entails, but from reading Recital 20 of GDPR it becomes clear that it should be 'apparent that the controller is *envisaging* the offering' of goods/services to European data subjects.[112] Through this recital, it is also clarified that, whereas mere access to a website or e-mail address are not sufficient for the GDPR to apply, other criteria, such as the mention of Member State's currency or offering of goods/services in a language of this Member State could point to controller's intention to offer goods/services to European data subjects.[113] In practice this means that many online stores based in the US and not having a subsidiary in the Union will have to comply with the European data protection legislation when they offer goods or services online to European data subjects.[114]

The criterion of envisaging doing business in a particular Member State of the European Union can be compared with criteria for 'orientating' business activities to a Member State, as developed by the CJEU in *Pammer and Hotel Alpenhof,*[115] *Mühlleitner*[116] and *Emrek*.[117] Just as in *Pammer*, the accessibility of the website, e-mail address or other contact details is insufficient to fulfil the criteria of 'orientating'.[118] However, the criteria developed in *Pammer* are much more detailed than those in Article 3(2)(a) of the GDPR and the related Recital 20. The *Pammer* judgment offers a non-exhaustive list of criteria, among which are, other than the use of language (of a particular Member State) and possibility to make reservation in that language (also used in Recital 20 GDPR) also the international nature of the activity, mention of telephone numbers with an international code, use of a top-level domain name other than that of the state of establishment.[119] Moreover, the criteria from Article 3(2)(a) GDPR and Recital 20 can also be compared with the CJEU's reasoning in *Google Spain and Google*, which requires that the subsidiary of a search engine 'orientates' its activity towards the Member State where it promotes and sells advertising space.[120]

Therefore, with the GDPR, the question of applicable law will move more on a global level in that the European authorities and third-country companies will have to, prior to raising the issue of compliance with the GDPR, address the question whether EU law applies or not. From the mere text of Article 3(2)(a) it seems that the applicability of GDPR will extend far over EU borders[121] and is therefore controversial[122] for two principal reasons.

On the one hand, the third-country controller only has to *offer* goods or services within the Union in order for GDPR to apply. In view of Svantesson, this means that 'this provision seems likely to bring all providers of Internet services...under the scope of EU Regulation as soon as they interact with data subjects...in the European Union'.[123] It has been argued that the GDPR changed the connecting element from 'country of origin' to 'country of destination'.[124] For GDPR to apply, it is not important whether the controller offering goods or services has any territorial connection with the EU and it is not important whether the data subject in the EU actually buys goods or services.[125] In practice this will probably mean that third-country controllers will build different websites for different countries (or at least a special website for EU customers) with in-built Privacy-By-Design settings complying with GDPR. For smaller businesses which cannot afford such settings, it will be much more difficult to comply with GDPR, in particular in a stage where they merely offer goods or services to data subjects in the EU.

---

112 Emphasis added.

113 See Recital 20 of the GDPR.

114 As a comparison, on extra-territorial application of Data Protection Directive, see Article 29 Data Protection Working Party, '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' (2002), 5035/01/EN/Final, WP 56, 4. See also Kuner, 'Internet Jurisdiction' (n 52) 178.

115 *Pammer and Hotel Alpenhof* (n 25).

116 *Mühlleitner* (n 26).

117 *Emrek* (n 27).

118 *Pammer and Hotel Alpenhof* (n 25) para 94.

119 ibid para 93.

120 *Google Spain and Google* (n 9) para 60.

121 James Castro-Edwards, 'The Proposed European Data Protection Regulation' (2013) Journal of Internet Law 6, points out that non-EU businesses 'will need to be mindful of the potential 'long arm' of the Regulation and the potential heavy sanctions for failing to comply'.

122 Jacob M Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 The Yale Law Journal 514, stresses that the GDPR is 'controversial for its potential applicability to any corporation that processes the personal data of EU citizens (including U.S. corporations)'.

123 Dan Jerker B Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto 2013), 107.

124 Dennis Holmes, 'Debating the "Where" of Online Jurisdiction' The Privacy Advisor <https://iapp.org/news/a/debating-the-where-of-online-jurisdiction/> accessed 11 April 2016.

125 Alexander Dix, 'The Commission's Data Protection Reform After Snowden's Summer' (2013) 5 Intereconomics 269, points out that many US companies have accepted this rule.

On the other hand, the criterion from Article 3(2)(a) GDPR only requires that data subjects are 'in the Union'. There is no requirement that data subjects have to reside (permanently or temporarily) in the Union, but merely that they are present on its territory. It is questionable though how this phrase should be interpreted. If a friend from India pays a visit to the EU and orders a book online to be delivered to his hotel during his stay in Europe, does the GDPR apply? Svantesson understands this criterion as requiring residence in the EU,[126] but such an interpretation is not supported by the text of the article which the legislator, should it have had residence of data subject in mind, would have drafted differently.

