International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR

Lydia Lundstedt*

1 Introduction

The new European Union (EU) Regulation 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 (hereinafter "General Data Protection Regulation or "GDPR")[1] aims to strengthen individual rights for the protection of personal data by, *inter alia*, facilitating private enforcement actions.[2] To this end, the GDPR clarifies the data subject's right to a direct and independent private enforcement action directly against the controller or processer.[3] As the infringement of personal data rights increasingly takes on cross border dimensions, the GDPR sets out rules on jurisdiction allowing the data subject to bring a private enforcement action in the Member State where the offending controller or processor has its establishment, or alternatively in the Member State where the data subject has his or her habitual residence.[4]

The aim of this article is to analyze the jurisdictional options available to a data subject to bring a private enforcement action to enforce his/her data protection rights before the GDPR, under the Member States' general rules on jurisdiction in private international law, and after the GDPR, under the GDPR's own rules on jurisdiction. In addition, the article analyzes whether the new rules on jurisdiction in the GDPR supplement or supplant the Member States' general rules on jurisdiction. The article discusses and analyzes the areas where the application and interpretation of the rules are unclear, and proposes interpretations that best serve the objectives of the GDPR to strengthen the rights of data subjects by facilitating private enforcement actions without jeopardizing the principle of legal certainty deemed necessary for the free movement of data within the EU.

* The author would like to thank Ija Fink Lundgren, LL.M., Dr. Stanley Greenstein, Dr. Erik Sinander, and Christine Storr, LL.M., all from Stockholm University, and Laura Chadwick from the U.S. Department of Health and Human Services for their valuable feedback. Any mistakes are my own.

1 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, GDPR or Regulation (EU) 2016/679). The GDPR applies as of May 25, 2018. Article 99 Regulation (EU) 2016/679. In addition to the GDPR, the EU Data Reform package includes Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2 *See* recitals 141-142 Regulation (EU) 2016/679; Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM (2012) 9 final p. 6.

3 Article 79 Regulation (EU) 2016/679.

4 Article 79(2) Regulation (EU) 2016/679.

1.1 The GDPR's Primary Objectives: Strengthening Individual Rights and Facilitating the Free Movement of Data

One of the principle objectives of the GDPR is to strengthen individual rights to the protection of personal data. [5] Indeed, the protection of personal data is a fundamental right that the Charter of Fundamental Rights of the European Union (EU Charter) and the Treaty on the Functioning of the European Union (TFEU) explicitly protect. [6] Another principle objective is to ensure the free movement of personal data within the EU.[7] The EU legislature believes that a strong and coherent data protection framework is essential to the development of the digital economy across the EU's Single Market, and will contribute to the EU's economic and social progress.[8] The rapid technological developments and globalization have led to an unprecedented collection, storage, and sharing of personal data, in particular over national borders.[9] Due to the existence of differences in the Member States' implementation and application of Directive 95/46/EC on Data Protection,[10] data protection rights and obligations among the Member States had been fragmented, which has led to legal uncertainty, both for natural persons, but also for economic operators and public authorities.[11]

In order to ensure a consistent and homogenous application of the rules with regard to the processing of personal data throughout the EU, and legal certainty for natural persons, economic operators and public authorities, the EU legislature chose a regulation instead of a directive as the form for the Data Protection

5 Article 1(2) Regulation (EU) 2016/679 on Subject Matter and Objectives; COM(2012) 9 final Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final p. 2.

6 *See* article 8(1) of the Charter of Fundamental Rights of the European Union (EU Charter); Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). *See* also recital 1 Regulation (EU) 2016/679 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

7 Article 1(3) Regulation (EU) 2016/679 on Subject Matter and Objectives; Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final p. 2.

8 Recital 2 Regulation (EU) 2016/679: ("This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."); Regulation (EU) 2016/679 recital 7 ("Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.").

9 Recital 6 Regulation (EU) 679/2016.

10 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 (Directive 95/26/EC).

11 Recital 9 Regulation (EU) 679/2016.

Reform.[12] Unlike a directive, a regulation is directly applicable in all Member States without the need for implementation into national law.[13] This simplifies the legal landscape for data controllers and processors by increasing legal certainty and providing a level playing field.[14] Nevertheless, the GDPR leaves room for the Member States to adopt complementary national rules to further specify the application of the GDPR's rules with respect to the lawfulness of processing and specific sectors, and to adopt national rules for the processing of special categories of personal data.[15] In addition, the GDPR does not prevent Member States from enacting or applying national provisions regarding issues that the GDPR itself does not cover.[16]

When it comes to strengthening individuals' rights for the protection of personal data, the GDPR not only strengthens the substantive law rights (such as the right to rectification and erasure and the new right to data portability)[17] but it also strengthens procedural remedies and sharpens the sanctions. In particular, the GDPR grants the Data Protection Authorities (DPAs) the broad powers to act and to impose heavy administrative fines.[18] The GDPR also aims to make it easier for individuals to exercise and enforce their rights.[19] With respect to this aim, the GDPR confirms, clarifies, and extends a data subject's right to an effective judicial remedy and introduces the possibility for collective actions.[20] While the primary focus of the GDPR is public law enforcement of data protection rights through

12 Recitals 9 and 10 Regulation (EU) 679/2016 ("In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union... ").

13 Article 288(2) TFEU.

14 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final p. 10.

15 Recital 10 and article 6(2), 23, 80(2), 85, 88 Regulation (EU) 679/2016. *See* generally Wagner, J. & Benecke, A., *National Legislation within the Framework of the GDPR: Limits and Opportunities of the Member State Data Protection Law*, European Data Protection Law Review, Volume 3/2016 p. 353-361; Chen, Jiahong, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*, International Data Privacy Law, Volume 6, Issue 4, 1 November 2016, p. 310–323.

16 Chen, Jiahong, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*, International Data Privacy Law, Volume 6, Issue 4, 1 November 2016, p. 310–323, p. 312.

17 *See* generally Chapter III Regulation (EU) 2016/679 for a detailed catalogue of rights.

18 Article 86 Regulation (EU) 679/2016.

19 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM (2012) 9 final p. 6.

20 *See* article 80 Regulation (EU) 679/2016.

administrative remedies and fines[21], the GDPR explicitly provides for a right to a private enforcement action, that is, the "[r]ight to an effective judicial remedy against a controller or processor."[22]

1.2 Advantages of Private Enforcement Actions

In the past, it has been rare for individuals to bring private enforcement actions directly against a controller or processer for the enforcement of data protection rights.[23] One reason for this is that judges, practitioners, and scholars have traditionally viewed data protection law as a field of public or administrative law enforced by state authorities and resulting in fines rather than giving rise to claims against individuals for private law remedies.[24] Another reason for the paucity of private enforcement actions is that legal uncertainty, the costs of litigation, and the considerable efforts involved in bringing formal courts proceedings deter potential claimants. [25] This is especially true if the offending controller or processor is located in another country.

---

21 *See* Galetta, Antonella & De Hert, Paul, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, Review of European Administrative Law, Volume 8, number 1/2015 p. 125-151, p. 145.

22 Article 79 Regulation (EU) 679/2016.

23 Korff, Douwe, *Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, final [extended and re-edited] version, European Commission 2010 p. 98 (maintaining that court litigation by ordinary citizens for breaches of data protection law is extremely rare and observing that in the UK, the case of Naomi Campbell was the first case ever in which compensation was awarded for such a breach); Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 179 (observing that national courts' involvement in enforcing data privacy law has been marginal compared to the role played by Data Protection Authorities); Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 258 (observing that DPAs play a major role in data protection enforcement).

24 *See* Svantesson, Dan, *Enforcing Privacy Across Different Jurisdictions* p. 195-222, in Wright, David & De Hert, Paul (eds.), Enforcing Privacy Regulatory, Legal and Technological Approaches, Springer International Publishing (Online service) 2016 p. 196 (remarking that scholars in the field of private international law have not yet understood that data privacy law raised questions within their field of law). *See* also Kuner, Christopher, *Data protection law and international jurisdiction on the Internet (Part 1)*, 2010, Vol. 18, Issue 2, International Journal of Law and Information Technology p. 176–19, p. 181 (discussing the difficulty and (lack of) usefulness of classifying data protection law as private or public law).

25 Korff, Douwe, *Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, final [extended and re-edited] version, European Commission 2010 p. 98; European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* 2014 p. 8 (stating that most individuals will not pursue cases before a court because of the lengthy, time-consuming and complicated procedures and costs involved).

Increasingly, however, individuals are taking direct action against the offending controller or processor in court.[26] There are advantages to bringing a private action as it puts the individual in control of his/her own personal data. If a data subject makes a complaint to a DPA for the infringement of data protection rights, it is the DPA that decides whether and how to pursue the complaint. As DPAs often lack sufficient funding and must prioritize which complaints to pursue, the DPA may decide not to take any enforcement action with respect to an individual complaint.[27] An individual that files a private enforcement action directly against the offending controller or processer is able to exercise control of his/her own personal data, even with respect to how enforcement of his/her rights are carried out.[28] The possibility to bring a private enforcement action is in itself an aspect of empowerment.[29] Facilitation of private enforcement actions reflects the general trend away from a paternalistic attitude toward data protection to an attitude that values autonomy.[30]

Another advantage of filing a private enforcement action is that Member State judgments concerning "civil and commercial matters" must be recognized and enforced in the other EU Member States as well as Norway, Iceland and Switzerland.[31] Private law claims for the infringement of data protection rights fall within the concept of "civil and commercial matters", thereby triggering the application of the rules on recognition and enforcement in Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Ia Regulation, BIa, or Regulation (EU) 1215/2012) and the 2007 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (2007 Lugano

---

26 Svantesson, Dan, *Enforcing Privacy Across Different Jurisdictions* p. 195-222, in Wright, David & De Hert, Paul (eds.), Enforcing Privacy Regulatory, Legal and Technological Approaches, Springer International Publishing (Online service) 2016 p. 211.

27 Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 258; Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 189 (citing studies showing that low levels of enforcement of data protection rights is due to insufficient funding of DPA); Galetta, Antonella & De Hert, Paul, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, Review of European Administrative Law, Volume 8, number 1/2015 125-151, p. 147.

28 *See* recital 7 Regulation (EU) 679/2016 ("... Natural persons should have control of their own personal data... .").

29 *See* generally Greenstein, Stanley, *Our Humanity Exposed*, Doctoral Thesis in Law and Information technology at Stockholm University 2017 and more specifically p. 396-406 (discussing private enforcement actions by way of collective redress as an aspect of empowerment); Article 29 Data Protection Working Party, *The Future of Privacy*, WP 168, 1 December 2009 p. 3, 15-16.

30 *See* Wiese Schartum, Dag, *Data Protection: Between Paternalism and Autonomy*, in Magnusson Sjöberg, Cecilia & Wahlgren, Peter (ed.), Festskrift till Peter Seipel, Nordstedts Juridik 2006 p. 558.

31 Chapter III Recognition and enforcement Regulation (EU) 1215/2012 and Title III 2007 Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters.

Convention).[32] The Court of Justice for the European Union (CJEU) has defined the scope of the concept "civil and commercial matters" "essentially by the elements which characterize the nature of the legal relationships between the parties to the dispute or the subject-matter thereof."[33] In general, the concept encompasses claims between private parties, and even claims by or against a public authority when it is acting as a private party (i.e. when the public authority is not exercising its public powers).[34] Moreover, the fact that the private right is enforced by a public law enforcement mechanism such as an injunction or fines does not change the characterization of the legal relationship as a "civil or commercial matter."[35] Thus, there should not be any obstacle to one Member (or Lugano) State enforcing a judgment from another Member (or Lugano) State ordering a controller or processor to rectify or erase personal data under penalty of fine.

In addition, judgments resulting from private enforcement actions as opposed to decisions taken by the Member State DPAs, have a greater potential for being recognized and enforced in third countries.[36] The "public law taboo" informs that countries are unlikely to enforce foreign public law measures such as DPA orders and fines. [37] Indeed, states generally have no interest in draining valuable state resources to further foreign governmental interests.[38] The perspective is different however when a private individual asks a foreign court to enforce private rights. In the interest of doing justice for the parties, a judgment enforcing a private law right has a good likelihood of enforcement, provided the enforcing state finds that the originating court had jurisdiction and the judgement does not violate the enforcing state's public policy.

Finally, an advantage with private enforcement actions is that they can result in interpretations of complicated legal rules that can serve as prescriptive guidance

32 Article 1 Regulation (EU) 1215/2012; article 1 2007 Lugano Convention.

33 *See* e.g. Judgment of 11 April 2013, Sapir and others (C-645/11) ECLI:EU:C:2013:228, para. 32.

34 *See* Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 262 (for further references to CJEU case law).

