Global applicability of the GDPR in context

Claes G. Granmar*

Key Points

- In this article, the basic concepts determining the territorial scope of the General Data Protection Regulation (GDPR) are analysed in the context of constitutional EU law.
- Proposals made by the European Data Protection Board (EDPB) in the guidelines on Article 3 of the GDPR are critically reviewed in the light of the 'methodological source code' of the European unification program enshrined in Treaty provisions stipulating a teleological and system-coherent approach.
- More specifically, when it comes to Article 3(1) of the GDPR, the meaning of words such as 'controller' and 'processor', 'establishment of a controller or a processor in the Union' and processing 'in the context of' an establishment, are systematically analysed.
- When it comes to Article 3(2) of the GDPR, in particular the need to construe the spatial and temporal aspects of being 'in the Union' in a consistent way moves into the limelight.
- As a result of the systematic construction of Article 3 of the GDPR, that departures from the distinction between a factual and formal approach advocated by the EDPB in its 'data protection law' specific analysis, it is possible to make more solid policy recommendations.

Introduction

On 12 November 2019, the European Data Protection Board ('EDPB') issued its guidelines on theterritorial scope of the General Data Protection Regulation ('GDPR').[1] In view of the debate about the obligation for undertakings not having their main establishments in the Union to comply with EU data protection standards, the effort to promote a consistent application of Article 3 of the GDPR is commendable. However, the reasoning is at times far from convincing and important questions are left unanswered. In particular, it is problematic that the concepts defining the spatial applicability of the Regulation are analysed in a legal vacuum, abstracted from the broader context of constitutional EU law. Indeed, the GDPR can be properly understood only in the light of the competences conferred upon the European Union ('EU') in accordance with the Treaty on European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU').[2] Furthermore, all substantive EU law transposes the Charter of Fundamental Rights of the European Union ('EU Charter') that was adopted as a policy instrument in 2000 and attributed the same legal value as the Treaties in 2009 pursuant to the Lisbon revision.[3] Whereas the Treaties and the EU Charter have primacy over all other legal sources within the scope of EU law, secondary legislation adopted on the basis of these acts such as the GDPR, can only specify, as opposed to expand, alter or confine the scope of primary law.[4] In fact, the GDPR must fit like a piece in the EU law puzzle and reconcile data protection with other objectives, such as the freedom to conduct a business and the general interests of technology development. Hence, terms like 'controller', 'processor', 'establishment', 'monitoring', and 'targeting' must have the same meaning in the GDPR as in primary law and other

*Associate Professor in European Law, DIHR, Faculty of Law, Department of Law, Stockholm University, , Email:claes.granmar@juridicum.su.se
The author would like to thank everyone at the Institute for European and Comparative Law (IECL), Oxford University, for their support and encouragement in the course of researching the GDPR as a visiting fellow.

1 EDPB guidelines 3/2018 on the territorial scope of the GDPR (Art 3), Version 2.0, 12 November 2019, <https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en> accessed 03 April 2021. Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC, Official Journal ('OJ') 2016 L 119/1.

2 Consolidated version of the TEU and TFEU, OJ 2012 C 326/1.

3 EU Charter, 2010 OJ C 83/389.

4 See as to the 'constitutional fabric' of the GDPR, Communication from the Commission, *Exchanging and Protecting Personal Data in a Global World*, [2017] COM 7 final.

fields of secondary legislation. In this piece, the EDPB guidelines are discussed in the context of a systematic construction of Article 3 of the GDPR, and as a result, it is possible to make more solid policy recommendations.[5]

Article 3 of the GDPR and extraterritorial data protection

In the absence of international standards for the processing of personal data, the Union is seeking to create and maintain an effective system for data protection within its sphere of interests.[6] On the surface, it may seem as if the GDPR is reaching around the world without limitations, and commentators have expressed fear of a Union claim for 'extraterritorial' data protection.[7] Admittedly, 'extraterritoriality' is an ill-defined legal concept, but the situations that it normally refers to have in common that the legislator, courts, authorities, and other regulating bodies in one polity extend their normative powers into the territory of another polity without any formal approval.[8] For instance, countries and polities seeking to combat terrorism may enforce their laws irrespective of where in the world an act has taken place, and *data collection* is an important means to that end.[9] However, to require firms to retain traffic data from their communication networks is by nature different from ensuring people a right to *data protection* in the legal system of a country or polity.[10] These opposing interests may be reconciled in data transfer agreements.[11] In its preliminary ruling on the second *Schrems* Case handed down in July 2020, the Court of Justice clarified that the standards for data transfers under such an agreement must largely comply with the rights set out in the GDPR.[12] Hence, the adequacy decisions of the European Commission shall ensure the fundamental rights to data protection as well as to effective remedy and to a fair trial beyond the territorial scope of the GDPR. However, as the decisions apply only to data exported by legal entities caught by the Regulation, the need for undertakings not having a main establishment in the Union to align their business models with EU data protection standards, depends on the territorial scope of the GDPR. It is the purpose of this article to explore and explain the applicability of the Regulation in relation to undertakings that are headquartered in a non-EU Member State ('third country').

In its guidelines, the EDPB is silent on the issue of 'extraterritorial applicability' of the GDPR. Nonetheless, it is evident from the wording of Articles 3(1) and (2) of the GDPR that the Regulation applies only insofar as there is a *genuine link* between the processing activity and the Union. According to Article 3(1) of the GDPR, the link required for the Regulation to apply is processing of data in the context of the activities of an *establishment of a controller or a processor in the Union.* If Article 3(1) of the GDPR is inapplicable, the Regulation is nonetheless triggered pursuant to Article 3(2) of the GDPR if the *data subjects concerned are in the Union.* According to Article 3(2)(a) of the GDPR, the Regulation applies when the processing activities are related to 'the offering of goods or services' to data subjects who are in the Union. According to Article 3(2)(b) of the GDPR, the Regulations applies when processing activities are related to the 'monitoring of their behaviour' in the Union.

In situations where there is no genuine link between the processing activities and the Union in accordance with Article 3(1) or 3(2) of the GDPR, the Regulation may nevertheless apply pursuant to Article 3(3) of the GDPR 'in a place where Member State law applies by virtue of public international law'.[13] This provision is clearly a remnant of the repealed Data Protection Directive ('DPD'), which approximated the Member States' laws on data protection and paved the way for the adoption of the Regulation.[14] As the Member States were free to decide how to adapt their domestic legal

5 A draft of this article was published in the DiVA open access portal 03 January 2019.

6 Compare with the Opinion of Advocate General Saugmansgaard Øe on Case C–311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximiliam Schrems*, ECLI:EU:C:2019:1145. Compare with World Trade Organization's, Work Programme on Electronic Commerce (WPEC) adopted on 25 September 1998, WT/L/274.

7 See, eg DJB Svantesson, 'Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effects on U.S. Businesses' (2014) 1 Stanford Journal of International Law 53; and C Kuner, 'Extraterritoriality and Regulation of International Data Transfer in EU Data Protection Law' (2015) 4 International Data Privacy Law 235.

8 See M Cremona and J Scott, *EU Law Beyond EU Borders* (Oxford University Press, Oxford, 2019).

9 See, eg the USA Patriot Act (HR 3162) of 24 October 2001; the USA CLOUD Act (HR 4943) of 2 June 2018; and the US Supreme Court in *United States v Microsoft Corp*, No 17–2, 584 US (2018).

10 Compare with Joined Cases C–293/12 and C–594/12 *Digital Rights Ireland and Kärntner Landesregierung,* ECLI:EU:C:2014:238; and Joined Cases C–203/15 and C–698/25 *Tele2 Sverige AB and Secretary of State of the Home Department,* EU:C:2016:970.

11 Articles 44–45 of the GDPR and Recitals 101–108 in the preamble to the GDPR.

12 Case C–311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximiliam Schrems,* ECLI:EU:C:2020:559 ('*Schrems II*') where the Court ruled on Commission Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the EU US Privacy Shield, 2016 OJ L207/1.