A very extensive reading of this provision could even lead to an interpretation according to which the Union legislation on data protection would apply even if a European data subject buys goods or receives services while being physically in the territory of a third state and not online.[127] Such an interpretation would however lead to a too extensive extraterritorial application of Union legislation on the territory of a third state and can therefore not be upheld.[128] It would also go against the wording of Article 3(2)(a) GDPR.

Since the offering of goods or services from Article 3(2)(a) GDPR would be based on a contract, it is important to address the question whether the parties to that contract could agree on the application of a *third-country law* and hence entirely exclude the application of GDPR for data protection matters raised by the contract. For example, according to Facebook's Terms of Service, any dispute between the company and its users will be governed by the law of the State of California, 'without regard to conflict of law provisions'.[129] Or, to provide another illustration: suppose that it is non-disputed that a Chinese provider of cloud computing offers these services on the territory of Ireland, but the general terms and conditions of the cloud computing service contract stipulate that, regarding all disputes arising from this contract, Chinese law applies. The contract does not differentiate between data protection breaches and other contractual breaches. Which law would be relevant for contractual data protection breaches by this company?

According to the general conflict-of-law rules (Rome I Regulation), the parties have in principle a freedom of choice to decide which law will govern the contract.[130] Moreover, this regulation has 'universal application', meaning that the law to which the regulation – or the agreement on the basis of this regulation – points to should not necessarily be the law of a Member State; it can be also be a law of the third country.[131] However, under Article 3(2)(a) GDPR, it is this regulation that should be applicable, since the services are offered in the Union. Could the GDPR still apply regardless of the agreement?

It is submitted that this question should be answered in the affirmative. Just as with regard to the agreements pointing to the application of Member States' law in the framework of Data Protection Directive analysed above, it is possible to qualify the GDPR rules as overriding mandatory provisions the use of which cannot be altered by an agreement. As examined within the framework of Data Protection Directive, these provisions aim at safeguarding public interests of a country[132] which can be, in case of data protection, demonstrated by the GDPR's aim to protect fundamental rights. The examples above amount to a comparable factual constellation to the one in *Ingmar*, where the contractual parties, one of them being a commercial agent for the other, agreed on the applicability of the law of the State of California for the contract.[133] If we draw an analogy with data protection and the parties agree on the applicability of a third-country law for processing of data, it is submitted that such an agreement is precluded due to the mandatory character of GDPR provisions.

b. Articles 3(2)(b) and 3(3)

The GDPR will apply also if activities of the controller not established in the Union relate to the monitoring

126 Svantesson (n 123) 107.

127 Compare ibid.

128 Compare also Moerel (n 2) 44; who points out that 'an unbridled expansion of applicability of EU data protection laws to processing of data on EU citizens wherever in the world should be prevented'.

129 See s 15.1. of Terms of Service of Facebook <https://www.facebook.com/terms> accessed 9 September 2016.

130 See art 3(1) of the Rome I Regulation.

131 art 2 of the Rome I Regulation. Differently from the classic rules on applicable law enshrined in Rome I and II Regulations, art 4 of Data Protection Directive does not have universal application. In other words, the law that can be applicable according to the Data Protection Directive can only be the law of one of the Member States and not the law of a third country.

132 art 9(1) of the Rome I Regulation.

133 *Ingmar GB* (n 80) para 10.

of the behaviour of data subjects in the Union [Article 3(2)(b)]. It is not clear how broad this article should be interpreted. On a more realistic interpretation, this provision covers monitoring of behaviour by companies established in third countries (such as Google or Facebook), in order to use the gathered information for commercial purposes, such as targeted advertising. Such an interpretation seems to be confirmed by Recital 21 of the GDPR where 'monitoring' is explained as an activity where

> individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Therefore, the third-country companies that profile[134] data subjects in the Union will be able to perform their marketing activities and target their advertising, but only under the legal regime and requirements of the GDPR.[135]

On a (much) more expansionist interpretation, it could also be argued that even the US National Security Agency, when processing data of Union citizens or obtained from Union authorities, has to respect Union law. Although this is, admittedly, an extremely broad interpretation of this article, the text of the article does not seem to limit such an application *ratione personae* of this article (the Recital 21, however, does). One could stretch this interpretation even further and ask a question whether this would also mean that the US authorities have to observe Union law when a Union citizen travels to the US and gives his fingerprints on the US border. Such an interpretation, however, seems to be rather far-reaching, in particular because it would lead to a broad extraterritorial application of the EU data protection legislation. It should therefore not be accepted.