35 *See* Judgment of 18 October 2011, Realchemie Nederland (C-406/09, ECR 2011 p. I-9773) ECLI:EU:C:2011:668, para. 44 (holding that the Brussels Ia Regulation applies to the recognition and enforcement of a decision of a court that contains an order to pay a fine in order to ensure compliance with a judgment given in a civil and commercial matter). *See* e.g. Swedish Supreme Court case, NJA 2000 s. 435 I and II (stating that an injunction in a public law sanction that the parties to the dispute cannot dispose over).

36 Svantesson, Dan, *Enforcing Privacy Across Different Jurisdictions* p. 195-222, in Wright, David & De Hert, Paul (eds.), Enforcing Privacy Regulatory, Legal and Technological Approaches, Springer International Publishing (Online service) 2016 p. 195.

37 *See* Lowenfeld, Andreas F., *Public law in the international arena: conflict of laws, international law, and some suggestions for their interaction*, 163 Recueil des cours Hague 315 1979 p. 322-326 (coining the term "public law taboo").

38 *See* Bogdan, Michael, *Svensk internationell privat- och processrätt*, 8th ed., Stockholm: Nordstedts Juridik 2014 p. 80-81.

to other controllers and processors in similar situations. [39] Bygrave points out that many DPAs rely on "'back-room' negotiations", which can be an obstacle to transparency.[40] Private enforcement actions result in publicized judgments, which play an important role in the development of the law. Moreover, some DPAs have taken a conciliatory stance toward controllers and processors and have acted more as mediators than as advocates.[41] In a private enforcement action, the data subject is in an adversarial position toward the offending controller and processor, and is usually the one with the greatest incentive to pursue the case, thereby leading to the development of the law.

1.3 The GDPR Clarifies the Right to a Direct and Independent Private Enforcement Action

The GDPR clearly envisages the possibility for the data subject to bring a private enforcement action in court directly against the controller or processor. Indeed, the GDPR stipulates, "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation." [42] This right is without prejudice to any administrative remedy that a data subject may have such as the possibility to make a complaint to a national DPA.[43]

A similar right existed already under the Data Protection Directive[44], although the right in the GDPR differs in two respects. First, the GDPR clarifies that it is a right to a private enforcement action directly "against the controller or processor", which is explicitly stated in the heading to article 79 of the GDPR. In contrast, the Data Protection Directive did not explicitly state that the judicial remedy was

39 Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 189.

40 Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 189.

41 Korff, Douwe, *Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, final [extended and re-edited] version, European Commission 2010 p. 101 (stating that the DPAs *see* themselves as conciliators or mediators rather than fierce watchdogs). This conciliatory stance toward controllers and processors may change however under the GDPR with its detailed list of tasks and powers. *See* Chapter VI Regulation (EU) 679/2015.

42 Article 79(1) Regulation (EU) 2016/679 ("Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.").

43 Article 79(1) Regulation (EU) 2016/679.

44 Article 22 Directive 95/46/EC) ("Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.").

against the controller or processor. In fact, one might interpret article 22 of the Data Protection Directive as merely providing a right to a judicial remedy against an administrative decision, such as the right to appeal a decision of a DPA to a judicial authority.[45]

Second, the GDPR suggests that the data subject may bypass the DPA altogether and file a claim directly against the controller or processor. Bygrave observes that Data Protection Directive left it to the Member States to determine whether to require that the data subject exhaust an administrative remedy such as a complaint to a DPA before bringing a claim in court.[46] Indeed, the CJEU recently confirmed that the Data Protection Directive did not exclude the possibility for national law to require that the data subject first exhaust administrative remedies before bringing a court action, provided the administrative remedies comply with article 47 of the EU Charter on the right to an effective remedy.[47]

The GDPR, however, excludes the qualification concerning an administrative remedy "prior to referral to the judicial authority", which appeared in the Data Protection Directive. This exclusion suggests that the data subject can bypass the DPA and take his/her claim directly to court. This qualification "prior to referral to the judicial authority" did not appear in the original or amended Data Protection Directive proposals but appeared for the first time in the Common Position.[48] Bygrave notes that if the final version of the Data Protection Directive had not included the qualification, data subjects would have found it easier to go straight to the courts with their complaints.[49] As the GDPR omits the qualification, a textual interpretation suggests that the GDPR gives a data subject the right to go directly to court with a private enforcement claim without the need to exhaust

45 The right to appeal a decision by a DPA is specifically addressed in article 28(3) Directive 95/46/EC (... "Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.").

46 *See* Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 187 (stating that the Data Protection Directive does not require the Member States to give individuals direct access to the courts for the breach of data protection rights thereby bypassing national DPAs but merely leaves the Member States the possibility to do so).

47 C-73/16, Judgment of 27 September 2017, Puškár (C-73/16) ECLI:EU:C:2017:725, para. 55 ("That directive, which does not contain any provisions governing specifically the conditions under which that remedy may be exercised, does not however exclude the possibility that national law may also establish remedies before the administrative authorities."). The Court held that in order to comply with article 47 of the EU Charter, the limitation on the right to an effective remedy must be provided for by law, respect the essence of the right, and comply with the principle of proportionality. Ibid. para. 62.

48 *See* article 14(8) of the ProposaI for a Council Directive concerning the protection of individuals processing of personal data in relation to the COM (90) 314 final- SYN 287; article 22 of the Amended proposaI for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287 p. 101; article 22 Common Position (EC) No /95 Adopted by the Council on 20 February 1995 with a view to adopting Directive 94/ /EC of the European Parliament and of the Council on the Protection of individuals with regards to the processing of personal data and on the free movement of such data, 12003/3/94 REV 3, Brussels, 3 February 1995.

49 *See* Bygrave, Lee, *Data Privacy Law*, Oxford University Press (Online resource) 2014 p. 187.

other available remedies such as a complaint to a DPA.[50] This interpretation is also consistent with the aim of the GDPR to strengthen the data subject's rights and put the data subject in control of his/her personal data. [51]

1.4 Available Remedies in a Private Enforcement Action

While the GDPR stipulates the right to an effective judicial remedy directly against the controller or processor, it does not dictate the form of remedy that the court may or must provide, apart from the right to compensation.[52] The GDPR is silent on whether a court may issue orders and injunctions to enforce a data subject's rights (e.g. the right to erasure or to rectification) in a private enforcement action.[53] This is in contrast to the public law enforcement of a data subject's rights, where the GDPR specifically grants the DPAs the power to order the rectification or erasure of personal data or restriction of processing.[54]

As noted above, the Data Protection Directive also contained an obligation on the Member States to make a judicial remedy available.[55] Similarly, the Data Protection Directive did not dictate the form of remedies that the Member States must provide for other than that a data subject should have the right to compensation.[56] Beyond that, the Data Protection Directive left it to the Member States to "adopt suitable measures to ensure the full implementation of the provisions of this Directive".[57] This discretion is in keeping with the nature of a directive, which gives the Member States the discretion to choose the measures, including the remedies, when implementing a directive, provided the Member States fulfil the aim of the directive. [58]

One of the criticisms of the Data Protection Directive was however that it allowed for divergence in the rules across Member States, which resulted in a

50 But *see* Advocate General Kokott's opinion, C-73/16, Judgment of 27 September 2017, Puškár (C-73/16) ECLI:EU:C:2017:725, para. 43 (stating that the GDPR "still does not clarify whether the bringing of legal proceedings may be made contingent upon exhaustion of another remedy. All that can be taken from Article 79 of the General Data Protection Regulation is that the judicial remedy must be effective."). The Advocate General was not referring to a remedy before a DPA however but before a competent administrative body. *See* ibid. para. 40.

51 *See* recital 7 Regulation (EU) 679/2016 ("... Natural persons should have control of their own personal data... .").

52 *See* article 82 Regulation (EU) 679/2016 on the right to compensation and liability. *See* also article 82(6) Regulation (EU) 679/2016 (stating that court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)).

53 *See* Chapter III Regulation (EU) 679/2016 on the rights of the data subject.

54 Article 58(2)(g) Regulation (EU) 679/2016

55 Article 22 Directive 95/46/EC.

56 Article 23 Directive 95/46/EC (stipulating that the Member States provide a right to receive compensation for damage suffered as a result of an unlawful processing).

57 Article 24 Directive 95/46/EC.

58 Article 288(3) TFEU.

fragmented legal environment, and created legal uncertainty and uneven protection for individuals.[59] As noted above, there were divergences among Member States with respect to substantive rights and also with respect to remedies and the powers to enforce the rights. Moreover, not only did the paths for an individual to access remedies at the national level in case of a data protection violation vary among the Member States (e.g. DPAs, administrative and judicial courts, non-judicial bodies and other administrative institutions, civil society organizations)[60] but the powers granted to these institutions varied greatly.[61] Indeed, the DPAs' powers to remedy data protection violations, and the extent to which they used them, varied greatly across the EU.[62] Likewise, the powers of the courts in a private enforcement action to remedy a data protection violation varied such that some of the Member States' national laws allowed individuals to claim injunctive relief while other Member States did not allow for this possibility.[63]

---

59 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM (2012) 9 final p. 7.

60 *See* European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* 2014 p. 19.

61 European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* 2014 p. 21 ("DPAs' powers to remedy data protection violations, and the extent to which they use them, vary greatly across the EU.").

62 European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* 2014 p. 21; Galetta, Antonella & De Hert, Paul, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, Review of European Administrative Law, Volume 8, number 1/2015 125-151, p. 136.

63 *See* European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* 2014 p. 22 (stating with respect to available remedies in civil and administrative Procedures before the Member State courts: "In five EU Member States, courts can issue an order demanding that access be granted to specific data; 10 Member States use orders for the controller to rectify, erase or cease the processing of specific data; and in four Member States the courts are able to order that relevant third parties or the public be informed of any violation or subsequent court judgment."). The UK Data Protection Act provided the data subject with a right to bring a claim for an injunction ordering the controller to rectify, block, erase and destroy personal data in a private enforcement action. *See* Section 14 UK Data Protection Act 1998 on Rectification, blocking, erasure and destruction (repealed). *See* e.g. Max Mosely 2015 EWHC 59 (QB) (allowing a claim for an injunction in a private enforcement action for illegal data processing under the UK Act implementing the Data Protection Directive); Hegglin v. Person(S) Unknown, [2014] EWHC 2808 (QB) (same). In contrast, the Swedish Personal Data Act did not explicitly allow for this possibility. The Swedish Act stipulated that the DPA may request an order for erasure before the country administrative court but it did not provide this possibility to the data subject. *See* section 47 Swedish Personal Data Act (1998:204) (repealed) ("The supervisory authority may at the County Administrative Court in the county where the authority is situated apply for the erasure of such personal data as has been processed in an unlawful manner."). The Swedish Act stipulated that a data subject has the right to bring a claim for compensation. *See* section 48 on the right to compensation in the Swedish Personal Data Act (1998:204) (repealed). In the Swedish government's proposal for implementing the Data Protection Directive into Swedish national law, it took the position that Sweden would satisfy the Directive's obligation on the right to a judicial remedy by providing for the right to damages. Regeringens proposition 1997/98:44 Personuppgiftslag

The choice of a regulation as the format for the Data Protection Reform was to "ensure a consistent level of protection for individuals throughout the Union" and to ensure "the same level of legally enforceable rights and obligations and responsibilities for controllers and processors".[64] To address the variations in the DPAs' powers, the GDPR contains a long list of extensive and harmonized powers granted to the DPAs, including the power to order the rectification or erasure of personal data or restriction of processing and detailed rules on imposing administrative fines.[65] With respect to private enforcement actions, the GDPR continues to leave the Member States with discretion with respect to the form of the judicial remedies.[66] The only mandatory remedy stipulated by the GDPR is

(Swedish Government proposal on Personal Data Law) p. 106. *See* also Öman/Lindblom, Personuppgiftslagen: en kommentar 2011 (The Swedish Personal Data Law: A Commentary) p.417 (stating that a data subject can make a complaint to the DPA, which has the possibility to bring an action for a fine if the controller does not rectify the illegal processing or the data subject can bring a private enforcement action in court and demand e.g. damages if the controller has not fulfiled its obligations) and p. 507 (stating that section 48 on compensation in the Swedish Data Protection Act implements and fulfils the obligations in articles 22 and 23 of the Data Protection Directive). This issue cannot be said to be completely settled under Swedish law. *See* Hellgren v. Google Inc., Case nr T 4355-15, Stockholm District Court May 9, 2016 (finding that Google did not breach any data protection rights so it was not necessary to reach the question whether a data subject has the right to bring a claim for erasure in a private enforcement action), appealed on other grounds, Case nr T 4721-16, Svea Court of Appeals, May 5, 2017. *See* also Regeringens proposition 1997/98:44 Personuppgiftslag (Swedish Government proposal on Personal Data Law) p. 86, 132 (stating somewhat ambiguously: "If the data controller and the data subject disagree about whether data is to be corrected or not, the data subject may make a complaint to the DPA, which is able to order fines if the law is not followed and to apply for the deletion of the data (*see* section 13) or to bring a private enforcement action in court." (my translation) "Uppkommer oenighet mellan den personuppgiftsansvarige och den registrerade om uppgifterna skall korrigeras eller inte, kan den registrerade anmäla förhållandet till tillsynsmyndigheten, som har möjlighet att förelägga vite om lagen inte följs och att ansöka om utplånande av uppgifterna (se avsnitt 13), eller själv väcka talan om saken vid allmän domstol."). *See* also Korff, Douwe, Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, final [extended and re-edited] version, European Commission 2010 p. 95 (stating that the Data Protection Directive did not establish the precise form (or forms) that the remedy should take and that the right to compensation should be seen as a minimum requirement).