13 Recitals 22–25 in the preamble to the GDPR.

14 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 OJ L281/31.

systems to the DPD, it was considered necessary to clarify that the domestic legislation should transpose the directive also when applied beyond the State's territory in for instance embassies, consulates and on ships. By contrast, an EU Regulation is per definition *directly applicable* as law in the domestic legal systems.[15] Hence, the GDPR applies as domestic law beyond the EU territory of a Member State by virtue of international agreements or generally accepted peremptory customs ('jus cogens') without a detour over Article 3(3) of the GDPR.[16] Furthermore, it is recognized under public international law that the GDPR may pursuant to the constitutional traditions of some of the EU Member States apply indirectly in their 'Overseas Countries and Territories' or 'Outermost Regions'.[17] The applicability of the GDPR may also be extended beyond the territory of the Member States by the Union's international agreements. Like most other Regulations, the GDPR is transposed into the laws of Iceland, Norway, and Liechtenstein pursuant to the Agreement on the European Economic Area ('EEA').[18] Furthermore, the Union refers to the GDPR in the new generation of trade and investments agreements and, as mentioned, it seeks to ensure an adequate level of data protection beyond the Member States through data transfer agreements.[19] There are also sector specific data protection arrangements.[20] Naturally, the fact that data protection can be subject to public international law and apply beyond the territory of a Member State, adds nothing to the definition of the territorial scope of the GDPR. However, the resort to public international law contradicts the very idea of 'extraterritorial' applicability. As neither Article 3(3) of the GDPR, nor agreements or jus cogens regarding data protection define the territorial scope of the GDPR, only Articles 3(1) and 3(2) thereof are examined here.

Data protection, the rule of law and the 'methodological source code' of EU law

In the introduction to the EDPB guidelines, it is said that the GDPR 'in part confirms choices made' by the EU legislator and the Court of Justice in the context of applying the revoked DPD. True, a legislator has a certain amount of leeway to shape legal norms and a Court has a certain margin of interpretation. However, the normative freedom of the EU institutions to determine the applicability of the GDPR is limited by the methods for interpretation and application stipulated by the Member States in the Treaties. Indeed, the European unification process ultimately hinges on the basic principle of *pacta sunt servanda*, like all other collaborations between autonomous states under public international law.[21] More concretely, a consistent evolution of EU data protection law is promoted by the duty of the EU Institutions and the Member States to cooperate sincerely pursuant to Article 4(3) of the TEU.[22]

According to Article 5(2) of the TEU, the EU institutions shall act only within the limits of the powers that have been conferred upon them by the Member States to *attain the objectives* set out in the Treaties. On the highest level of abstraction, Article 3 of the TEU establishes the objectives of the Union. According to Article 3(1) of the TEU, the Union shall promote peace, its values and the wellbeing of its people, and the values shared by the Member States are manifested in Article 2 of the TEU. Hence, the Union is 'founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'. Since the EU Charter was elevated to primary law by Article 6(1) of the TEU pursuant to the Lisbon revision in 2009, the 'human rights' form part of a broader category of 'fundamental rights'. Article 7 of the EU Charter stipulates a right for everyone in the Union (as opposed to only for EU citizens) to 'respect for his or her private

15 Article 288 of the TFEU. Communication from the Commission, *Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation of 25 May 2018*, [2018] COM 43 final.

16 Compare with the EDPB guidelines (n 1) 22–23.

17 There are 13 Overseas Countries and Territories, see <http://www.octassociation.org/> accessed 29 July 2020, and nine Outermost Regions, see <https://www.europarl.europa.eu/factsheets/en/sheet/100/outermost-regions-ors-> accessed 29 July 2020. See, eg as to the relation between the EU, Denmark and Greenland, Council Decision 2014/137/EU 2014 OJ L76/1, and the Danish law Anordning om ikraftraeden for Gronland af lov om behandling af personuplysningen, Lovtidene A Nr 1238, 15 October 2016.

18 Treaty of Oporto, 1994 OJ L1/3.

19 See, eg the Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part, 2017 OJ L11/23; and Commission implementing decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, 2019 OJ L76/1.

20 See, eg Agreement on Air Transport between Canada and the European Community and its Member States, 2010 OJ L207/33. See also alternative venues under Arts 46–50 of the GDPR. In addition, the GDPR provides a legal framework for private measure such as binding corporate rules.

21 See Case C–621/18 *Andy Wightman and Others v Secretary of State for Exiting the European Union,* ECLI:EU:C:2018:999; and Art 31 of the Vienna Convention on the Law of Treaties, 23 May 1969, United Nations Treaty Series vol 1155, 331.

22 See, eg T Hartley, *Constitutional Problems of the European Union* (Hart, Oxford, 1999) 152 *et sec.*

and family life, home and communications', and Article 8 thereof establishes even more unequivocally the 'right to the protection of data concerning him or her'.[23] Along the lines of Article 5(2) of the TEU, the Court of Justice has reiterated that situations cannot exist which are covered by EU law without the rights enshrined in the Charter being applicable.[24] Indeed, the rights to privacy and data protection are omnipresent within the ambit of EU law. However, all the other fundamental rights recognized in the EU Charter are also ubiquitous and, as the Corona virus pandemic has made utterly clear, there may also be overriding public interests. As there is no ranking of fundamental rights or interests, and the objectives are neither static nor absolute, Article 52 of the EU Charter stipulates that they can all be limited to some extent if necessary. Although, each fundamental right has a core meaning that must not be compromised, conflicting interests are reconciled by means of *proportionality tests* to ensure a consistent legal development.[25] Due to the *sui generis* nature of the Union legal order and the complexity of multi-layered governance, 'the rule of law' depends more on legal systematics in EU law than in domestic law. While norms are transposed vertically through secondary legislation into domestic law, they are reconciled horizontally by proportionality and developed in the interplay between internal and external actions.[26] Indeed, 'the rule of law' must be understood in terms of a *methodological source code* for the unification program enshrined in the Treaty provisions ensuring a *teleological* and *consistent* legal development.[27]

Besides Article 5(2) of the TEU, also Article 13 thereof requires a *teleological* development of EU law as it stipulates that the Union shall have 'an institutional framework which shall aim to promote its values, advance its objectives and serve its interests, those of its citizens and those of the Member States [...]'. In many instances, a teleological and consistent approach are virtually two sides of the same coin.[28] Article 13 of the TEU also stipulates that the Union shall '[...], ensure the consistency, effectiveness, and continuity of its policies and actions.' Article 7 of the TFEU summaries the EU competences by establishing that 'the Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers.'

In order to cooperate sincerely, the Member States shall apply EU law in the same way as the EU institutions. Pursuant to Article 19 of the TEU, the Member States have afforded the Court of Justice the interpretative prerogative regarding the Treaties and, hence, all normative measures based on the Treaties. Along those lines, Article 267 of the TFEU establishes that all domestic Courts may ask the Court of Justice for clarifications, and the Courts of last instance have an obligation to do so when necessary.[29] Gradually, the meaning of the provisions in the GDPR including Article 3 thereof will be clarified. However, the Regulation is not complete in the sense that it covers all aspects of data protection. There are implicit and explicit gaps that need to be filled by the domestic norm giving powers. In that case, the territorial scope of the domestic rules should harmonize with that of the Regulation.[30]

All vertical consistency aside, the GDPR must fit horizontally into a system of Union legislation and measures.[31] Even if the Regulation focuses on data protection that is not the only fundamental right at stake. As stated in Recital 4 in the preamble to the GDPR, the protection of personal data breaks against for instance the freedoms of expression and information and the freedom to conduct a business.[32] In general, the Regulation is an important step in the realization of a

23 Case C–131/12 *Google Spain SL and Google Inc v Agencia España Proteccion de datos (AEPD) and Mario Costejo González*, ECLI:EU:C:2014:317 ('*Google I*') paras 68–69, 74, 81, 97, and 99. See as to 'horizontal direct effect' of the EU Charter in, eg Case C–414/16 *Vera Egenberger v EvangelischesWerk für Diakonie und Entwicklung e.V.*, ECLI:EU:C:2018:257.

24 See, eg Case C–617/10 *Åklagaren v Hans Åkerberg Fransson*, ECLI:EU:C:2013:105, paras 21–22.

25 In the context of data protection, the Court of Justice has clarified the territorial importance of proportionality in Case C–507/17 *Google v CNIL ('Google II')*, ECLI:EU:C:2019:772.

26 Compare with Report of the Secretary-General Kofi Annan to the United Nations Security Council, 'The Rule of Law and transnational justice in conflict and post conflict societies', S/2004/616, 23 August 2004.

27 This is the 'law' that the Court of Justice shall recognize under Article 19 of the TEU.

28 See for an overview of provisions requiring consistency in RA Wessel and J Larik, 'The European Union as a Global Actor' *EU External Relations Law* (Hart, Oxford, 2020).

29 Compare with Case C–210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388 ('*Facebook Insights*') para 47; eg Case C–343/19 *Verein für Konsumentinformation v Volkswagen AG*, ECLI:EU:C:2020:534, para 19. See also Case C–398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, ECLI:EU:C:2017:197.