In case of a tortuous claim regarding data protection breaches, it is necessary to clarify the relationship between Article 3(2)(b) GDPR and the general conflict-of-law rules (Rome II Regulation). Indeed, Rome II Regulation – just as Rome I Regulation – has universal application, meaning that 'any law specified by this Regulation shall be applied whether or not it is the law of a Member State'.[136] According to the general rules from Rome II Regulation, the applicable law in case of tort – such as an infringement of data protection rights in the framework of monitoring – would be the law of the country where the damage occurred,[137] which could also be a law of a third country. Nevertheless, as already established within the framework of analysis on Data Protection Directive, Rome II Regulation is not applicable in privacy and data protection matters; hence the GDPR would be applied.

Finally, the third paragraph of Article 3 of the proposed Data Protection Regulation is, again, comparable to the rule set out in the current Article 4(1)(b) of the Data Protection Directive, since both legal instruments provide for the applicability of, respectively, Union and Member State's law, in case where the national law of a Member State 'applies by virtue of public international law'. This paragraph is not often applicable in practice and does not raise questions of conflict-of-laws.

V. Conclusion

The analysis in the present article focuses on questions of applicable law in data protection matters, both as regards determining this law within the system of Data Protection Directive or GDPR as well as concerning relationship between data protection legislation and general conflict-of-law rules. The outcome of this analysis is that both current and future rules concerning applicable law in the field of data protection would, in certain aspects, need to be clarified.

As far as the current legislation is concerned, the nature of the relationship between the 'classic' conflict-of-law rules (Rome I and II Regulations) and the provisions of more specific rules on applicable law, contained in Data Protection Directive, would need

134 The notion of 'profiling' is defined in art 4 GDPR as 'any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

135 See Olivier Proust, 'Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed' (*Privacy, Security and Information Blog*, 4 December 2015) <http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed/> accessed 9 September 2016.

136 See art 3 of the Rome II Regulation.

137 See art 4(1) of the Rome II Regulation.

to be laid down. It is submitted that the Directive should contain a special provision clearly stating that it should be considered as *lex specialis* towards the general conflict-of-law rules from Rome I and II Regulations.

Yet, given that the GDPR will soon enter into force, the proposal for an amendment of its provisions should be put into the spotlight. The GDPR, contrary to the Data Protection Directive, unifies EU data protection rules and hence no longer contains an overarching conflict-of-law provision. Therefore, it in principle no longer raises conflict-of-law issues between laws of different Member States. Nevertheless, the questions of applicable law could still be problematic notably in cases where the GDPR does not regulate an issue or where it authorises Member States to adopt divergent rules on certain issues. Moreover, the GDPR would need to contain a clear provision on the question whether data protection rules can constitute overriding mandatory provisions from which no deviation is possible. This is particularly important from the perspective of agreements on applicable law which are still very often a standard when it comes to big multinational companies. Therefore, it is proposed that the GDPR be amended in the following manner:

> Article 3 (Territorial scope)
>
> ...
>
> 4. Where this Regulation does not contain rules on a particular issue or specifically authorises Member States to adopt rules diverging from this Regulation, the issues of applicable law are to be regulated by EU or Member States' general conflict-of-law rules.
>
> 5. In case of an agreement on applicable data protection law between data subject and data controller, the provisions of this Regulation should be considered as mandatory overriding provisions. In consequence, agreements on applicable law that are not in accordance with the provisions of this Regulation should be considered null and void.

It is submitted that such an amendment of Article 3 GDPR would give a clear guidance in cases of doubts as to applicable law in data protection matters. Going back to the examples from the introduction to this piece, under such amended rules, neither the agreement on applicable law with Facebook nor the agreement with Europcar – to the extent that they concern applicable data protection law – would be possible. With regard to the Chinese company selling its products to European customers, the latter would still be able to invoke the protection from GDPR in case of an agreement on applicable law.

Finally, as demonstrated in the present piece, the future data protection rules open the possibility of extraterritorial application of GDPR that expands the circle of addressees far beyond Europe. While the European data protection rules (will) bind these third-country controllers, it is, however, questionable, how these rules will be enforced towards these controllers.[138] The issue of extraterritorial enforcement, which will become even more topical after the entry into force of the GDPR, therefore gives already food for thought for further research.

138 See, for example, Kropf (n 20) 507, who points out that 'the Union's inability to enforce judgments for processing activities that occur outside EU territory could create conflicts with other commercial frameworks at a time when interoperability of commercial regimes is critical.'