64 Recital 11 Regulation (EU) 679/2016.

65 *See* article 58 och recital 100 Regulation (EU) 679/2016 ("In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings."). The GDPR obligates the Member States to lay down rules on other penalties for the infringement of the GDPR. Article 84 Regulation (EU) 679/2016.

66 *See* Galetta, Antonella & De Hert, Paul, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, Review of European Administrative Law, Volume 8, number 1/2015 125-151, p. 150-151 (criticizing the GDPR for its lack of efforts to reform court remedies). Article 47 of the EU Charter leaves broad discretion to the Member States to determine the remedies and procedures for enforcing rights under EU law in areas where EU law does not provide for its own remedies and procedures. *See* Chalmers, Damian, Davies, Gareth & Monti, Giorgio,

the right to compensation. Thus, differences among the Member States continue as before the GDPR. For example, under the new Irish Data Protection Act, data subjects who bring a private enforcement action before the courts can obtain both monetary awards and injunctive relief.[67] In contrast, the new Swedish Data Protection Act 2018 does not provide for the possibility of injunctive relief.[68] The Swedish Data Protection Investigation concluded that Sweden fulfils the obligation to provide an effective judicial remedy by giving the data subject the possibility to bring a claim for damages in court.[69] Thus, the form of remedies available to the data subject depends on the applicable national law, which will be determined pursuant to the EU rules on private international law.[70]

European Union Law, 3rd ed., Cambridge University Press 2014 p. 298-305. Article 13 ECHR also provides the contracting states with broad discretion concerning the form of remedy. *See* Smith and Grady v. the United Kingdom, nos. 33985/96 and 33986/96, para. 135 (Article 13 ECHR "guarantees the availability of a remedy at national level to enforce the substance of Convention rights and freedoms in whatever form they may happen to be secured in the domestic legal order. Thus, its effect is to require the provision of a domestic remedy allowing the competent national authority both to deal with the substance of the relevant Convention complaint and to grant appropriate relief. However, Article 13 does not go so far as to require incorporation of the Convention or a particular form of remedy, Contracting States being afforded a margin of appreciation in conforming with their obligations under this provision."). Recital 147 Regulation (EU) 679/2016, which refers to "proceedings seeking a judicial remedy including compensation, against a controller or processor", suggests that compensation is the minimum but that the Member States may grant additional remedies).

67 Section 117(4) (a) Irish Data Protection Act 2018.

68 *See* Lag (2018:218) med kompletterande bestämmelser till EUs dataskyddsförordning (Swedish Law with additional provisions to the EU Data Protection).

69 SOU 2017:39 p. 304.

70 *See* Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) and Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). *See* also Judgment of 28 July 2016, Verein für Konsumenteninformation (C-191/15) ECLI:EU:C:2016:612, para. 60 ("the law applicable to an action for an injunction within the meaning of Directive 2009/22 directed against the use of allegedly unfair contractual terms by an undertaking established in a Member State which concludes contracts in the course of electronic commerce with consumers resident in other Member States, in particular in the State of the court seised, must be determined in accordance with Article 6(1) of the Rome II Regulation, whereas the law applicable to the assessment of a particular contractual term must always be determined pursuant to the Rome I Regulation, whether that assessment is made in an individual action or in a collective action."). *See* also Chen, Jiahong, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*, International Data Privacy Law, Volume 6, Issue 4, 1 November 2016, p. 310–323 (concluding that the solution to the applicable law, at least when it comes to the complementary national rules, should be found in the GDPR itself and not by choice of law rules).

2 Jurisdiction over Private Enforcement Actions before the GDPR

The Data Protection Directive did not contain any rules on the jurisdiction of the Member State courts with respect to jurisdiction over private enforcement actions, or at least not any explicit rules.[71] However, article 4 of the Data Protection Directive explicitly regulated which national law was applicable to the processing of personal data.[72] The main rule was that the applicable law is that of the Member State where the controller has an establishment where the processing is carried out in the context of its activities.[73] When it comes to public law enforcement actions, if a state authority determines that its domestic law is applicable, the authority generally assumes that it is competent to investigate and enforce the law, and the domestic courts are competent to review its rulings.[74] In other words, the cart pulls the horse; the domestic authorities (and courts) have jurisdiction if the national (forum) law is applicable. Generally, if a state authority determines that its domestic law is not applicable, it does not exercise jurisdiction over the matter. Indeed, state authorities do not enforce the public law of a foreign state.[75] The Data Protection Directive was in fact an exception to this general rule as it empowered the national DPAs to exercise their powers on their territories even when the law of another Member State applied.[76]

With respect to private enforcement actions, however, a court's jurisdiction is usually not dependent on the application of forum law.[77] True, one might assume

---

71 *See* Colonna, Liane, *Legal Implications of Data Mining: Assessing the European Union's Data Mining Principles in Light of the United States Government's National Intelligence Data Mining Principles*, Ragulka förlag 2016 p. 340 (raising the question whether article 4 of Directive 95/46/EC governs only applicable law or whether it also governs jurisdiction).

72 Article 4 Directive 95/46/EC.

73 Article 4(1)(a) Directive 95/46/EC.

74 *See* Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179, 16 December 2010 p. 10 (stating that in most cases applicable law and the competence of the national DPA will coincide); Kuner, Christopher, *Data protection law and international jurisdiction on the Internet (Part 1)*, 2010, Vol. 18, Issue 2, International Journal of Law and Information Technology p. 176–193, p. 180. *See* e.g. In the case of Debeuckelaere v. Facebook Inc., Dutch-Speaking Court of First Instance Brussels, Case list number 15/57/C, 9 November 2015) ("... the present case is about the application of Belgian legislation on the Belgian territory... The Belgian judge thus has international jurisdiction to decide on the present claim, and furthermore he applies Belgian legislation in the process."), English translation available at the Belgian Commission for the Protection of Privacy, "www.privacycommission.be/sites/privacycommission/files/documents/Judgement%20Belgian%20Privacy%20Commission%20v.%20Facebook%20-%2009-11-2015.pdf".

75 Kuner, Christopher, *Data protection law and international jurisdiction on the Internet (Part 1)*, 2010, Vol. 18, Issue 2, International Journal of Law and Information Technology p. 176–193, p. 181.

76 *See* article 28(6) Directive 95/46/EC. *See* also Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179, 16 December 2010 p. 10.

77 Korff, Douwe, *Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and

that if a Member State's law were applicable to the dispute, the Member State court would have jurisdiction to hear the private enforcement action. However, interpreting article 4 of the Data Protection Directive as providing an indirect rule on jurisdiction over private enforcement claims would have led to the conclusion that a Member State court did not have jurisdiction in situations where forum law was not the applicable law even though the parties or the dispute otherwise had a close connection to the forum.[78] Such a conclusion was not warranted based merely on an indirect interpretation of article 4 of the Data Protection Directive as it would have had unintended consequences with respect to jurisdiction over private enforcement actions.

The answer to the question concerning jurisdiction over private enforcement actions arising from the Member States' laws implementing the Data Protection Directive had to be found in the Member States' general rules on jurisdiction in private international law.[79] More specifically, these rules are found in the Brussels Ia Regulation, the 2007 Lugano Convention, and in the Member States' national rules on jurisdiction. These rules on jurisdiction in private international law usually allow the claimant to choose between at least two, and in many cases several, possible fora.

From the perspective of a Member State court, the rules on jurisdiction in the Brussels Ia Regulation generally apply when the defendant is domiciled in a Member State, the rules on jurisdiction in the 2007 Lugano Convention apply when the defendant is domiciled in a contracting state to the Lugano Convention (EU, Denmark, Iceland, Norway, Switzerland), and the forum rules apply when the defendant is domiciled in a third state. The rules on jurisdiction in the Brussels Ia Regulation and in the Lugano Convention are basically identical and are to be interpreted in a similar manner.[80] The rules on jurisdiction in the Member States' national law are usually similar to but often more expansive (and sometimes exorbitant) than the rules in the Brussels Ia Regulation and the Lugano

---

Technical Developments, final [extended and re-edited] version, European Commission 2010, New challenges 2010 p. 96 (discussing how the question of applicable law is separate from the question of jurisdiction).

78 *See* Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, 259; Kuner, Christopher, *Transborder data flows and data privacy law*, Oxford University Press (ebook) 2013 p. 121 (stating that the question of jurisdiction, or more specifically adjudicative jurisdiction, has often been conflated with applicable law or prescriptive jurisdiction, especially in the field of data protection law).

79 Dorff, New Challenges 2010 p. 97 (stating that the question of forum and procedure are everywhere basically determined by the ordinary procedural laws (ie the laws on administrative or civil procedure); Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 260 (stating that the Brussels Ia Regulation rules on jurisdiction apply if the proceedings fall within the scope of the Brussels Ia Regulation's definition of civil and commercial matters).

80 Protocol No 2 on the uniform interpretation of the Convention and on the Standing Committee, OJ L 339 p. 27-29.

Convention.[81] The applicable rules on jurisdiction are analyzed below to elucidate what options were available to a data subject before the GDPR, and potentially continue to be available even under the GDPR. For the sake of simplicity, reference is made primarily to the rules in the Brussels Ia Regulation.

2.1 General Jurisdiction

The rules on jurisdiction in the Brussels Ia Regulation are based on the general principle *actor sequitur forum rei*, namely, that a defendant can and shall be sued in his/her place of domicile.[82] Domicile is a basis of general jurisdiction in that a "local" defendant may be sued in its home state with respect to any and all claims regardless of whether the dispute has any connection to the forum state, provided the proceedings do not fall within the exclusive jurisdiction of another Member State. Not only is it possible to bring a private enforcement action under the law of another Member State, but it is also be possible to bring such an action under the law of a third state.

The Brussels Ia Regulation establishes an autonomous definition of the concept of domicile for legal persons, which is statutory seat, central administration or principal place of business.[83] The location of statutory seat is found in the Member State where a legal person is incorporated in accordance with its law, the central administration is the location of the legal person's management and control center (i.e. the real seat), and the principal place of business means where the main business activities are located.[84]

The Brussels Ia Regulation uses the same criteria to define domicile for the purpose of jurisdiction as used in article 54(1) TFEU to determine the nationality of legal persons. The purpose of the definition in article 54(1) TFEU is to determine which legal persons enjoy the right to freedom of establishment within the meaning of article 49 et seq. of the TFEU.[85] The use of the same alternative criteria for the definition of domicile in the Brussels Ia Regulation is to ensure that there are no negative conflicts of jurisdiction where a legal person having a Member State nationality is not considered to be domiciled in any Member

81 Nuyts, Arnaud, *Study on Residual Jurisdiction: Review of the Member States' rules concerning the "Residual Jurisdiction" of their courts in civil and commercial matters pursuant to the Brussels I and II Regulations*, Service contract with the European Commission, JLS/C4/2005/07-30-CE)0040309/00-37, General report, 2007 p. 19-21.

82 Article 4 Regulation (EU) 1215/2012; article 2 2007 Lugano Convention.

83 Article 63(1) Regulation (EU) 1215/2012; article 60(1) 2007 Lugano Convention.

84 Vlas, Paul, *Chapter V: General Provisions*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 994-995.

85 *See* article 54(1) TFEU ("Companies or firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Union shall, for the purposes of this Chapter, be treated in the same way as natural persons who are nationals of Member States.").

State.[86] The broad definition of domicile can lead to positive conflicts of jurisdiction as a legal person that has its statutory seat, central administration, and principal place of business in three different Member States will have three domiciles. Consequently, if an offending controller or processer has its statutory seat, central administration, and principal place of business in three different Member States, a data subject may bring a private enforcement action in any one of those Member states.