30 See, eg Article 8 of the GDPR on the definition of 'child', and Recital 10 in the preamble to the GDPR. See also K Lenaerts, 'Interlocking Legal Orders in the European Union and Comparative Law' (2003) 52 International and Comparative Law Quarterly873, 902; and C Granmar, 'Chronopost: Horizontal Harmonization through Overlapping National Jurisdictions' (2012) 4 Europarättslig Tidskrift 681 *et sec.*

31 See references to other legal frameworks in Articles 2, 4(25), 21, 43, 76, and 95 of the GDPR, and in Recitals 17, 19, 21, 35, 42, 54, 106, 147, 154, 161, 163, 167, 172, and 173 thereof.

32 See as to freedom of expression Article 85 of the GDPR and Recital 153 thereof. See also the EDPB guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the search engines cases under the GDPR (Part 1), Version 2.0, 7 July 2020 ('EDPB search engine guidelines') 9, 11–16. See also, eg Case C–136/17 *GC, AF, BH, ED v CNIL*, EU:C:2019:773 ('Google

'digital internal market'.[33] Hence, the GDPR must tally with legislation regarding for instance e-commerce, 'cookies', geo-blocking, consumer protection, company law, and intellectual property rights.[34] However, horizontal consistency is required more broadly, and the GDPR must not contradict eg competition law and *vice versa*.[35] In addition, specific trade-offs between data protection and other fundamental rights are made in secondary legislation regarding eg electronic communication, EU institutions, and law enforcement agencies.[36]

Evidently, also consistency between *external and internal* Union measures is required.[37] Whereas internal measures may translate into external competences in accordance with the doctrines on parallelism and implied powers, all the external commitments are normally given effect within the Union through internal measures.[38] In fact, it is often difficult (if possible) to disentangle the internal and external aspects of EU law. Along those lines of reasoning, the European Commission concluded in its *travaux préparatoires* to the GDPR in 2010 that '[a] high and uniform level of data protection within the EU will be the best way of endorsing and promoting EU data protection standards globally.'[39]

Finally, *evolutionary* consistency is essential for legal certainty. Although there is no EU *stare decisis* doctrine, the Court of Justice seeks to shape consistent lines of reasoning. Evidently, a teleological and consistent construction of Union concepts is key to system-coherency. Furthermore, legislation builds as far as possible on earlier legal structures and codifies, if suitable, the case law regarding repealed acts. On that note, Article 3 of the GDPR testifies to the lessons learned from applying Article 4 of the DPD, but also to a changing techno-social context. In the age of digital globalization, location of data in interlinked computer networks is an ill-suited criterion for determining the territorial scope of data protection. Indeed, the answers to questions about the site for data processing become philosophical when tasks are assigned to available resources in the global networks, metaphorically known as 'the cloud'.[40] Whereas the location of servers used for the processing of data could be taken into consideration when determining the territorial scope of the domestic laws approximated by the DPD, Article 3(1) of the GDPR clarifies that the existence of an EU establishment is decisive for the applicability of the Regulation irrespective of where the data is processed. Furthermore, the EU legislator has recognized that even if the processor acts on 'behalf of the controller', the power relationships between the controllers and processors may look very different. In fact, the appointed processor may in many instances be in control of the processing activities. Whereas the processor may be a multinational company specialising in data processing in a field, the controller may be a self-employed person having no real control over the processing activities.[41] In contrast to what applied in domestic law within the scope of the DPD, also an EU

III'); and Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke GbR and Hartmuns Eifert v Bundesanstalt für Landwirtschaft und Ernährung*, EU:C:2010:662.

33 Communication from the Commission, *A Digital Single Market Strategy for Europe*, (2015) COM 192 final. See also Communication from the Commission, *on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All*, (2017) COM 288 final. See also, eg N Helberger, F Zuiderveen Borgesius, and A Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427.

34 See, eg Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 OJ L178/1 (under revision); Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC (now repealed), Directive 2002/58/EC concerning processing of personal data and the protection of privacy in the electronic communication sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 2009 OJ L337/11; Directive (EU) 2019/790 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC, 2019 OJ L130/92. See for the time being proposal for a Digital Service Act COM/2020/825/final; and for a Digital Market Act COM/2020/842/final.

35 Joined Cases C–403/08 and C–429/08 *Football Association Premier League Ltd and Others v QC Leisure and Others and Karen Murphy v Media Protection Services Ltd*, ECLI:EU:C:2011:631; Commission decision of 27 June 2017 in Case *Google Search (Shopping)* AT.39740 C (2017) 4444 final.; and Commission report by J Crémer, Y-A de Montjoye, and H Schweitzer, Competition Policy for the Digital Era (2019), European Commission. <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 29 July 2020. See also C Granmar, 'The Cases Regarding Premier League: In Pursuit of Unity and Coherency of the European Union Legal Order' (2012) 1 Europarättslig Tidskrift 96 *et sec.*

36 Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services, 2002 OJ L108/33 (under revision); Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 2018 OJ L295/39; and Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose 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, 2016 OJ L119/89.

37 See Articles 3(5) and 21 of the TEU.

38 Article 3(2) of the TEU and 216(1) of the TFEU, respectively, and eg Opinion 1/13 EU:C:2014:2303; and Opinion 2/13 EU:C:2014:2454. Compare with Case C–311/18 *Schrems II* (n 12); and C–362/14 *Maximillian Schrems v Data Protection Commission and joined party Digital Rights Ireland*, ECLI:EU:C:2015:650 (*'Schrems I'*).

39 Communication from the Commission, *A Comprehensive Approach on Personal Data Protection in the European Union*, (2010) COM 609 final, 19.

40 See, eg KL Jackson and S Goessling, 'Architecting Cloud Computing Solutions: Build Cloud Strategies that Align' (Packt, Birmingham, 2018).

41 Observed already in C Millard, 'Proposed EC Directives on Data Protection' (1990–91) 7 The Computer Law and Security Review 20 et sec.

establishment of the processor is therefore relevant for the determination of the territorial scope of the GDPR. Hence, when applying Article 3 of the GDPR to data processing after 25 May 2018, the consistency requirement implies that the provision shall *as far as possible* be read in the light of the rulings regarding Article 4 of the DPD.[42]

A system-coherent concept of 'controller'

As recognized in the EDPB guidelines, it is necessary to understand who the 'controller' and 'processor' are, before analysing the more specific criteria that determine the territorial scope of the GDPR.[43] These concepts are defined in Articles 4(7) and (8) of the GDPR in the same way as they were defined in the DPD. Hence, the EDPB is right to refer to the clarifications regarding the concepts provided in 2010 by the working party for the protection of data set up under Article 29 DPD ('Art. 29 WP'). However, it shall be noted that the EDPB itself adopted new guidelines on the matter in September 2020.[44] In general, the legal value of guidelines provided by EU expert authorities can be questioned in the absence of case law from Court of Justice that ensures a consistent and teleological legal development. Nonetheless, documents of that kind are likely to have a normative effect. Because, the market participant normally seek to steer clear from conduct that have been considered incompatible with EU law by such an authority.

As a starting point, any natural or legal person can shoulder the role as 'controller' since there are no inherent characteristics that distinguish the legal entity called controller from other natural or legal persons. It is the fact that the legal entity 'determines the purpose and means of the processing of personal data' that classifies a 'natural or legal person, public authority, agency or other body' among controllers. This causes the EDPB to advocate a *casuistic and factual rather than formal* conceptual construction.[45] However, the dichotomy between a factual and formal understanding of 'controller' is rather factitious.[46] There is always a formal side to legal requirements and yet, the letter of the law should be applied in a purposeful way when taking all the relevant facts in the individual case into consideration. Perhaps more accurately, formal legal requirements are facts to take into consideration when shaping conceptual building blocks that purposefully fit into the overall legal structure. When it comes to allocating the responsability as "controller", the actual power to determine the *purpose* of a processing activity carries much weight irrespective of any contracts or formal arrangements.[47] As the concept of *means* of a given processing activity is even vaguer it gives the norm giving powers much leeway to allocate responsibilities in a purposeful way. In fact, the processor has always a certain discretion to decide how to process the data, and the controller may delegate additional rights to decide.[48] However, some decisions regarding the means are essential for the processing activity, and those decisions are significant for a controller. For instance, decisions about the personal data to be processed, the length of the storage of the personal data, and access to the personal data, are *essential means* for a given processing activity that identify the controller.[49]

According to both the old and the new guidelines, the decisions regarding the 'purpose' and 'means' of data processing amount 'to determining respectively the 'why' and the 'how' of certain processing activities'.[50] If more than one natural or legal person determines the purpose and essential means of a processing activity, either symbiotically or on different levels of abstractions, they are acting as 'joint controllers'.[51] However, if the legal entities have decided that the data shall be processed for different purposes (or by different means), for instance in a 'block chain', they are controllers for different activities.[52]

Schematically, a natural person that processes personal data for private purposes may *de facto* be the controller. True, processing by individuals in the course of

42 Article 94 of the GDPR. Compare with Case C–136/17 *Google III* (n 32) para 33; Opinion of Advocate General Saugmansgaard Øe on Case C–311/18 *Schrems II* (n 6) paras 88–93.