2.2 Special Jurisdiction for Matters Relating to Contract

The Brussels Ia Regulation provides for rules on special jurisdiction that allow a defendant to be sued in the forum state even though the defendant is not domiciled there. If the data subject and the offending controller or processor have a contractual relationship, the private enforcement action may be characterized as a matter relating to a contract and the rules on special jurisdiction for contracts in the Brussels Ia Regulation may apply. [87] For example, when purchasing goods or services on-line, a professional consents to the use of his/her personal data for a specific purpose, and the seller subsequently uses the data for other purposes in violation of the contractual consent given by the professional. Regardless of how data protection is characterized under substantive law, for the purpose of jurisdiction, a data protection claim might be characterized as a matter relating to contract where the interpretation of the parties' contract is indispensable to establishing whether the processing of the date is unlawful.[88]

Pursuant to the special rule on contract jurisdiction, jurisdiction lies at the place of performance of the obligation in question. The rule autonomously defines this place to be where, under the contract, the goods were delivered or should have been delivered or where, under the contract, the services were provided or should have been provided.[89] For contracts that cannot be characterized as sale of goods nor provision of services, the forum must first identify the specific obligation in question in the dispute, and then identify its place of performance under the applicable law.[90] In particular, with respect to sales of digitized products, difficulties can arise with respect to whether they can be characterized as sales of goods, provision of services, or a third undefined category. In addition, difficulties can arise in localizing the place of delivery, provision of services, or the place of the performance of the obligation in question. Nevertheless, this basis of

86 Vlas, Paul, *Chapter V: General Provisions*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 994.

87 Article 7(1) Regulation (EU) 1215/2012. *See* also article 5(1) 2007 Lugano Convention.

88 *See* by analogy Judgment of 13 March 2014, Brogsitter (C-548/12) ECLI:EU:C:2014:148, para. 25. *See* also Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 266.

89 Article 7(1)(b) Regulation (EU) 1215/2012; article 5(1)(b) 2007 Lugano Convention.

90 *See* Judgment of 6 October 1976, Industrie tessili italiana / Dunlop AG, ECLI:EU:C:1976:133.

jurisdiction provides the data subject with an alternative to bringing a claim where the offending controller or processor is domiciled.

2.3 Special Jurisdiction over Consumer Contracts

If the data subject concludes a contract for a purpose outside his/her trade or profession with a controller or processor who directs commercial or professional activities in the Member State of the consumer's domicile and the contract falls within the scope of such activities, the data subject may be able to sue in his/her domicile under the special rule on jurisdiction over consumer contracts.[91] The aim of the consumer contract rule in the Brussels Ia Regulation is to protect the consumer as the economically weaker and less experienced party in a contractual relationship rather than to attribute jurisdiction to the court with which the claim has proximity.[92] Thus, if the consumer moves after concluding the contract out of which an action subsequently arises, the consumer would be able to bring a claim in the courts of the Member State of his/her new domicile, provided the controller or processor directs commercial or professional activities to that Member State.[93] It is submitted however that a consumer would not be able to raise a claim in the Member State of his/her former domicile.[94] Indeed, giving the consumer this alternative is irreconcilable with the wording on the article, which refers to the "courts for the place where the consumer is domiciled" and not the court for the place where the consumer was domiciled at the time he/she entered into the contract.[95] Moreover, such interpretation would go beyond what is necessary to protect the consumer as the weaker party to the contract.

For the protective rule on consumer jurisdiction to apply, the data subject and the controller or processor must have concluded a contract.[96] Unlike some states such as the United States, data protection in the EU is not classified under consumer protection law and the fact that data subjects are often in a weaker

91 Article 17(1)(c) Regulation (EU) 1215/2012; article 15(1)(c) 2007 Lugano Convention.

92 *See* Mankowski, Peter & Nielsen, Peter, *Introduction to Articles 17-19,* in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 443-444 (with references to case law).

93 *See* Schlosser, Peter, Report on the Association of the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland to the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters and to the Protocol on its interpretation by the Court of Justice, OJ C 59/71 para. 161 (discussing the somewhat similar provision in the Brussels Convention and concluding that the consumer may sue in the courts of his/her new State of domicile if s/he moves to another Community State after concluding the contract out of which an action subsequently arises).

94 But *see* Mankowski, Peter & Nielsen, Peter, *Introduction to Articles 17-19,* in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 512 (suggesting that the consumer could alternatively bring proceedings in the Member State of his/her former domicile although acknowledging case law to the contrary).

95 Article 18 BIa; article 16 Lugano Convention.

96 Judgment of 28 January 2015, Kolassa (C-375/13) ECLI:EU:C:2015:37, para. 32.

position in relation to many controllers and processors (e.g. Facebook and Google) does not qualify them as consumers.[97] In addition to concluding a contract, the data subject must be acting in a context that can be regarded as being outside his/her trade or profession. [98] The CJEU has interpreted the concept of consumer strictly with respect to dual purpose contracts, that is, contracts that serve both professional and private purposes. The CJEU has stated that the burden of proof lies with the person claiming to be a consumer to show that the business or professional use is only negligible.[99]

The ongoing claim raised by the Austrian law student Schrems against the social media giant Facebook for illegal data processing raised the question whether the status of a consumer can change over time.[100] The question arose because although Schrems opened a Facebook account exclusively for private purposes, his Facebook page was later used to act as a "professional litigant in consumer matters". [101] The CJEU made clear that one's status as a consumer could change over time, in particular with respect to long term social media service contracts.[102] The CJEU stated that "it is necessary, in particular, to take into account, as far as concerns services of a digital social network which are intended to be used over a long period of time, subsequent changes in the use which is made of those services."[103] Thus, the CJEU held that a user of such services may rely on his/her status as a consumer only if the predominately non-professional use of those services, for which the individual initially concluded a contract, has not subsequently become predominately professional.[104]

It is submitted that this ruling is consistent with the text, system and purpose of the rule on protective jurisdiction. Indeed, Article 17 BIa, which determines the scope of application of the provisions on jurisdiction for consumer contracts, refers to "a contract concluded by a person, the consumer", which suggests that the status at the time the contract is concluded is relevant. Article 18(1) BIa, which regulates jurisdiction for claims pursued by the consumer, refers, as noted above, to the "courts for the place where the consumer is domiciled" and not to the courts for the place where the party who was a consumer at the time the contract was entered into is domiciled.[105] Consequently, the relevant time for assessing status is both the time the contract is concluded and the time the action is lodged with the court. The concept "consumer" for the purpose of the protective rule on

97 Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 267.

98 Judgment of 28 January 2015, Kolassa (C-375/13) ECLI:EU:C:2015:37, para. 23.

99 Judgment of 14 September 1999, Gruber (C-249/97, ECR 1999 p. I-5295) ECLI:EU:C:1999:405, para. 46.

100 *See* generally "www.fbclaim.com" for information about the case.

101 Opinion of Advocate General Bobek, Case C-498/16, Schrems, ECLI:EU:C:2017:863, para.3.

102 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 37-38.

103 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 37.

104 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 38.

105 Article 18 Regulation 1215/2012; article 16 2007 Lugano Convention.

jurisdiction must be strictly construed as it is an exception to the general rule on domicile. Requiring the status of consumer to be held at the time of contracting and retained at the time the claim is filed, is consistent with the aim of protecting the weaker party in the contractual relationship without going beyond what is necessary to fulfil this aim. In addition, it preserves the aim of foreseeability and the legitimate expectations of the parties because at the time of contracting, both parties are in a position to know the individual's status as a consumer. At the time that the consumer lodges a claim, s/he is in a position to know whether s/he is a consumer or not and the opposing party is in a position to confirm whether the individual is in fact still a consumer.

The Schrems case also raised the question how the rule on dual purpose contracts should be applied to contracts for social media services. Contracts for services such as Facebook, Instagram, and Twitter are difficult to place in the binary classification of consumer or professional contracts.[106] As the Advocate General observed, individuals often use social network platforms for "personal development and communication" as "an expression of the person and their personality" even when used for self-promotional purposes with a professional impact or purpose.[107] In the Advocate General's view, this type of use would not be considered to be within one's trade or profession as the use is not aimed at generating an immediate commercial effect. On the other hand, the Advocate General observed that social media marketing influencers, 'prosumers' (professional consumers), and community managers often use their personal accounts on social networks in a way that might appear to be private, but that are entirely commercial in nature. In the end, the Advocate General found that it was not necessary to resolve these complex scenarios for the Schrems case as the Advocate General found that Schrems was a consumer at the relevant point in time. While it is easy to agree with the Advocate General that "prosumers" and the like are not consumers for the purpose of jurisdiction, it is not as clear that individuals who use Facebook to promote their professional activities will be consumers under the negligibility burden of proof discussed above.

In the context of this specific case, however, the CJEU ruled that publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of enforcing data protection rights does not mean that the purpose of the (Facebook) contract can be regarded as being outside of one's trade or profession.[108] The CJEU explained that the concept of a "consumer" is defined by contrast to that of an "economic operator" and is distinct from the knowledge and information that the person concerned actually possesses. Thus, neither the expertise which that person may acquire in the field covered by those services nor the assurances given for the purposes of representing the rights and interests of the users of those services can deprive that individual of the status

106 Opinion of Advocate General Bobek, Case C-498/16, Schrems, ECLI:EU:C:2017:863, para. 46-49.

107 Opinion of Advocate General Bobek, Case C-498/16, Schrems, ECLI:EU:C:2017:863, para. 48.

108 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 41.

of a consumer for the purpose of the protective rule of jurisdiction.[109] In other words, Schrems is a consumer, albeit a very knowledgeable and civically engaged one. To hold otherwise, the CJEU noted, would disregard the objective set out in Article 169(1) TFEU of promoting the right of consumers to organize themselves in order to safeguard their interests. [110]

2.4 Special Jurisdiction over Employment Contracts

If the data subject is an employee of the processor or controller and the private enforcement action is related to the individual employment contract, the data subject may be able to sue the controller or processer in the place where the data subject habitually carries out his/her work.[111] An example might be where a data subject alleges that the employer has illegally monitored the employee's conduct or performance at the workplace using information technology systems. The criterion "matters relating to individual contracts of employment", which is a prerequisite for the application of the special rules on employment jurisdiction, is broad enough to encompass non-contractual data protection claims arising under the data protection law and not only claims for the breach of the employment contract.[112] The rules on special jurisdiction over individual employment contracts aim to protect the employee as the weaker party in the contractual relationship. Pursuant to these rules, the employee can bring proceedings against the employer in the Member State of the employer's domicile or in the Member State where the employee habitually carries out his/her work. The employer however can bring a claim against the employee only in the Member State of the employee's domicile.[113]

A reason for providing the employee with this alternative is that it is likely to be less expensive for the employee to commence court proceedings in the Member

109 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 39.

110 Judgment of 25 January 2018, Schrems (C-498/16) ECLI:EU:C:2018:37, para. 40.

111 Article 21(1)(b)(i) Regulation (EU) 1215/2012. If the employee did not habitually carry out his/her work in any one country, an action may be brought in the courts for the place where the business that engaged the employee is situated. *See* article 21(1)(b)(ii) Regulation (EU) 1215/2012. The rule on habitual residence is given such an extensive interpretation that the rule on where the business is engaged is only applicable to very special cases where the work is carried out on a territory that does not belong to any one state. *See* Sinander, Eric, *Internationell kollektivavtalsreglering: En studie i internationell privaträtt av den svenska modellen för reglering av anställningsvillkor*, Doctoral Thesis in Private law at Stockholm University 2017 p. 112-114.

112 *See* Judgment of 10 September 2015, Holterman Ferho Exploitatie and others (C-47/14) ECLI:EU:C:2015:574, para. 49 (holding that employer could not base tort claim against former employee under the tort jurisdiction rule because these claims fell within the scope of the protective rule on individual employment contracts). *See* also Sinander, Eric, *Internationell kollektivavtalsreglering: En studie i internationell privaträtt av den svenska modellen för reglering av anställningsvillkor*, Doctoral Thesis in Private law at Stockholm University 2017 p. 105-106.

113 *See* section 5 Regulation (EU) 1215/2012. There is also a limited possibility for party autonomy.