43 EDPB guidelines (n 1) 5.

44 Supra (n 43) 6. Art 29 WP 'Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'' (WP 169, 16 February 2010) ('Art 29 WP Opinion 1/2010') 8. EDPB Guidelines 7/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 2 September 2020 ('EDPB Guidelines 7/2020') <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en> accessed 03 April 2021.

45 EDPB guidelines (n 1) 4. Compare with European Data Protection Supervisor guidelines on the concepts of controller, processor and joint controllership Under Regulation (EU) 2018/1725, 7 November 2019 <https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf> accessed 31 July 2020.

46 Art 29 WP Opinion 1/2010 (n 44) 9–12. See also Art 29 WP, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006).

47 Art 29 WP Opinion 1/2010 (n 44) 15.

48 Art 29 WP Opinion 1/2010 (n 44) 13–15.

49 Art 29 WP Opinion 1/2010 (n 44) 32; EDPB Guidelines 7/2020 (n 44) 12–15.

50 Art 29 WP Opinion 1/2010 (n 44) 13; EDPB Guidelines 7/2020 (n 44) 3.

51 Article 26 of the GDPR and Case C–25/17 *Tietosuojavaltuutettu*, ECLI:EU:C:2018:551, paras 63–75.

52 See, eg the EDPB Guidelines 7/2020 (n 44) 25–26.

a *purely personal or household activity* is pursuant to Article 2(2)(c) of the GDPR excepted from the substantive scope of the Regulation.[53] However, the Court of Justice has along the lines of general principles of EU law interpreted and applied this statutory exception from the fundamental rights of data subjects in the Union restrictively. Famously, in the *Lindquist* Case the Court explained that a person creating a database over colleagues for private purposes infringed their rights under domestic law approximated by the DPD.[54] Evolutionary consistency requires that the same should apply also under Article 2(2)(c) of the GDPR.[55] Consequently, any individual using information and communication technology ('ICT') could (or should) be classified among controllers in a 'casuistic and factual' rather than 'formal' analysis. However, if the 'determining body' in a processing activity is not in a position to ensure the data subject an effective right to data protection, the responsibility may be transferred to another legal entity. Indeed, the contours of the 'controller' appear clearly only in the light of the *teleology* of EU law.

In view of the digital transition, a factual construction of 'controller' is becoming more and more untenable. An undertaking providing an online forum for others to interact ('online platform') typically *de facto* processes the data on behalf of the legal and natural persons interacting on the platform. Whereas the end-user knows why the data shall be processed, the platform provider's servers automatically resolve the requests without determining the purpose for the activity in any intelligible sense. Hence, it is difficult to hold the platform provider accountable as the 'determining body' for the activity. Nonetheless, the Court of Justice explained in its seminal *Google Spain* ruling that the operator of a search engine can very well be the controller, without even discussing the role of the end-user.[56] This conclusion is explained only by the endeavour to allocate the responsibility for ensuring the fundamental right to data protection in an efficient way within the scope of EU law ('super teleology'). In other words, the *effet utile* of the legal instrument (DPD) justified a categorical allocation of responsibilities and, hence, a 'formal' rather than 'casuistic and factual' analysis applied.

In the *Google Spain* ruling, a daily newspaper with a large circulation in Spain, had published notices on its website of a real estate auction that was organized by the Spanish Ministry of Labour and Social Affairs. As the notices had not been removed from the website twelve years later upon request, the data subject filed a complaint with the Spanish Data Protection Authority ('DPA') against the newspaper, as well as against Google Inc. and its local sales office in Spain. As the DPA rejected the complaint against the newspaper but upheld the complaints against Google Inc. and Google Spain SL, only questions about the liability for the undertakings in the Google group were referred to the Court of Justice.[57] Although Google Spain SL only sold advertising space under the top-level-domain ('TLD') .es, the activity was considered inextricably linked to the processing activity and, hence, the domestic rules approximated by the DPD could be invoked against Google Inc. headquartered in the USA.[58]

Indisputably, a search engine provider processes personal data for a reason, and the reason is profit maximation. By offering virtually anyone having access to the internet a service 'for free' in terms of no pecuniary costs, it attracts business on the market for advertisement space and tailored market communication.[59] However, the operator of a search engine rarely has an intention to, or interest in, directing users of the search engine to a place where information about a specific data subject is available. In *Google Spain*, the operator of the search engine could neither answer the question why notices regarding the EU citizen were retained on the website, nor why anyone searched for the notices. Hence, it was hardly Google Inc. that determined the purpose of the given processing activities.[60] Nonetheless, the Google servers that were dedicated to resolve the requests, pointed the end-user purposefully, as opposed to coincidentally, to the website where the information was to be found. Whereas Google Inc. processed the data for the purpose of selling advertising space, the data subject had filed a complaint to prevent data processing that made it possible to retrieve obsolete notices regarding the auctioning of his property online. Even if the search engine was instrumental for the infringement it did not process data for the purpose of disseminating information about the data subject.

53 Compare Article 2(2)(c) of the GDPR with Recital 18 thereof.

54 Case C–101/01 *Bodil Lindqvist*, ECLI:EU:C:2003:596 ('*Lindquist*') para 27; Case C–212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428; and Case C–345/17 *Sergejs Buivids*, ECLI:EU:C:2019:122.

55 See section 'Data protection, the rule of law and the "methodological source code" of EU law".

56 See Communication from the Commission, *Online platforms and the Digital Single Market Opportunities and Challenges for Europe*, (2016) COM 288 final. See also Case C–131/12 *Google I* (n 23).

57 Case C–131/12 *Google I* (n 23) paras 14–20.

58 Case C–131/12 Google I (n 23)para. 49.

59 See Commission report by Crémer, de Montjoye, and Schweitzer (n 35).

60 Case C–131/12 *Google I* (n 23) paras 14–15. It must be said that the EDPB Guidelines 7/2020 (n 44) are conspicuously silent on this matter.

What makes the *Google Spain* ruling problematic is that the Court of Justice explained in general terms that the provider of a search engine shall be considered the controller of a processing activity since it has a purpose that *can be distinguished* from the purpose of a legal entity providing media content.[61] This line of reasoning seems rather backwards. Why should the fact that a search engine processes data to sell advertising space as opposed to disseminating information about a data subject, make it the 'determining body' with regard to the dissemination of information about the data subject?[62] In addition to the questionable logics, such an allocation of responsibilities is suboptimal in practice. Even if a search engine would refrain from linking to places online where the personal data is to be found, the personal data will remain available on that site to be retrieved by other means until the content provider erases the information.[63] By contrast the operator of a search engine could be considered a *joint controller* that provides essential means for the end-user to retrieve online information for the coinciding purpose of attracting more customers.[64]

In *Google Spain*, only the daily newspaper could erase the notices regarding the data subject from its website.[65] A content provider making personal data available to attract clicks is the determening body and, hence, the controller, or at least a joint controller, since the information is an essential element of each processing activity.[66] Then again, as no questions about the liability for the Spanish newspaper were referred to the Court of Justice for a preliminary ruling in *Google Spain*, the Court was silent on the matter. Nonetheless, the Spanish DPD should have held also the daily newspaper liable as a controller.

In many instances, the use of a search engine can be considered a purely personal or household activity.[67] However, considering the facts in the proceedings resulting in the *Google Spain* ruling it is possible that people had other reasons to search for information about the person who had been on dire straits. Although that could *prima facie* make the end-users the controller of the processing activity, or at least a joint controller, the individual's *freedom of expression* would prevail in most proportionality tests.[68] Furthermore, there are *a fortiori* weak incentives to enforce the data protection rights against individual internet users since the personal data remains available online for other internet users to retrieve.[69] By not even discussing the possibility of holding the end-users liable as controllers in the *Google Spain* Case, the Court of Justice implicitly and categorically rejected such an impractical approach. Then again, teleology rather than formalism was the underlying *rationale* of the ruling. By recognising a far-reaching obligation for providers of online platforms to de-reference data subjects upon request, the Court of Justice set course for effective and automated data protection 'by design'.[70] Having said that, if the provider of an online platform is classified among 'controllers' the protection of personal data must be weighed against the *freedom to conduct a business* in terms of a proportionality test akin to 'fairness'. As 'fairness' is a concept that most machines have difficulties to comprehend human intervention in the decision making may nonetheless be necessary when allocating responsabilities to platform providers.[71]

A system-coherent concept of 'processor'

Since the processor acts 'on behalf' of the controller in a processing activity, they cannot be the same person.[72] A natural or legal person can be the controller for a processing activity and the processor for another, but under no circumstances both the controller and processor for one and the same processing activity.[73] If a legal entity determines the purpose and means of a processing activity, and processes the data for that purpose, the data is processed by the controller and there is no separate

61 Case C–131/12 *Google I* (n 23) paras 32–35. See also Case C–136/17 *Google III* (n 32) para 36; and Recitals 81–82 in the preamble to the GDPR. See also Art 29 WP 'Opinion 1/2008 on data protection issues related to search engines' (WP148, 4 April 2008) ('Art 29 WP Opinion 1/2008') 9; and Art 29 WP 'Opinion 5/2009 on online social networking' (WP163 12 June 2009) ('Art. 29 WP Opinion 5/2009')] 9.