State where the employee habitually carries out his/her work than it would be to bring proceedings at the employer's Member State of domicile.[114] This alternative is based also on the proximity of the proceedings to this Member State as the law of the Member State where the employee habitually carries out his/her work will generally be the applicable law to contract claims and also applicable as mandatory rules protecting employees.[115] It is also reasonable and foreseeable from the employer's perspective that it is sued there as the employer decides where the employee shall carry out his/her work.[116]

2.5 Special Jurisdiction for Matters Relating to Tort, Delict, or Quasi Delict

If the data subject and the offending controller or processor do not have a contractual relationship, the private enforcement action may be characterized as an action in tort and the special rule on tort jurisdiction will apply. An example is where a controller domiciled in another Member State collects personal information about the visitors to the controller's website without their consent.[117] The rule on tort jurisdiction attribute jurisdiction to the Member State where the harmful event occurred.[118] Pursuant to established CJEU case law, this concept includes the place of the event giving rise to the damage and the place where the damages occurs.[119]

While the CJEU has not interpreted the application of this basis for jurisdiction specifically to data protection claims, it has interpreted the basis with respect to claims for the infringement of personality rights, which are similar to or encompass data protection rights as both rights protect the integrity of the individual.[120] When it comes to infringements of personality rights taking place

114 Judgment of 13 July 1993, Mulox IBC / Geels (C-125/92) ECLI:EU:C:1993:306, para. 19.

115 Judgment of 13 July 1993, Mulox IBC / Geels (C-125/92) ECLI:EU:C:1993:306, para. 15. *See* article 8 Regulation (EC) No 593/2008 (regulating the applicable law). *See* also article 88 Regulation (EU) No 679/2016 On Processing in the context of employment.

116 Mota, Carlos Esplugues & Moreno, Guillermo Palao, *Section 5: Jurisdiction over individual contracts of employment*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 545.

117 *See* e.g. In the case of Debeuckelaere v. Facebook Inc., Dutch-Speaking Court of First Instance Brussels, Case list number 15/57/C, 9 November 2015 (where Facebook Ireland was alleged to have collected information via cookies from Belgian internet users that visited Facebook's website). The Belgium DPA brought the case.

118 Article 7(2) Regulation (EU) 1215/2012; article 5(3) 2007 Lugano Convention. *See* e.g. Chapter 10, section 8 Swedish Code of Judicial Procedure.

119 *See* e.g. Case C-68/93, Judgment of 7 March 1995, Shevill and others / Presse Alliance, ECLI:EU:C:1995:61.

120 *See* Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 270. *See* also Hellner, Michael, Rom II-Förordningen: tillämplig lag för utomobligatoriska

over the internet, the CJEU has held that a victim may bring an action where the defendant is established, where the victim has his/her center of interests, or where the offending content is or has been accessible. [121] Each of these three heads of jurisdiction will be discussed below.

2.5.1 The defendant's establishment

As noted, the tort rule on jurisdiction establishes jurisdiction at the place of the event giving rise to the damage. In the cases applying this rule to infringements of personality rights, the CJEU has localized this place to where the defendant has its establishment.[122] The CJEU reasoned that this place is at the origin of the harm because it is where the defendant makes the decision to carry out the act that causes damage.[123] The reason for attributing jurisdiction to this place is that due to its proximity to evidence, it facilitates the sound administration of justice.[124] One cannot exclude the possibility that the harmful act could be localized at the place of the actual processing of the data when the decision about the processing is taken in another Member State or third state.[125] This might be the case if the data subject brings an action against the processer, because attributing jurisdiction at the place of the actual processing would facilitate the gathering of evidence and the efficient conduct of the proceedings, provided this place was known to the parties and therefore foreseeable.

The CJEU has not defined the concept of establishment for the purpose of jurisdiction under the special rule on tort jurisdiction. As noted, the concept of establishment is found in the TFEU setting forth the right to an establishment in other Member States.[126] Pursuant to established CJEU case law, the concept of establishment means "the actual pursuit of an economic activity through a fixed

förpliktelser, Stockholm: Nordstedts Juridik 2014 p. 66 (discussing the concept of personality rights in the Rome II Regulation and concluding that data breaches are included).

121 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685.

122 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685.

123 Case C-523/10, Judgment of 19 April 2012, Wintersteiger, ECLI:EU:C:2012:220, para. 37. Wintersteiger is a trademark case but the reasoning with respect to the event giving rise to the damage is applicable to personality rights.

124 Case C-523/10, Judgment of 19 April 2012, Wintersteiger, ECLI:EU:C:2012:220, para. 32, 33, 37.

125 *See* by analogy Case C-45/13, Judgment of 16 January 2014, Kainz, ECLI:EU:C:2014:7, para. 26-27 (stating that in a product liability case, the harmful act is the place where the product is manufactured because this facilitates the possibility of gathering evidence in order to establish the defect in question).

126 Articles 49-55 TFEU.

establishment in another Member State for an indefinite period."[127] Nevertheless, the CJEU has given the concept of establishment a very broad interpretation. In a recent case, the CJEU held that freedom of establishment extends to a situation where a company transfers its statutory seat to another Member State even though that company conducts its main, if not entire, business in the first Member State.[128] Thus, it is submitted that statutory seat, central administration, and principal place of business could all qualify as an establishment under the CJEU's interpretation of article 7(2), and the harmful act could be localized there if such establishment was at the origin of the harm. It is important to remember, however, that jurisdiction always lies with the Member State where the defendant has its statutory seat, central administration, or principal place of business based on domicile.

It is submitted, however, that the concept of establishment as used by the CJEU for the purpose of establishing tort jurisdiction is broader than the concept of domicile in the Brussel Ia Regulation. Indeed, the act that causes the damage might be localized at an establishment that is not the statutory seat, central administration, or principal place of business. For example, the decision to process a data subject's data might be taken at the controller's secondary establishment, which does not qualify as domicile. Likewise, the actual data processing might take place at a processor's secondary establishment.

If the defendant has a secondary establishment in another Member State, another rule on special jurisdiction based on an establishment may provide a basis for jurisdiction without any need to resort to the special rule on tort jurisdiction.[129] Article 7(5) BIa establishes jurisdiction "as regards a dispute arising out of the operations of a branch, agency or other establishment, in the courts for the place in which the branch, agency or other establishment is situated."[130] However, the CJEU has defined the concept of establishment for the purpose of article 7(5) BIa more restrictively than it has under TFEU in that an establishment under article 7(5) must be materially equipped to negotiate business with third parties.[131]

---

127 C-221/89, Judgment of 25 July 1991, The Queen / Secretary of State for Transport, ex parte Factortame, ECLI:EU:C:1991:320, para. 20; C-246/89, Judgment of 4 October 1991, Commission v United Kingdom, EU:C:1991:375, para. 21.

128 Judgment of 25 October 2017, POLBUD - WYKONAWSTWO (C-106/16) ECLI:EU:C:2017:804, para. 38 ("[] a situation in which a company formed in accordance with the legislation of one Member State wants to convert itself into a company under the law of another Member State, with due regard to the test applied by the second Member State in order to determine the connection of a company to its national legal order, falls within the scope of freedom of establishment, even though that company conducts its main, if not entire, business in the first Member State.").

129 *See* Mankowski, Peter, *Section 2: Special jurisdiction*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 359 (stating that in the majority of cases, the place of establishment under article 7(5) BIa will coincide with the place of the harmful act under 7(2) BIa).

130 *See* also article 5(5) 2007 Lugano Convention; Chapter 10, section 5 Swedish Code of Judicial Procedure.

131 *See* Judgment of 22 November 1978, Somafer SA / Saar-Ferngas AG (33/78) ECLI:EU:C:1978:205, para. 12 (defining establishment in article 7(5) BIa as "a place of business which

Consequently, it might be easier to fulfil the criteria for an establishment that is at the origin of the harm in article 7(2) than the criteria for an establishment in article 7(5) BIa. Thus, the possibility to bring a direct enforcement action at the place of the harmful act localized at the defendant's (secondary) establishment would give a data subject an additional forum beyond the fora located in Member State(s) of the defendant's domicile.

2.5.2 The victim's center of interests

As noted, the rule on tort jurisdiction establishes jurisdiction at the place where the damage arises. Pursuant to the CJEU's interpretation of this concept with respect to infringements of personality rights taking place on the internet, a victim may bring an action where s/he has his/her center of interests. [132] The reason for the attribution of jurisdiction is that this court is best placed to assess the impact that material placed online is liable to have on an individual's personality rights, thereby facilitating the sound administration of justice. [133] In addition, the establishment of jurisdiction at the victim's center of interest fulfils the objectives of legal certainty and foreseeability because the criterion allows both the victim easily to identify the court in which s/he may sue and the defendant reasonably to foresee before which court it may be sued. [134]

According to the CJEU, the victim's center of interests will usually be localized at his/her habitual residence. [135] The CJEU observes however that a victim may also have his/her center of interests in the Member State where he/she pursues a

---

has the appearance of permanency, such as the extension of a parent body, has a management and is materially equipped to negotiate business with third parties so that the latter, although knowing that there will if necessary be a legal link with the parent body, the head office of which is abroad, do not have to deal directly with such parent body but may transact business at the place of the business constituting the extension."). *See* also Mankowski, Peter, *Section 2: Special jurisdiction*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 352 (stating that an establishment under article 7(5) BIa must be used for external business on the market).

132 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685. *See* also Korff, Douwe, *Comparative Study on the Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*, Working Paper No. 2: Data Protection Laws in the EU. The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, final [extended and re-edited] version, European Commission 2010 p. 96 (stating that in practice, the Member State national courts have assumed jurisdiction over actions against foreign controllers that allegedly cause damage to claimants who are residents of the state where the court sits).

133 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 48.

134 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 50.

135 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 49.

professional activity if that activity establishes a particularly close link with the forum state.[136] While the CJEU does not explicitly state so, it seems logical to assume that it is the victim's center of interests at the time that the victim's personality rights are infringed and not the time when the victim lodges a claim with the court. The aim of the rule of special jurisdiction in matters relating to tort is not to protect the weaker party but to determine the Member State whose courts are best able to hear and to rule upon the dispute.[137] The Member State in which the victim acquires a new center of interests would not be best placed to assess the impact that the damaging material had on the victim's personality rights in the Member State of his/her original center of interests. In addition, it is submitted that attributing jurisdiction at the Member State of the victim's new center of interests does not fulfil the objective of foreseeability because the defendant cannot reasonably foresee where the victim might establish a new center of interest.

As noted, the CJEU has not interpreted the application of the center of interest basis for jurisdiction specifically to data protection claims. Like personality rights, however, data protection protects the integrity of the individual.[138] In a similar way to personality right violations, the damage caused to an individual as a result of illegal data processing would be felt most keenly at the individual's center of interests at the time of the illegal data processing. Thus, the tort rule should be interpreted as allowing a data subject to bring a private enforcement action at his/her original center of interest, which might be located in a different Member State from where the data subject has his/her current habitual residence at the time when the action is filed. This basis of jurisdiction is an alternative to bringing a claim where the offending controller or processor is domiciled or has an establishment.

2.5.3 Where the content has been accessible

The CJEU has held that damage arising from the infringement of personality rights taking place over the internet can also be localized in any Member State where the infringing content has been accessible on the internet.[139] Pursuant to the CJEU's case law, it is not necessary that the content has been directed to or targeted at the forum Member State.[140] Indeed, unlike the rule on jurisdiction over consumer

136 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 49.

137 Judgment of 17 October 2017, Bolagsupplysningen and Ilsjan (C-194/16) ECLI:EU:C:2017:766, para. 39.

138 *See* Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 270. *See* also Hellner 2014 p. 66 (discussing the concept of personality rights in the Rome II Regulation and concluding that data breaches are included).

139 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 51.

140 Judgment of 22 January 2015, Hejduk (C-441/13) ECLI:EU:C:2015:28, para. 32; Judgment of 3 October 2013, Pinckney (C-170/12) ECLI:EU:C:2013:635, para. 42 (observing that

contract claims, the rule on tort jurisdiction in the Brussels Ia Regulation does not contain a requirement that explicitly requires the activity to be "directed to" the forum Member State.[141] It is sufficient that the plaintiff has a right in the forum Member State that is capable of being infringed there.[142] The jurisdiction of these courts is limited however only to damage arising in the forum territory.[143] Notwithstanding these limitations on the court's jurisdiction, the possibility to sue in any Member State court where content has been accessible provides the claimant with significant possibilities to forum shop.

Again, the CJEU has not interpreted the application of this basis for jurisdiction specifically to data protection claims. However, if the illegal data processing involves making personal data accessible on the internet, it seems likely that the data subject, in a similar way to personality right violations, could bring a claim in any Member State where the his/her personal data is or has been accessible, for the damage arising in the forum Member State.

As noted, the rules on jurisdiction in the Member States' national laws, while similar, are often more expansive than the rules in the Brussels Ia Regulation.[144] In a case from the United Kingdom (UK), a data subject resident in Hong Kong but with very close connections to the UK brought a claim against Google Inc. and unknown persons who had allegedly published offending content on the internet. [145] As Google is domiciled in the United States, the UK court applied its national rules to establish jurisdiction over Google. Applying the national rule on tort jurisdiction, the UK court found that there was damage in the UK because the data subject had business interests and a home in the UK and the offending content on the internet risked damaging the data subject's reputation in the UK.[146] In this case, the data subject requested an injunction against Google requiring it to block specific sites. The court found that the national rule on injunction jurisdiction also supported the UK court's jurisdiction because there was a good arguable case that Google had an obligation enforceable in the UK to comply with the UK Data

---

unlike the basis for special jurisdiction concerning consumer contracts, the rule on special jurisdiction over tort does not require that the activity concerned to be 'directed to' the Member State in which the court seised is situated).

141 Compare article 17(1)(c) Regulation (EU) 1215/2012.

142 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 51.

143 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 51.

144 Nuyts, Arnaud, *Study on Residual Jurisdiction: Review of the Member States' rules concerning the "Residual Jurisdiction" of their courts in civil and commercial matters pursuant to the Brussels I and II Regulations*, Service contract with the European Commission, JLS/C4/2005/07-30-CE)0040309/00-37, General report, 2007p. 19-21.

145 Hegglin v. Person(s) Unknown, [2014] EWHC 2808 (QB).

146 *See* also Vidal-Hall v Google 2014 EWHC 13 (QB) (finding that the court had jurisdiction under its national tort jurisdiction rule because personal data was published in the UK when it was accessible on the plaintiffs' computer screen where it was seen by them and potentially by third parties).

Protection Act, both when hosting a website on which data appeared and when operating the search engine google.co.uk on which data is processed.

2.5.4 Scope of jurisdiction

The scope of the national court's jurisdiction at the defendant's establishment and at the victim's center of interest encompasses the jurisdiction to make an order for the rectification and/or removal of the content and to rule on the entirety of the damage.[147] In contrast, the scope of jurisdiction where content is accessible on the internet is limited only to damage arising in the forum territory.[148] In addition, these courts are not competent to rule on the rectification and/or removal of the information with effect for the other Member States.[149]

The scope of a Member State court's jurisdiction under its national rules including the rule on tort jurisdiction based on damage in the territory, is not necessarily limited to the territory of the forum state.[150] In the UK case discussed above, the court specifically held that the scope of the injunction was an issue left for trial, suggesting that the court did not exclude the possibility to grant cross-border injunctive relief.[151]

2.6 Prorogation of Jurisdiction and Exclusive Jurisdiction

The Brussels Ia Regulation allows parties to agree that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship.[152] This provision recognizes the parties' autonomy to dispose over procedural matters.[153] The parties may also tacitly agree on a forum by one party starting proceedings and the other party entering an appearance.[154]

147 Judgment of 17 October 2017, Bolagsupplysningen and Ilsjan (C-194/16) ECLI:EU: C:2017: 766, para. 48-49.

148 *See* Joined cases C-509/09 and C-161/10, Judgment of 25 October 2011, eDate Advertising and others, ECLI:EU:C:2011:685, para. 51.

149 Judgment of 17 October 2017, Bolagsupplysningen and Ilsjan (C-194/16) ECLI:EU: C:2017: 766, para. 49.

150 Lundstedt, *Territoriality in Intellectual Property Law*, Doctoral Thesis in Private law at Stockholm University 2016 p. 211-212.

151 Hegglin v. Person(s) Unknown, [2014] EWHC 2808 (QB).

152 Article 25 Regulation (EU) 1215/2012; article 23 2007 Lugano Convention; Chapter 10, section 16 Swedish Code of Judicial Procedure.

153 Magnus, Ulrich, *Section 7: Prorogation of jurisdiction*, in Magnus, Ulrich & Mankowski, Peter (ed.), Brussels Ibis Regulation, European Commentaries on Private International Law, Cologne: Otto Schmidt 2016 p. 583.

154 Article 26 Regulation (EU) 1215/2012; article 24 2007 Lugano Convention; Chapter 10, section 18 Swedish Code of Judicial Procedure.

Party autonomy is limited however with respect to consumer contracts and employment contracts. That is, prorogation agreements between consumers and professionals, and between employees and employers, are only enforceable if the parties enter into them after the dispute has arisen or if they give the consumer or employee more choices with respect to the forum in which s/he can bring proceedings.[155] In addition, party autonomy is excluded if the courts of another Member State have exclusive jurisdiction as discussed below.

The Brussels Ia Regulation contains rules on exclusive jurisdiction for matters where the subject matter of the dispute is closely linked to a Member State.[156] These rules give exclusive jurisdiction to the Member State, e.g. where a legal person has its seat, for proceedings that have as their object the validity of the constitution, the nullity or the dissolution of legal persons, or the validity of the decisions of their organs.[157] For example, if a data subject's personal data is illegally processed in connection with a decision by the board of directors of a corporation and the illegal processing affects the validity of the decision, the Member State where the corporation has its seat would have exclusive jurisdiction over proceedings concerning the validity of the decision. Depending on the relationship between the question concerning invalidity of a decision and the question concerning the illegality of the data processing, the Member State where the legal person has its seat may or may not have exclusive jurisdiction over the data protection claim.[158] That is, if the illegality of the data processing would be an essential premise to the question of the legality of the decision, the Member State where the legal person has its seat would arguably have exclusive jurisdiction. The situation would be different if one of the questions was merely incidental to the other.

2.7 Multiple Defendants

If the data subject brings a private enforcement action against two or more controllers for data protection claims that are closely connected, the data subject may be able to bring the action against both controllers in the Member State where any one of them is domiciled.[159] The purpose of this rule, which is found in article 8(1) Bia, is "to facilitate the sound administration of justice, to minimize the possibility of concurrent proceedings and thus to avoid irreconcilable outcomes if cases are decided separately."[160] To the extent that this rule continues to be applicable even after the GDPR begins to apply, this would be a basis for

155 Article 19 and article 22 Regulation (EU) 1215/2012.

156 Articles 24 Regulation (EU) 1215/2012; article 22 2007 Lugano Convention; section 10:12 Swedish Code of Judicial Procedure.

157 Article 24(2) Regulation (EU) 1215/2012; article 22(2) 2007 Lugano Convention.

158 Compare Judgment of 12 May 2011, BVG, ECLI:EU:C:2011:300 with Judgment of 13 July 2006, GAT, ECLI:EU:C:2006:457.

159 Article 8(1) Regulation (EU) 1215/2012; article 6(1) 2007 Lugano Convention.

160 Painer, C 145/10 (referring to recitals in the preamble to Brussels Ia Regulation).

cumulating an action against a controller and its processor domiciled in different Member States in either of those Member States. Indeed, an important novelty under the GDPR is that the processor can be held directly liable for its obligations under the GDPR and for failing to obey the controller's lawful instructions.[161]

2.8 Summary

The rules on jurisdiction in the Brussel Ia Regulation provide the data subject with a wide number of alternative fora in addition to the Member State of the controller or processor's domicile. Depending on how the data subject's claim is characterized, a private enforcement action might be brought in a Member State where the contractual obligation that was breached was performed, where the controller or processor commits a harmful act that leads to the illegal data processing, where the data alleged to have been illegally processed has been accessible on the internet, or where the data subject had his/her center of interests when the illegal data processing occurred. In weaker party contracts disputes such as where the data subject is a consumer or an employee, the data subject may be able to bring the private enforcement action in his/her Member State of domicile or where s/he habitually carried out his/her duties. In cases of multiple defendants, the data subject has the possibility to cumulate actions against all defendants in the Member State where one of them is domiciled. The parties are also allowed to agree to bring the dispute in a different Member State other than the Member State having jurisdiction under the Brussels Ia Regulation, although this option is somewhat restricted with respect to consumer and employment contracts. The bases of jurisdiction do not apply if the illegality of the data processing is a matter over which another Member State has exclusive jurisdiction.

3 Jurisdiction over Private Enforcement Actions under the GDPR

Unlike the Data Protection Directive, the GDPR contains specific rules on the jurisdiction of the Member State courts to adjudicate claims against a controller or processor for the infringement of a data subject's rights under the GDPR. Article 79(2) GDPR allows the data subject to bring his/her private enforcement action in the Member State where the controller or processor has an establishment, or alternatively in the Member State where the data subject has his or her habitual residence.[162]

---

161 Voigt Paul, von dem Bussche Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer Link 2017, p. 207.

162 Article 79(2) Regulation (EU) 2016/679 ("Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."). *See* also recital 145 Regulation (EU) 2016/679 ("For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the

The jurisdiction granted under the GDPR is limited *ratione materiae* to data protection claims arising from rights under the GDPR.[163] In other words, the Member State court has jurisdiction only if the data subject asserts a claim where the GDPR will be the applicable law (again the cart is pulling the horse). In order for a controller or processor's activities to fall within the territorial scope of application of the GDPR in the first place, the controller or processor must fulfil one of the criteria in article 3 GDPR. The first criterion stipulates that "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." [164] Thus, a prerequisite for the application of the GDPR under this rule is that the processing of personal data take place in the context of the activities of a controller or a processor's EU based establishment. Article 3(1) GDPR does not encompass controllers and processors having an establishment in the EU if the processing of personal data does not take place in the context of at least one of its EU establishments' activities. One could imagine a scenario where a company is domiciled in a third state and processes data in a third state in the context of its activities there but which has an EU establishment for another division of its business that is wholly unrelated to the processing activities. This controller would not fall within the territorial scope of the GDPR under article 3(1) GDPR.

The criterion "in the context of the activities" however, appears to be relatively easy to satisfy provided there is some minimal connection between the controller or processer's processing and its EU based establishment's activities. A similar criterion existed in the Data Base Directive.[165] When interpreting that Directive, the CJEU interpreted the criterion broadly to mean that the processing of personal data takes place in the context of the EU based establishment's activities if the activities of the controller and its establishment are "inextricably linked."[166] In the Google Spain case, the CJEU held that the activities of a search engine and those of its establishment are inextricably linked when the activities relating to the selling of advertising space constitute the means of rendering the search engine at

courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.").

163 *See* article 79(1) Regulation (EU) 2016/679 (establishing "the right to an effective judicial remedy where he or she considers that his or her rights *under this Regulation* have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation." (Emphasis added)).

164 Article 3(1) Regulation (EU) 2016/679.

165 *See* article 4(1)(a) Directive 95/46/EC ("Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;").

166 Judgment of 13 May 2014, Google Spain and Google (C-131/12) ECLI:EU:C:2014:317, para. 56.

issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.[167]

If the controller or processor does not have an establishment in the EU which fulfils the criterion "in the context of the activities" in article 3(1) GDPR, the second criterion in article 3(2) GDPR may apply. Article 3(2) GDPR applies where the controller or processor does not have any or only an "irrelevant" establishment in the EU, that is, where the data processing is not carried out in the context of the EU based establishment. [168] Pursuant to article 3(2) GDPR, the GDPR applies to a controller or processor not having a relevant establishment in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of their behavior as far as their behavior takes place within the EU.[169]

It is submitted that claims arising under the complementary provisions of the national data protection laws are also encompassed by the *ratione materiae* of article 79(2) GDPR. Rights arising under these national laws can be said to arise under the GDPR as the GDPR authorizes the Member States to adopt their own national data protection rules under specific circumstances set out in the GDPR.[170] Moreover, the right to compensation under the GDPR includes damage suffered due to processing that infringes the complementary national data protection laws adopted in accordance with the GDPR.[171] In contrast, claims arising under the law of a third state would be outside the scope of the court's jurisdiction under the GDPR, as rights arising under third state law cannot be said to be rights arising under the GDPR. In such cases, however, the general rules on jurisdiction in the Brussels Ia Regulation, 2007 Lugano Convention, or the national Member State's rules on jurisdiction might be available. The two bases of jurisdiction in the GDPR

167 Judgment of 13 May 2014, Google Spain and Google (C-131/12) ECLI:EU:C:2014:317, para. 56-60.

168 Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, WP 179, 16 December 2010 p. 17-19 (making a similar analysis under the Data Protection Directive).

169 A third criterion in article 3(3) Regulation (EU) 2016/679 states: ("This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.").

170 *See* generally Wagner, J. & Benecke, A., *National Legislation within the Framework of the GDPR: Limits and Opportunities of the Member State Data Protection Law*, European Data Protection Law Review, Volume 2, issue 3 2016 p. 353 – 361. But *see* Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 25 (stating that the wording of article 79(1) GDPR suggests that the jurisdictional grounds in article 79(2) only apply when the GDPR as such is violated and not the complementary provisions of national law).

171 *See* recital 146 Regulation (EU) 2016/679 ("The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation.... Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation."). *See* also Regeringens proposition 2017/18:105 Ny dataskyddslag (Swedish Government proposal on a new data protection law) p. 148-150.

for data subjects wishing to enforce their data protection rights under the GDPR will be discussed below.