62 Art 29 WP Opinion 1/2010 (n 44) 9. See also the absence of clarification in Case C–136/17 *Google III* (n 32).

63 Articles 17 and 21 of the GDPR and Recital 65 thereof. See also the EDPB search engine guidelines (n 32) 4–9. See also Case C–507/17 *Google II* (n 25).

64 See Section 'A system-coherent concept of "controller"'. Recital 18 in the preamble to the GDPR. Compare with the reasoning in Case C–131/12 *Google I* (n 23) 40.

65 Compare with EDPB search engine guidelines (n 32) 5. There are also other remedies available under civil and criminal law.

66 Case C–40/17 *Fashion ID & CO KG v Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629 ('*Fashion ID*').

67 See Case C–101/01 *Lindquist* (n 54).

68 Recital 4 GDPR. See also Section 'Data protection, the rule of law and the "methodological source code" of EU law'.

69 Recital 18 in the preamble to the GDPR. Compare with Art 29 WP Opinion 5/2009 (n 61) 5–7.

70 Articles 25 and 47 of the GDPR, Recitals 78 and 108 in the preamble to the GDPR. Case C–131/12 *Google I* (n 23) para 36.

71 Compare with Article 17(9) in Directive (EU) 2019/790 (n 34). See also Article 22 of the GDPR.

72 Art 29 WP Opinion 1/2010 (n 44) 25.

73 Ibid.

processor involved. However, when stretching the concept of 'controller' as the Court of Justice did in the *Google Spain* Case, the distinction between the 'controller' and the 'processor' collapses in a factual analysis.[74] Indeed, the 'factual' approach advocated by the EDPB easily leads astray and may casue inconsistencies in the Union legal order.. If anyone who *de facto* processes data on behalf of someone else is a 'processor, also the teleological construction of 'controller' in *Google Spain* would create inconsistencies. However, there is a formal side to the definition of 'processor' that explained the reasoning of the Court.

A processor shall pursuant to Article 28 of the GDPR be formally *appointed* by the controller and the assignment shall be specified in a contract or other legal act in accordance with EU or Member State law. Admittedly, it would be too easy for a person that processes data on behalf of the controller to escape the liability as processor, if the GDPR would apply only to those who meet the formal requirements. However, to classify anyone who *de facto* processes personal data on behalf of someone else among processors would also have odd consequences.[75] If returning to the *Google Spain* Case, it can be no doubt about that a search engine automatically resolves the searches on behalf of other legal entities.[76] However, the search engine is available for anyone to use without any formal appointment and that in turn makes it impossible for the individual conent provider or end-user to control that the data is processed in accordance with the requirements in the GDPR.[77] Even if the classification of search engine providers among controllers were strained, it would simply be incompatible with the systematics of EU law to disregard the formal requirements and consider the legal entity a processor in a factual analysis. Since the GDPR is premised on the idea of an *individualised collaboration* between the controller and the processor, where the former can *influence the activities* of the latter, albeit not necessarily control the activities, a publicly available search engine escapes the responsibilities of a processor. Hence, if the formal requirements enshrined in Article 28 of the GDPR are not met, only a principal–agent relationship could make a legal entity that processes data on behalf of someone else a 'processor'.

In contrast to operators of search engines, for instance an internet service provider ('ISP') or a provider of a social media platform or an online marketplace normally has contracts with its end-users.[78] However, these 'click-and-wrap' contracts rarely afford the end-user any real possibility to decide and, hence, do not establish a principal-agent relationsship. Having said that, a more specific task such as providing reports and statistics on behalf of the end-user may qualify as a principal–agent relationship where the service provider assumes the role as processor. However, depending on the circumstances it may also make the end-user and platform joint controllers.[79] Indeed, more clarifications about the responsibility of providers of online platforms are welcome.[80]

When it comes to the territorial scope of EU data protection law, the main reason why the *Google Spain* Court overstretched the concept of 'controller' was, as mentioned, the fact that the DPD applied only in so far as data had been processed in the context of the activities of the *controller's* EU establishment.[81] Although it was possible to extend the applicability of domestic (Spanish) law beyond the field of approximation, the Union had a duty to ensure everyone in the Union their fundamental rights.[82] Then again, this teleological approach may result in a confusion of concepts and, hence, systematic inconsistencies. In order to ensure the consistency of EU law, it was necessary to construe 'controller' more narrowly and to recognize also an EU establishment of the 'processor' as a basis for applying the Regulation. This is now the state of EU law pursuant to Article 3(1) of the GDPR.[83]

A controller or a processor in the Union and the concept of establishment

In a systematic analysis, there is no need to investigate the territorial scope of the Regulation pursuant to Article 3 of the GDPR if the controller or processor *is in the Union* at the time for the processing activity. In the

74 Compare with the need for a clear allocation of responsibilities expressed in Recital 79 in the preamble to the GDPR.

75 Art 29 WP Opinion 1/2010 (n 44) 11.

76 Art 29 WP Opinion 1/2010 (n 44)24–31. EDPB Guidelines 7/2020 (n 44) 10–11.

77 Article 28 of the GDPR.

78 See Case C–210/16 *Facebook Insights* (n 29); and Case C–191/15 *Verein für Konsumentinformation v Amazon EU Sàrl*, ECLI:EU:C:2016:612 ('*Amazon EU*').

79 Compare with Art 29 WP Opinion 5/2009 (n 61).

80 Communication from the Commission (n 56); See also the proposed Digital Service Act Package (n 34). See as to 'over-the-top' electronic communication (n 36). See also Regulation (EU) 2019/1150 of 20 June 2019 *on promoting fairness and transparency for business users of online intermediation services*, 2019 OJ L186/57.

81 See section 'Data protection, the rule of law and the "methodological source code" of EU law'.

82 Recital 81–82 in the preamble to the GDPR. See also Art 29 WP Opinion 1/2008 (n 61) 9.

83 See section 'Data protection, the rule of law and the "methodological source code" of EU law'.

perhaps unusual situation where a natural person who is in the Union is the controller of an activity, it transpires from the *Lindquist* Case that EU law applies *by default*.[84] Arguably, the situation where a natural person residing in a third country processes data for private purposes in the Union beyond the scope of Article 2(2)(c) of the GDPR could be distinguished from the situation in the *Lindquist* Case where a citizen of a Member States processed data in the Union. However, it would be inconsistent with the general effect-criterion in EU law to confine the scope of the GDPR to conduct by individuals in the Union who are citizens or residents of a Member State. Conversely, there is no extraterritorial claim for applicability of the GDPR to data processing by individuals who are in a third country at the time for the activity, even if they are EU citizens or residents. Hence, the applicability of the GDPR depends on the physical location of the individual concerned.

Contrary to the situation where a natural person processes personal data for private purposes, the place where a *self-employed natural person* is established determines the applicability of the GDPR to the processing activity. If the professional establishment is in the Union, the GDPR applies without inquiries into its territorial scope, even if the person would be in a third country at the time for the processing activity. Conversely, since the GDPR has no extraterritorial applicability it should not apply if a self-employed person who processes personal data in the course of trade when in the Union has no EU-establishment.

In the situation where the personal data is processed in the context of the activities of a *legal person* with a single establishment that is located in an EU Member State, the Regulation also applies *by default*.[85] Notably, the *employer* is normally responsible for all the data processing activities of its employees.[86] Contrary to a self-employed person with an establishment, an employee has a 'boss and a salary'.[87] If one employee determines the purpose for a processing activity and another employee processes data for that purpose, the employer is still the controller and there is no separate processor involved.[88] Digression from this vicarious liability can pursuant to the guidelines be made only if data is used 'for his or her own purposes, outside the scope and the possible control of the legal person's activities.'[89] Since the place where the employee is when processing the data is immaterial for determining whether the employer is established in the Union, the Regulation is inapplicable pursuant to Article 3(1) of the GDPR if the employee is in the Union at the time, but the employer has no EU establishment.