3.1 The Controller or Processor's Establishment

As noted, a data subject may bring a data protection claim in the Member State where the controller or processor has an establishment. Article 4 of the GDPR contains a long list of definitions but the concept of establishment is not included among them. Nevertheless, recital 22 of the GDPR states: "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."[172] Identical language appeared in recital 19 of the Data Protection Directive. [173] This definition is based on the CJEU's definition of establishment under the TFEU, which as noted is quite broad. The CJEU has also given the concept of establishment in the Data Protection Directive a very extensive interpretation.[174] While it is clear that the mere accessibility of a website in a Member State is not sufficient for an establishment, the CJEU has suggested that an establishment can be based on a virtual presence in a Member State when that presence satisfies the criteria of an effective and real exercise of activity through stable arrangements.[175]

The rule in article 79(2) GDPR attributing jurisdiction to the Member State where the controller or processor has "an establishment" does not contain any qualifications apart from that there is an EU based establishment. Indeed, article 79(2) does not contain any stipulation that the data subject must bring the claim in the Member State of the controller or processor's establishment that processes personal data in the context of its activities. Thus, provided the controller or processor's activities fall within one of the criteria defining the territorial scope of the GDPR, a literal interpretation of the text of article 79(2) GDPR would allow a data subject to bring proceedings in any Member State where the controller or processor has an establishment, even if the allegedly illegal data processing activities are wholly unrelated to the establishment.[176] Revolidis argues that the concept of establishment in article 79(2) GDPR should be interpreted in the same way as in article 3 GDPR, that is, to mean an establishment whose activities are

172 Recital 22 Regulation (EU) 2016/679.

173 *See* Recital 19 Directive 95/46/EC.

174 Judgment of 1 October 2015, Weltimmo (C-230/14) ECLI:EU:C:2015:639, para. 31 ("the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one — exercised through stable arrangements.").

175 Judgment of 28 July 2016, Verein für Konsumenteninformation (C-191/15) ECLI:EU:C:2016:612, para. 75-77, 80.

176 *See* Voigt Paul, von dem Bussche Axel, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer Link 2017, p. 216 (stating that "where an entity has several establishments in different EU Member States, the data subject can choose whichever of these EU Member States' courts shall be competent.").

inextricably linked to the data processing.[177] However, as Revolidis rightly states, even with this qualification, the data subject will be able to bring an action where there is an establishment with a minimal connection, which could lead to extensive forum shopping. [178] In his view, allowing jurisdiction based on such a weak connection can undermine the mutual trust among Member States and potentially disrupt the circulation of judgments under the Brussels Ia Regulation and the 2007 Lugano Convention.[179]

A more restrictive way to qualify the concept of establishment in article 79(2) GDPR when a controller or processor has establishments in more than one Member State, would be to make an analogy to article 56 GDPR, which grants special competence to the DPA where the controller or processor has its "main establishment".[180] Article 4(16) GDPR defines the main establishment to be the Member State where the processor or controller has its central administration.[181] If another establishment of the controller in the EU decides on the purposes and means of the processing of personal data and has the power to have such decisions implemented, this establishment is considered the controller's main establishment.[182] In addition, if a processor has no central administration in the EU, its main establishment is defined as its establishment in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.[183]

As noted, the text of article 79(2) GDPR does not contain any qualification and the question can be raised whether one should read a "main establishment" criterion into article 79(2) GDPR.[184] Nevertheless, a teleological interpretation would provide greater legal certainty for the economic operator and data subjects, and thereby fulfil one of the primary objectives of the GDPR.[185] Moreover, although this interpretation limits the data subject's ability to forum shop among

177 Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 27.

178 Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 27.

179 Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 27.

180 *See* article 56 Regulation (EU) 679/2016.

181 Article 4(16) Regulation (EU) 2016/679.

182 Article 4(16)(a) Regulation (EU) 2016/679.

183 Article 4(16)(b) Regulation (EU) 2016/679.

184 Indeed, when the EU legislature intended to specify the main establishment, it knew how to do so. *See* article 56 Regulation 679/2016 defining the DPA in the Member State where the controller or processor has its "main establishment" as the "lead supervisory authority" among the national DPAs for investigations concerning illegal cross-border processing.

185 *See* Chalmers, Damian, Davies, Gareth & Monti, Giorgio, *European Union Law*, 3rd ed., Cambridge University Press 2014 p. 176-77.

different Member States where a controller or processor has establishments, the data subject still has the possibility to bring an action in the Member State where the data subject is habitually resident, which is sufficient to protect the data subject's rights. If the controller has its central administration outside the EU and the decisions on the purposes and means of the processing are taken outside the EU, but it has more than one establishment in the EU, it is submitted that jurisdiction should lie with the establishment in the EU that has the greatest link to the data processing.

3.2 The Data Subject's Habitual Residence

As an alternative, article 79(2) GDPR provides that a data subject may bring a private enforcement action in the Member State where the data subject has his or her habitual residence.[186] The alternative to bring proceedings where the data subject has his/her habitual residence should be seen as a rule of protective jurisdiction and be understood as a measure to strengthen the data subject's rights.[187] It is submitted that this rule must be understood to mean the habitual residence of the data subject at the time s/he starts proceedings and not the habitual residence at the time the data is illegally processed. Indeed, the text of article 79(2) GDPR refers to the courts of the Member State where the data subject has his or her habitual residence and not the Member State where the data subject had his or her habitual residence at the time of the illegal data processing. This interpretation also serves the aim of the GDPR to protect the data subject. Indeed, it is more convenient for a data subject to bring a claim at the place of his/her current habitual residence as opposed to his/her former habitual residence. It should be noted that this basis for jurisdiction does not include a targeting ("directs such activities to") requirement like the rule on special jurisdiction over consumer contracts in the Brussels Ia Regulation.[188]

186 Article 79(2) Regulation (EU) 2016/679 (Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.").

187 *See* recital 141 Regulation (EU) 2016/679 ("Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject... ."). *See* also Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 23 and footnote 62.

188 *See* article 17(1)(c) Regulation (EU) 1215/2012. *See* also Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, 273-274 (distinguishing the "orientating" criterion as used in the Google Spain case is determine prescriptive jurisdiction from the "directing" criterion in article 17(1)(c) Regulation (EU) 1215/2012).

3.3 Scope of the Court's Jurisdiction under Article 79(2) GDPR[189]

There is nothing in the text of article 79(2) GDPR to suggest that the scope of a Member State court's jurisdiction is limited to the territory of the forum state. Article 82(6) GDPR stipulates that court proceedings for exercising the right to receive compensation shall be brought before the courts referred to in article 79(2), that is, the Member State where the controller or processor has an establishment or where the data subject is habitually resident.[190] Recital 146 refers to the right to "full and effective compensation" and liability for "the entire damage", and article 82(4) GDPR stipulates that the controller or processor shall be jointly liable for the "entire damage".[191] Thus, it seems clear that the scope of the court's jurisdiction to award damages encompasses all damage that a data subject suffers as a result of the data processing in violation of the GDPR regardless of where in the world the damage arises. For example, assume that a controller, in the context of its establishment's activities, illegally processes the personal data of a data subject habitually resident in another Member State, which leads to the data subject losing certain business contracts in a third State. It is submitted that a court in the Member State where the controller or processor has its main establishment or where the data subject is habitually resident would have jurisdiction to award compensation for all damage arising from the illegal processing under the GDPR and complementary national provisions without any territorial restrictions, including damage arising in the third State as in the example above.

A more difficult question is whether a Member State court has jurisdiction to issue orders and injunctions to enforce a data subject's rights under the GDPR (e.g. the right to erasure or to rectification) when the controller or processor is established in another Member State, assuming this form of remedy is available under the applicable national law. Assume for example that a court is exercising jurisdiction under article 79(2) GDPR based on the habitual residence of the data subject in the forum Member State. Would this court have jurisdiction to order a

189 A separate question that cannot be fully addressed here is the territorial scope of application of the GDPR itself. For example, assume that a search engine falls within the territorial scope of the GDPR pursuant to article 3 Regulation 679/2016. Would the search engine be required, when granting a request for de-referencing, to deploy the de-referencing to all domain names used by the search engine, even to those having a country code in a third state, and irrespective of the fact that a search is initiated outside the EU territory? This is a question of prescriptive jurisdiction as opposed to adjudicative jurisdiction as discussed here. A similar question concerning the territorial scope of the Data Protection Directive was recently referred to the CJEU in Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), Case C-507/17. *See* also Svantesson, Dan, *Private International Law and the Internet*, Wolters Kluwer 3 ed. 2016 p. 474 (observing that the CJEU was silent on the geographical scope of the right to de-referencing in the Google Spain case).

190 *See* articles 79(2) and 82(6) Regulation (EU) 679/2016.

191 *See* recitial 146 and article 82(4) Regulation (EU) 679/2016. The GDPR makes clear that the controller and processor are jointly liable for the entire damage, although compensation may be apportioned under certain circumstances provided the data subject is ensured full and effective compensation. There is nothing in the recital to suggest however that compensation should be apportioned among the Member States.

controller to erase personal data, if the controller has its main establishment in another Member State where it takes and implements decisions on the purposes and means of the processing of personal data?

The lack of a limitation on the scope of the national court's jurisdiction with respect to granting an effective judicial remedy is in contrast to the explicit rules on the division of competence (or jurisdiction) between the national DPAs for investigations concerning illegal cross-border processing.[192] With respect to the national DPAs competence, the GDPR stipulates "each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation *on the territory of its own Member State*." (emphasis added).[193] An exception to this rule exists however for the DPA which has the role as "lead supervisory authority", that is, the DPA where the controller or processor has its main or only establishment. The lead supervisory authority is competent to adopt binding decisions with respect to cross-border processing and take measures applying the powers conferred on it in accordance with the GDPR ("one-stop-shop mechanism"), although it should closely involve and coordinate with the other national DPAs.[194] In addition, these decisions may be subject to the consistency mechanism.[195]

Unlike decisions taken by the DPAs, which can produce legal effects as regards processing operations that substantially affect a significant number of data subjects in several Member States, a private enforcement action primarily affects only the parties to the dispute. Provided the court exercising jurisdiction has a sufficient connection to the parties or the specific dispute between them, there is no reason to limit its jurisdiction in relation to the courts of another state, as the decision will not affect third parties. Either a court in the Member State where the data subject is habitually resident or, as argued above, a court in the Member State where the controller or processor has its main establishment, have a sufficient connection to issue orders affecting the interests of the parties.

Moreover, there is a rule on related actions in article 81 GDPR, which permits a court to suspend proceedings if it has information that proceedings concerning the same subject matter as regards processing by the same controller or processor, are already pending in a court in another Member State.[196] The court may decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof, provided the proceedings are pending at first instance.[197] Proceedings are deemed related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate

192 *See* Chapters VI and VII Regulation (EU) 679/2016 concerning the competence and cooperation between the DPAs.

193 Article 56(1) Regulation (EU) 679/2016.

194 Recital 125 and articles 56 and 60 Regulation (EU) 679/2016.

195 *See* Chapter VII, section 2 Regulation (EU) 679/2016.

196 Article 81(2) Regulation (EU) 679/2016. *See* also article 81(1) Regulation (EU) 679/2016 on the duty to inform.

197 Article 81(3) Regulation (EU) 679/2016.

proceedings.[198] This rule facilitates cooperation among the courts of the Member States with respect to actions where a controller or processor illegally processes personal data of data subjects in different Member States. Article 81 GDPR reduces the risk that a controller or processer would be subject to irreconcilable orders relating to the same processing but affecting data subjects in different Member States.

3.4 Do the New Rules on Jurisdiction in the GDPR Supplement or Supplant General Rules on Jurisdiction?

Article 79(2) GDPR does not clarify its relationship with the rules on jurisdiction contained in the Brussels Ia Regulation, the 2007 Lugano Convention, and the Member States' national rules on jurisdiction.[199] However, recital 147 of the GDPR states: "Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (1) should not prejudice the application of such specific rules."[200] In a similar manner, article 67 of the Brussels Ia Regulation stipulates that it "shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union".[201] There is a similar rule in the 2007 Lugano Convention and in some Member States' national rules.[202] This raises the question whether the rules on jurisdiction in article 79(2) GDPR supplement or supplant

198 Recital 144 Regulation 679/2016. This text in the recital is identical to the text in article 30(3) on related actions in Regulation (EU) 1215/2012.

199 Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 21; Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 274.

200 *See* Recital 147 Regulation (EU) 2016/679.

201 Article 67 Regulation (EU) 1215/20012 ("This Regulation shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union or in national legislation harmonised pursuant to such instruments."). *See* Pålsson, Lennart & Hellner, Michael, Bryssel I-förordningen jämte Bryssel- och Luganokonventionerna, Zeteo 2016, para. 31 (stating that article 67 Brussels Ia Regulation has had only limited significance as there are only a small number of EU instruments that contain specific rules on jurisdiction).