A natural person may be both employed and self-employed besides acting in his or her private capacity. If, for instance, a United States ('US') citizen collects information in his or her private capacity about a Spanish citizen and business partner when on holiday in Malta, the GDPR should apply.[90] However, if the person collects the data as a self-employed person with an establishment only in the USA, or as an employee of an undertaking without an EU establishment, the Regulation is inapplicable. Because it would contravene Article 3 of the GDPR to apply the Regulation without requiring that, the professional processing takes place in the context of the activities of an EU establishment. Conversely, whereas the GDPR does not apply if the individual processes data in his or her private capacity in a third country, it applies if the person processing data in a third country is self-employed and has an EU establishment or is working for an undertaking with an establishment in the Union. Hence, the territorial scope of the GDPR regarding data processing by natural persons largely depends on whether the individual acts in his or her private capacity, as self-employed or as an employee.[91]

When it comes to data processing beyond the context of the activities of an establishment ie, for private purposes, the limelight moves to temporal aspects when determining the territorial scope of the GDPR. If the US citizen in the example above would make a stop in Malta for just a few hours on the way to Morocco, it may seem arbitrary to apply EU law. If the person stays for weeks, it gets easier to accept. However, to make the time spent in the Union decisive would only bring more questions to the fore. In this connection, 'domicile' might after all appear to be a relevant criterion to take into consideration.[92] In fact, the territorial scope of leg-

84 See, eg Case C–101/01 *Lindqvist* (n 54); and Case C–40/17 *Fashion ID* (n 66).

85 See section 'Article 3 of the GDPR and extraterritorial data protection'.

86 Art 29 WP Opinion 1/2010 (n 44) 15–16.

87 Case 66/85 *Deborah Lawrie-Blum v Land Baden Württemberg*, ECLI:EU:C:1986:284; Case C–138/02 *Brian Francis Collins v Secretary of State for Work and Pension*, ECLI:EU:C:2004:172; and Case C–196/87 *Udo Stayman v Staatssecretaris van Justitie*, ECLI:EU:C:1988:475.

88 See section 'A system-coherent concept of "processor"'.

89 Art 29 WP Opinion 1/2010 (n 44) 16.

90 Compare with the discussion on the *Google Spain* Case in section 'A system-coherent concept of "controller"'.

91 See, eg Case C–55/94 *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, ECLI:EU:C:1995:411 ('*Gebhard*') para 20.

92 By contrast, the location of the ISP providing the communication services is immaterial.

islative acts relating to the GDPR is defined in terms of an establishment *or residence* in a Member State.[93] Then again, both system-coherency and teleology tell against a construction implying that third country residents processing data in the Union for private purposes would escape the scope of the Regulation. In addition, there is no Union-wide definition of 'domicile', and it would therefore need to be determined in accordance with domestic laws. It could be difficult to establish where the person is domiciled when applying the GDPR.

In order to treat the processing of personal data for personal and professional purposes by natural persons alike, it may also be tempting to stretch the meaning of 'establishment' in Article 3 of the GDPR. An individual may of course be 'established' in a community in terms of having a social status. However, an 'establishment' is something else than 'social status' under the GDPR. For instance, a self-employed person with an establishment in Northern Ireland that is established in an Irish research community still has an establishment only in Northern Ireland. In view of effcicient enforcement it is probably wise to as far as possible steer clear from making individuals liable as controllers (or processors) of processing activities. Then again, it remains to be seen to what extent ISPs and online platforms can be held liable for conduct by their clients.[94]

As recognized in the EDPB guidelines, the Union concept of 'establishment' has been defined extensively.[95] Recital 22 in the preamble to the GDPR manifests, in the same way as the preamble to the DPD did, that an 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.' However, contrary to what the EDPB seems to suggest, there is no specific notion of establishment in 'EU data protection law'.[96] In internal market law cases, the Court of Justice has explained the notion of 'establishment' by distinguishing the cross-border activity that it refers to from those classified among 'services' and 'workers'.[97]

In *Gebhard*, concerning a German lawyer who wanted to use the title 'avvocato' when practicing law in Italy, the Court expanded on the EU law concepts of 'services' and 'establishments'.[98] According to the Court, 'establishment' is a broad concept allowing an EU citizen to 'participate, on a stable and continuous basis, in the economic life of a Member State other than his State of origin and to profit therefrom, so contributing to economic and social interpenetration within the Community in the sphere of activities as self-employed persons.'[99] A fixed time frame or limited period of performance often tells in favour of a 'service'.[100] However, the Court has reiterated that the nature of the activity has to be determined in the light, not only of its duration, 'but also of its regularity, periodicity or continuity.'[101]

Infrastructure should also be taken into account when determining whether a natural or legal person participates, on a stable and continuous basis in the economic life of a Member State. According to the Court of Justice in *Schnitzer*, regarding a Portuguese company performing plastering works in Germany, the fact that a firm performed tasks in a repeat or more or less regular manner in a host Member State, without an infrastructure 'enabling it to pursue a professional activity there on a stable and continuous basis and, from the infrastructure to hold itself out to, amongst others, nationals of the second Member State, cannot be sufficient for it to be regarded as established in the second Member State.'[102] In fact, the activity may still be considered a service if the person 'has equip himself with some form of infrastructure in the host Member State (including an office, chambers or consulting rooms) in so far as such infrastructure is necessary for the purposes of performing the services in question.'[103] Conversely, if a Member State accepts letterbox companies these establishments are recognized also in EU law, unless they are involved in criminal activities such as undeclared work of course.

As mentioned, the location of data is immaterial when deciding whether a legal entity has an EU establishment.[104] As long as only natural and legal persons have rights and obligations, and computers are mere tools in the hands of man, the place of machines has no bearing on the applicability of EU law.

93 Article 1(2) Regulation (EU) 2019/1150 (n 80); Article 8(7)(b) Directive (EU) 2019/790 (n 34).

94 See section 'A system-coherent concept of "controller"'.

95 EDPB guidelines (n 1) 6.

96 Compare with EDPB guidelines (n 1) 6–7.

97 See section 'Data protection, the rule of law and the "methodological source code" of EU law'.

98 Case C–55/94 *Gebhard* (n 91).

99 Case C–55/94 Gebhard (n 91)para 25.

100 Case C–131/01 *Commission v Italy*, ECLI:EU:C:2003:96.

101 Case C–55/94 *Gebhard* (n 91) para 27.

102 Case C–215/01 *Bruno Schnitzer*, ECLI:EU:C:2003:662, para 40.

103 Case C–55/94 *Gebhard* (n 91) para 27. See nowadays Directive 2006/123/EC of 12 December 2006 on services in the internal market, 2006 OJ L376/36.

104 See section 'Data protection, the rule of law and the "methodological source code" of EU law'. Case C–191/15 *Amazon EU* (n 78) para 76. See also Case C–347/09 *Criminal proceedings against Jochen Dickinger and Franz Ömer*, ECLI:EU:C:2011:582 ('*Dickinger and Ömer*'), paras 33–34.

Article 3(1) of the GDPR and an EU establishment 'of' the controller or processor

Obviously, only an 'establishment' in the Union can be an EU establishment *of* a controller or a processor. Hence, the EDPB is wrong when maintaining that 'in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement (amounting to an 'establishment' for the purposes of Article 3(1)) if that employee or agent acts with a sufficient degree of stability.'[105] In contrast to an 'agent', an employee has no 'establishment' and even if the individual would have an 'establishment' it has no bearing on the applicability of the Regulation in case the person processes the personal data in his or capacity as an 'employee'.[106] Words have meaning, and since the territorial scope of the Regulation is pursuant to Article 3(1) of the GDPR conditioned on the existence of an EU establishment, it takes an EU establishment of a controller or a processor for the Regulation to apply under Article 3(1) of the GDPR.[107]

A legal person, as well as a self-employed person, may form part of 'a group of undertakings', that according to Article 4(19) of the GDPR consists of 'a controlling undertaking and its controlled undertakings'.[108] In Recital 37 of the preamble to the GDPR, it is clarified that an undertaking 'which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.'[109] When it comes to government-controlled processing activities, the notion of 'institutions affiliated to a central body' is used in a corresponding way.[110] If steering clear from the distribution of public powers and the organization of the State, the private 'group of undertakings' is more broadly defined than a 'corporate group' under EU corporate law. A corporate group is an economic entity consisting of parent and subsidiary units controlled by the same legal entity in terms of ownership structures, indirect investments and decision-making powers.[111] However, the 'group of undertakings' that is recognized in the GDPR, encompasses also merely *affiliated* undertakings that *process data under the control* of the determining body. Such a determining body can be a corporate group, a specific company or a self-employed person. Hence, the determining body may have a single establishment or several establishments with a 'main establishment'.