202 *See* article 67(1) 2007 Lugano Convention ("This Convention shall not affect any conventions by which the Contracting Parties and/or the States bound by this Convention are bound and which in relation to particular matters, govern jurisdiction or the recognition or enforcement of judgments. Without prejudice to obligations resulting from other agreements between certain Contracting Parties, this Convention shall not prevent Contracting Parties from entering into such conventions."); Chapter 10, section 21 Swedish Code of Judicial Procedure ("If provisions concerning the competence of courts contained in any act or regulation deviate from the rules contained in this chapter, the former shall govern.").

(some or all) of the general rules on jurisdiction contained in the Brussels Ia Regulation, the Lugano Convention, and the Member States' national rules.

Other EU instruments containing rules on jurisdiction governing specific matters are somewhat clearer with respect to their relationship with the general rules on jurisdiction. The rules on jurisdiction in the EU Trademark Regulation and the Community Design Regulation with respect to infringement claims and invalidity counter claims have the character of *lex specialis* and clearly supplant the corresponding rules provided for by the Brussels Ia Regulation.[203] In contrast, the rules on jurisdiction in the Community Plant Variety Right Regulation and in Directive 96/71/EC concerning the posting of workers in the framework of the provision of services supplement the general rules on jurisdiction by providing the plaintiff with additional options without depriving the plaintiff of the possibility to invoke the general rules.[204]

The relationship between the rules on jurisdiction in the Brussels Ia Regulation, on the one hand, and the Montreal Convention for the Unification of Certain Rules for International Carriage by Air and Regulation 2027/97, which implements that Convention, on the other hand, was raised but not answered in Case C-240/14, Pruller-Frey.[205] Article 33 of the Montreal Convention states that an action for damages "must be brought" before certain designated State parties and that an action for damages resulting from the death or injury of a passenger "may be brought" before certain designated State parties.[206] These rules have mandatory

203 Case C-360/12, Judgment of 5 June 2014, Coty Germany, ECLI:EU:C:2014:1318, para. 27; Judgment of 23 January 2014, Nintendo and others (C-355/12) ECLI:EU:C:2014:25, para. 42. While the EU Trademark Regulation and the Community Design Regulation state that the Brussels Ia Regulation is to apply "Unless otherwise specified in this [EU trademark or Community design] Regulation", the Regulations go on to list specific articles in the Brussels Ia Regulation that are not applicable to specific types of actions (e.g. infringements) involving EU trademarks and Community designs, and provide other rules on jurisdiction to replace them. *See* articles 122 Regulation 2017/1001 on the European Union trade mark; articles 79 Regulation 6/2002 on Community Designs.

204 The Community Plant Variety Right Regulation refers to its special rules on jurisdiction as "complementary" to the Lugano Convention, and excludes only one specific article of the Lugano Convention. *See* article 101 Regulation 2100/94 on Community plant variety rights. *See* also Fawcett, James & Torremans, Paul, Intellectual property and private international law, 2nd ed., Oxford University Press 2011 p. 442. Likewise, the Directive 96/71/EC concerning the posting of workers in the framework of the provision of services states that the worker's right to institute proceedings in the Member State of posting is "without prejudice, where applicable, to the right, under existing international conventions on jurisdiction, to institute proceedings in another State." Article 6 Directive 96/71/EC concerning the posting of workers in the framework of the provision of services ("In order to enforce the right to the terms and conditions of employment guaranteed in Article 3, judicial proceedings may be instituted in the Member State in whose territory the worker is or was posted, without prejudice, where applicable, to the right, under existing international conventions on jurisdiction, to institute proceedings in another State."). *See* also Sinander, Eric, *Internationell kollektivavtalsreglering: En studie i internationell privaträtt av den svenska modellen för reglering av anställningsvillkor*, Doctoral Thesis in Private law at Stockholm University 2017 p. 120.

205 *See* Judgment of 9 September 2015, Prüller-Frey (C-240/14) ECLI:EU:C:2015:567, para. 36.

206 Article 33 Montreal Convention for the Unification of Certain Rules for International Carriage by Air.

application and any clause contained in the contract of carriage entered into before the damage occurred by which the parties alter the rules as to jurisdiction, shall be null and void.[207] The Advocate General observed that the rules on jurisdiction in the Montreal Convention aimed at eradicating conflicts of laws and jurisdiction and establishing a foreseeable set of rules on liability, protecting passengers and enabling air carriers to manage risk more effectively. [208] Consequently, the Advocate General would give article 67 Brussels Ia Regulation a broad interpretation and suggested that it precluded (supplants) the application of the Brussel Ia Regulation's general rules on jurisdiction when another EU instrument, in this case the Montreal Convention, contained *lex specialis* rules on jurisdiction.[209]

If article 79(2) GDPR is understood as supplanting the general rules on jurisdiction, a data subject could not base jurisdiction on any of the general rules on jurisdiction in the Brussels Ia Regulation, 2007 Lugano Convention, or the Member States' national rules discussed under chapter 2 (e.g. domicile, the place where the harmful event occurred, the place where the contractual obligation that was breached was performed, etc.).[210] Such a restrictive *lex specialis* interpretation is supported by the text of article 79(2) GDPR that states that proceedings against the controller or processer "shall" be brought before the courts of the Member State where the controller or processer has an establishment, and that alternatively proceedings "may" be brought in the Member State of the data subject. The use of the term "shall" may indicate that this basis of jurisdiction is mandatory except for the alternative specifically mentioned whereby the data subject "may" bring the proceedings in his/her home state. Likewise, article 82(6) GDPR stipulates that claims for compensation "shall be brought before the courts . . . referred to in Article 79(2)." An *e contrario* interpretation suggests that such claims may not be brought before any other courts. This *lex specialis* interpretation would serve the objective of the GDPR to provide greater legal certainty for economic operators and data subjects as there would be only two possible fora. This interpretation also does not detract from the objective to strengthen the data subject's rights as the data subject is allowed to bring a claim in his/her habitual residence, which is usually most favorable to him/her.

A drawback with interpreting the GDPR as supplanting the general rules on jurisdiction however is that there would not be any Member State court that was competent to adjudicate a private enforcement action by a data subject who was habitually resident outside of the EU and who claims that his/her rights under the GDPR have been infringed by a controller/processor that does not have any

207 Article 49 Montreal Convention for the Unification of Certain Rules for International Carriage by Air.

208 *See* Opinion of Advocate General Wahl, delivered on 18 September 2014, Case C-240/14 Pruller-Frey, ECLI:EU:C:2015:325, para. 60.

209 *See* Opinion of Advocate General Wahl, delivered on 18 September 2014, Case C-240/14 Pruller-Frey, ECLI:EU:C:2015:325, para. 51-53

210 *See* Ny dataskyddslag: Kompletterande bestämmelser till EU:s dataskyddsförordning, SOU 2017:39 (The New Data Protection Law: Complementary provisions to the GDPR, Official Reports of the Swedish Government) p. 304 (stating that the rule in article 79(2) GDPR "takes over" the general rules on jurisdiction under Swedish law).

establishment in the EU. Such a scenario is possible as the territorial scope of the GDPR encompasses controllers that do not have a (relevant) establishment in the EU, but that offer goods or services to data subjects in the EU or monitor their behavior as far as their behavior takes place within the EU.[211] The concept of a data subject in the EU is broader than data subjects habitually resident in the EU, and protects even foreign citizens and residents when they are on EU territory. [212] If these persons were denied access to court to enforce their rights under the GDPR, this might possibly be considered a breach of article 47 of the EU Charter and article 13 ECHR on the right to an effective remedy.

The better interpretation, and one which gives effect to recital 147, is that GDPR rules supplement but take precedence over the general rules on jurisdiction. The rules in the GDPR should be understood to take precedence over any inconsistent rules in the Brussels Ia Regulation, 2007 Lugano Convention, and national rules that would conflict with bases of jurisdiction under article 79(2) GDPR and deprive the data subject of them. One example would be where a data subject's data was illegally processed during entry into a public register in one Member State and the data subject brings an action in another Member State where s/he is habitually resident but the forum considers the action to fall with the exclusive jurisdiction of Member State where the register is kept.[213] Another example is where a business to business contract between a controller and an individual contains a choice of forum clause giving exclusive jurisdiction for all claims related to the contract to the Member State where the controller has its establishment but the individual data subject wants to bring a private enforcement action to enforce his/her data protection rights in the Member State of his/her habitual residence. In these two examples, the data subject should be able to bring a claim in the Member State of his/her habitual residence notwithstanding the rules on exclusive jurisdiction or on prorogation clauses in the general rules on jurisdiction. If the GDPR rules supplement the general rules on jurisdiction, it will be necessary to make a case by case assessment of each individual basis of jurisdiction in the Brussels Ia Regulation, 2007 Lugano Convention or national Member States rules to determine its compatibility with the rules in the GDPR.

Revolidis argues that the rules of the Brussels Ia Regulation should be considered inconsistent with the rules on jurisdiction in the GDPR if the rules serve a different underlying purpose, even if it is possible for the rules to apply in parallel. He submits that article 7(2) Brussels Ia Regulation is inconsistent with the jurisdictional rules in the GDPR because the underlying purpose of article 7(2) BIa is to facilitate the sound administration of justice, which is incompatible with

211 Article 3(2) Regulation (EU) 679/2016.

212 Recital 14 Regulation 679/2016 ("The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.").

213 *See* article 24(3) Regulation (EU) 1215/2012; article 22(3) 2007 Lugano Convention. *See* also Brkan, Maja, *Data Protection and European Private International Law: observing a bull in a China shop*, International Data Privacy Law, Volume 5, No. 5 2015 p. 257-278, p. 274 (suggesting that the data protection claim could be separated from the other claims relating to the exclusive jurisdiction or that the data subject should have the right to file all claims before the court having exclusive jurisdiction).

the underlying aim of article 79(2) GDPR, which is to empower the data subject.[214] Revolidis' definition of inconsistent however, is likely to be more difficult to apply as some rules on jurisdiction in the Brussels Ia Regulation aim to protect the weaker party and to attribute jurisdiction to a forum with proximity to the dispute.[215]

4 Conclusions

The GDPR significantly strengthens the data subject's procedural rights by providing the data subject with the alternative to bring a private enforcement action directly against the offending controller or processor in the Member State of his/her habitual residence. This alternative empowers the data subject by enhancing control over the enforcement of the data subject's rights by making it easier for the data subject to bring a private enforcement action. It can be expected that most data subjects who choose to bring a private enforcement action will make use of this alternative to bring proceedings in their own home state.

The other alternative available to the data subject under the GDPR is to bring the action in the Member State where the controller or processor has an establishment. It has been argued that if the controller or processor has more than one establishment in the EU, the rule on jurisdiction should be interpreted to mean the main establishment. This is because the CJEU has interpreted the concept of establishment so broadly that a strict textual interpretation could lead to extensive forum shopping and reduce legal certainty. The data subject is not in need of additional fora (as s/he already can bring the action in the Member State of habitual residence) and allowing the action to be brought in the Member State where the controller or processor has any establishment is not justified by the principle of proximity.

This article concludes that these two new rules on jurisdiction in the GDPR supplement rather than supplant the general rules on jurisdiction in the Brussels Ia Regulation, the 2007 Lugano Convention, and the Member States' national laws. True, the application of some of the bases of jurisdiction to data protection actions is unclear and therefore gives rise to legal uncertainty for both data subjects and economic operators. Also, the general rules potentially give the data subject additional alternatives for forum shopping above and beyond the alternatives in the GDPR. Nevertheless, most of these bases for jurisdiction in the general rules will be superfluous because they will coincide with the bases of jurisdiction in the GDPR itself or will be less advantageous alternatives for the data subject. Importantly, however, these general rules can fill in gaps when the rules on jurisdiction in the GDPR are not applicable because the data subject and/or the controller or processer is habitually resident/established outside the EU.

214 Revolidis, Ioannis, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, Masaryk University Journal of Law and Technology, Volume 11, issue 1 2017 p. 7-37, p. 23.

215 *See* chapter 2.4 above.

While the GDPR is successful in strengthening data protection rights for individuals in relation to offending controllers and processors, one should remember that not every data controller is a Google, Facebook or Twitter but can be a Mrs. Bodil Lindqvist blogging about fellow parishioners.[216] Giving the data subject the right to bring a private enforcement action directly against the offending controller or processor in the Member State of his/her habitual residence means that many controllers or processers will be hauled into a foreign court to defend potentially frivolous actions. Further research is needed to see what effect this might have on other fundamental rights such as freedom of expression.[217]

216 *See* Judgment of 6 November 2003, Lindqvist (C-101/01) ECLI:EU:C:2003:596.

217 *See* article 11 EU Charter; article 10 ECHR.