In the context of EU corporate law, the Court of Justice has reiterated that the main establishment of an undertaking is determined primarily by the place of its *registered office*, or alternatively the place of its *central administration*, and if that of some reason would be unknown, by the *principal place of its business*.[112] . Correspondingly, if a *controller* has establishments in more than one Member State, the central administration defines its main establishment pursuant to Article 4(16)(a) of the GDPR, unless another entity has the power to decide the purpose and means of the processing activity, and to implement the decisions. Similarly, if the *processor* has establishments in two or more Member States, the main establishment is determined by the place for its central administration, but if the legal entity has no central administration in the Union, the main establishment is pursuant to Article 4(16)(b) of the GDPR located 'where the main processing activities in the context of the activities of an establishment of the processor takes place to the extent that the processor is subject to specific obligations under this Regulation.'[113]

There is nothing in the letter of Articles 4(16)(a) or (b) of the GDPR that prevents the definitions of 'main establishment' from applying in case the undertaking has its central administration in a third country.[114] Consequently, a controller or a processor headquartered in a third country may have a second main establishment in the Union pursuant to the definitions in Articles 4(16)(a) or (b) of the GDPR.[115] On the surface, the importance attributed to the place of the 'main processing activities' when determining the location of a main establishment of a processor in the Union

105 EDPB guidelines (n 1) 6.

106 See for an overview S Grundmann, *European Company Law, Finance and Capital Markets* (2nd edn, Intersentia, Cambridge, 2012).

107 Fd Saussure, *Courses in General Linguistics* (trans W Baskin, ed P Meisel and H Saussy, Columbia University Press, New York, 2011).

108 See also Recital 36 in the preamble to the GDPR.

109 True, Recital 37 primarily clarifies the impact assessment procedure under Article 35 of the GDPR, and the rules in Article 47 thereof concerning adoption of binding corporate rules. But consistency requires that the definition has a more general applicability under the Regulation.

110 Article 29 of the GDPR; Recital 48 thereof.

111 See, eg Case C–107/83 *Ordre des Avocats au Bearreau de Paris v Onno Klopp of the Düsseldorf Bar*, ECLI:EU:C:1984:270.

112 See the cases on 'main establishment' under Art 54 TFEU such as Case C–212/97 *Centros Ltd v Erhvervs- og Selskabsstyrelsen*, ECLI:EU:C:1999:126.

113 See also Recital 36 in the preamble to the GDPR. L Tosini, 'Main Establishment', in C. Kuner and others (eds), *The EU Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, Oxford, 2020).

114 See eg the EDPB guidelines (n 1), referring in this context to the intra-Union data processing Case C–230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639 ('*Weltimmo*').

115 See eg Case C–210/16 *Facebook Insights* (n 29) para 65; and Case C–311/18 *Schrems II* (n 12).

pursuant to Article 4(16)(b) GDPR, may seem irreconcilable with Article 3(1) of the GDPR. If it is immaterial for the applicability of the Regulation under Article 3(1) of the GDPR whether the 'processing takes place' in the Union, how come the main establishment is defined in terms of where the 'main processing activities' take place? With a view to reconcile the two provisions, a distinction should be made between the act of 'processing' data, and a 'processing activity'. Whereas the territorial scope of data protection is abstracted from the place where equipment for data processing is located, the place for the processor's main 'processing activities' is rather determined by the human activities relating to the processing.[116] Support for such a reading is found in Recital 36 of the preamble to the GDPR, which clarifies that the 'use of technical means and technologies for processing personal data or processing activities, do not in themselves, constitute a main establishment'. Consequently, the location of the 'main processing activities' should be understood as a specification of the *principal place of the business*.

It is the main establishment that determines whether the controller or processor in a case is in the Union. If the controller or processor has a main establishment in the Union, the GDPR applies *by default*. In that case, the GDPR can be invoked in the Member State where the main establishment is located, even if the infringement would have taken place in the context of the activities of an affiliated undertaking.[117] Furthermore, if actions are brought against undertakings in more than one Member State in the same case, it is necessary to ascertain where the main establishment is located in order to determine which national DPA shall act as the lead supervisory authority pursuant to Article 56 GDPR.[118] However, in case the corporate group or group of undertakings has no main establishment in the Union, the Regulation can be invoked pursuant to Article 3(1) of the GDPR only in the Member State where data is processed in the context of the activities of an establishment 'of' the controller or processor.[119]

Notably, Article 3(1) of the GDPR extends the applicability of the Regulation beyond the existence of an affiliated undertaking in the Union that processes data under the 'control' of the controller or processor.[120] Hence, the provision encompasses three categories of establishments 'of' controllers or processors. It may be a subsidiary in a corporate group, an affiliated legal entity in a group of undertakings that processes data under the immediate control of the determining body, or an affiliated legal entity in a group of undertakings that processes data beyond the determining body's immediate control.

In *Dickinger and Ömer*, the Court of Justice clarified in a Case concerning repression of illegal online gambling, that an establishment of a legal entity requires an activity 'through a permanent presence in the host Member State, which may be done by means merely of an office managed by a person who is independent but authorized to act on a permanent basis for the operator, as would be the case with an agency.'[121] Furthermore, the Court emphasized that the agent must act as an intermediary and 'intervene' in the contact with the clients in order to constitute an establishment of the service provider. A legal entity that provides computer support or back office services does not amount to an establishment of its client.[122] However, a legal entity that on its website directs a commercial offer to a Member States, where an intervening representative is appointed, is considered having an establishment in that State. In other words, a *conglomerate* online and off-line EU establishment of the controller or processor is recognized.

Along the lines of *Dickinger and Ömer*, the Court of Justice recognized in *Weltimmo*, that a self-employed agent can be an EU establishment of the controller.[123] In this internal EU law Case, a Slovak company running websites under the TLD .hu for trade in real estate in Hungary, had ignored requests from its clients to remove personal data from a website. Since the advertisers had to pay a fee unless they removed their data from the website within a certain period, they lodged complaints with the Hungarian DPA that decided against Weltimmo s. r. o. ('Weltimmo'). In response, Weltimmo brought legal actions before a Hungarian Court and claimed that the DPA lacked jurisdiction since the controller had no registered office or branch in the country.[124] Eventually, the Case reached the Hungarian Supreme Court that stopped the proceeding

116 See section 'Data protection, the rule of law and the "methodological source code" of EU law'.

117 Case C–210/16 *Facebook Insights* (n 29) para 74.

118 See also Art 29 WP 'Guidelines for identifying a controller or processor's lead supervisory authority' (WP 244, 13 December 2006) ('Art 29 WP lead supervisory authority guidelines').

119 Case C–210/16 *Facebook Insights* (n 29) paras 50–74. See also section 'A controller or a processor in the Union and the concept of establishment'.

120 See Articles 51, 52, and 55 of the GDPR and the Art 29 WP lead supervisory authority guidelines (n 118) 5–8. See also Case C–230/14 *Weltimmo* (n 114) para 51; Case C–191/15 *Amazon EU* (n 78); and Case C–131/12 *Google I* (n 23).

121 Case C–347/09 *Dickinger and Ömer* (n 104) para 35. See also the concept of intermediaries in Dir 2000/31/EC (n 34).

122 See by contrast online platforms, in eg Case C–210/16 *Facebook Insights* (n 29).

123 Case C–230/14 *Weltimmo* (n 114) para 86.

124 Case C–230/14 Weltimmo (n 114)para 14.

and asked the Court of Justice for clarifications on *inter alia* the meaning of 'an establishment of a controller'.[125]

In the light of the objectives to be pursued, 'consisting in ensuring effective and complete protection of the right to privacy and in avoiding circumvention of national rules' the Court established, 'that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of necessary equipment for provision of the specific services concerned in the Member State in question'.[126] Furthermore, the Court emphasized that the legal representative was mentioned in the Slovak company register with an address in Hungary and 'was sought to negotiate the settlement of the unpaid depths with the advertisers'.[127] In addition, the person representing Weltimmo had a Hungarian bank account for the recovery of Weltimmo's debts, and a letter box for 'the management of its everyday business affairs.'[128] Hence, the Court concluded that the criteria in Article 4(1)(a) DPD were met when 'the controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity—even a minimal one—in the context of which' the data is processed.'[129]

When reading *Weltimmo*, it is easy to get the impression that the *controller* was established in Hungary through its representative. However, such a confusion of identity of legal entities would be untenable in any legal system. Instead, the ruling must be understood as clarifying the kind of *relationship* required to make an undertaking an EU establishment 'of' the controller or processor. As the representative in *Weltimmo* processed personal data in 'administrative and judicial proceedings' as opposed to in the course of online trade, the data was hardly processed under the authority of the controller. Hence, the agent was neither part of the controller's corporate group, nor a legal entity processing data under the immediate control of the determining body in a processing group of undertakings. Nonetheless, the affiliation and 'interference' in terms of data processing beyond the immediate control of the determining body sufficed to make the agent an establishment 'of' the controller.[130] Consistency demands that the same broad definition of an establishment 'of' a controller or processor applies under Article 3(1) of the GDPR.

In its guidelines, the EDPB suggests that all activities which are 'inextricably linked' to a given processing activity can make a legal entity in the Union an EU establishment of the controller or processor.[131] However, that is a rather fragile hypothesis. Data processing by one legal entity may be crucial for another legal entity's data processing even if they have no collaboration or even intention to collaborate. For instance, notices published online by a daily newspaper are 'inextricably linked' to data processing by the servers of a search engine that in turn facilitates the end-users' access to the notices. However, that does not make the newspaper an establishment 'of' the operator of the search engine. Only an expressed or implied *agreement* between the controller or processor and the EU establishment in accordance with general principles in civil and administrative law could constitute a genuine link to the Union. Indeed, a professional collaboration akin to a principal–agent relationship should be required for making a legal entity with an establishment in the Union an EU establishment 'of' a controller or a processor. It should also be possible to identify the controller or processor as the principal, albeit the legal entity is not necessarily in control of the EU establishment's processing activity.

Article 3(1) of the GDPR and the 'context' criterion

In its guidelines, the EDPB observes that the notion of data processing in the 'context of the activities of an establishment' embraces more situations than those where personal data is processed 'by' an establishment.[132] For instance, in *Google Spain*, trade in advertising space was considered a relevant context even though the Spanish subsidiary had nothing to do with the infringing processing activity.[133] Indeed, 'context' and 'affiliation' are two different criteria that need to be analysed separately.[134] It was perhaps easy to accept the sales office in *Google Spain* as an establishment of Google Inc., but difficult to consider trade in advertising space a relevant context for the processing activity. Conversely, in *Weltimmo* it was perhaps difficult to accept the agent as an establishment of the controller, but easier to consider

125 Case C–230/14 Weltimmo (n 114)paras 15–18.

126 Case C–230/14 Weltimmo (n 114)para 30.

127 Case C–230/14 Weltimmo (n 114)para 33.

128 Ibid.

129 Case C–230/14 Weltimmo (n 114)paras 31, 32.

130 This shall be distinguished from a 'representative' appointed under Art 27 of the GPDR as defined in Art 4(17) of the GDPR.

131 EDPB guidelines (n 1) 8.

132 EDPB guidelines (n 1) 7; Case C–230/14 *Weltimmo* (n 114); Communication from the Commission, *A comprehensive approach on personal data protection in the European Union* (n 39).

133 See section 'A system-coherent concept of "processor"'.

134 See the suggested 'threefold approach' in the EDPB guidelines (n 1) 5. However, a slightly difference approach is used here for the sake of clarity.

data processing in legal and administrative affairs to be a relevant context.

In its guidelines, the EDPB makes an effort to clarify the meaning of the required 'context' in terms of contributions made in the Union to the revenues of the controller or processor.[135] However, if 'revenue-raising' is decisive for whether data has been processed in the context of the activities of an EU establishment, all processing of data for non-commercial purposes would escape the scope of the GDPR, even if the data would be processed *by* such an establishment. In fact, the use of 'revenue-raising' as a criterion is questionable also in the course of trade, since it detaches the definition of the territorial scope of the GDPR from a kind of activity and makes results of the activity decisive for its applicability. It seems arbitrary that the GDPR would apply when data is processed in the context of the activities of a help-centre that charges a price, but not if the help-centre provides its services for free, and it would be even more arbitrary to apply the Regulation only in case the help-centres makes a profit. An argument can be made that 'revenue-raising 'should be understood as a contribution to the elusive value of 'goodwill'. However, that would only make the concept even more vague and still not cover economic activities, which do obviously not generate 'goodwill'. In fact, it is recognized in the GDPR that also commercial activities, which do not result in 'revenue-raising', can establish a sufficient link to the Union. In the context of binding corporate rules for international data transfers, the concept of 'enterprises engaged in a joint economic activity', is used to determine the applicability of the Regulation. Whereas 'revenue-raising' implies a positive result, 'economic activity' is more neutral.

Revenue-raising may be a creative way to explain why personal data was considered processed in the context of the activities of the EU establishments in *Google Spain* and *Weltimmo*, but it would create uncertainties if not confusion if elevated to a general norm. It is emphasized by the EDPB that the assessment of whether the 'context' criterion is met, 'should be carried out on a case-by-case basis and based on an analysis *in concreto*.'[136] Unfortunately, no more clarifications are provided as to what factors should be taken into account. However, it would promote consistency to consider only an activity *that contributes to the achievement of the goals of a given processing activity* to be a relevant context. Hence, the validity of the interpretative data provided in *Google Spain* must be called into question.[137]

Article 3(1) of the GDPR and the interrelations between the controller and processor

In its guidelines, the EDPB discusses whether the processor can be considered an establishment of the controller and *vice versa*. According to the EDPB, 'it is important to consider the establishment of the controller and processor separately when determining whether each party is of itself "established in the Union"'.[138] Because, the EDPB 'notably deems that a processor in the EU should not be considered an establishment of a data controller within the meaning of Article 3(1) GDPR merely by virtue of its status as processor on behalf of the controller.'[139] Perhaps, the relationship between the legal entities 'does not necessarily trigger the application of the GDPR to both, should one of these two entities not be established in the Union.'[140] However, if that should at the same time depend on analyses *in contreto* of all the relevant facts in each case, a distinction needs to be made between four different situations.

Firstly, if the controller and processor are in the Union, the GDPR should apply to both of them *by default*. If secondly, a controller in the Union has appointed a processor in a third country, the controller would be an EU establishment of the processor in case the decisive criterion would be whether the activities of the legal entities concerned are 'inextricably linked' as suggested by the EDPB. If instead at least a collaboration akin to a principal–agent relationship is required as suggested here, the controller would rarely qualify as an establishment of a legal entity processing data on its behalf. In a proper construction of Article 3(1) of the GDPR, a controller is not an 'EU establishment' of the processor since the processor does not act as the principal in the course of the professional collaboration. Having said that, a third country processor must, as explained by the EDPB, nevertheless abide by the GDPR through contractual arrangements.[141] It is, therefore, largely irrelevant for the processor's

135 EDPB guidelines (n 1) 8.

136 EDPB guidelines (n 1)7.

137 See section 'A system-coherent concept of "controller"'.

138 EDPB guidelines (n 1) 11. See also EDPB Guidelines 7/2020 (n 44) 29–40.

139 EDPB guidelines (n 1) 10.

140 Ibid.

141 Article 28 of the GDPR; and EDPB guidelines (n 1) 12–13.

liability whether an EU controller can be considered an EU establishment of the processor.

Thirdly, with regard to the reverse situation, where the processor is in the Union and the controller in a third county, the EDBP guidelines are even more puzzling.[142] In that case, data processing is according to the EDPB, not carried out in the context of the activities of an EU establishment, as 'the processor is merely providing a processing service that is not 'inextricably linked' to the activities of the controller.'[143] However, if an agent in the Union that processes data merely in relation to the controller's business activities is 'inextricably linked' to the processing activity, why should a legal entity appointed in the Union to process data on behalf of the controller categorically not be considered an EU establishment of the controller? Such a construction of Article 3(1) GDPR sits uncomfortably with the *in concreto* analysis that is tenaciously advocated by the EDPB itself. It tends to create legal inconsistencies particularly in situations where it is difficult to determine whether a person is a controller, joint controller, or processor.[144] If applying a 'factual' rather than a 'formal' analysis and deem any natural or legal person processing data on behalf of someone else a *de facto* processor, it would be problematic to consider eg an online platform provider in the Union an EU establishment of its clients in third countries. However, as discussed earlier, the absence of an individualized collaboration akin to a principal-agent relationship should in most instances tell against a classification of online platforms among 'processors' in relation to their clients.[145] By contrast, not to consider a legal entity in the Union that meets both the formal and factual requirements of a processor to be an EU establishment of a third country controller, is a systematic anomaly.

In the fourth situation, neither the controller nor the processor is in the Union at the time for the data processing. In that case, the Regulation does not apply under Article 3(1) of the GDPR unless the controller or the processor has an EU establishment. If data is processed in the context of the activities of an EU establishment of the controller, that entity is not an EU establishment of the processor. Conversely, if data is processed in the context of the activities of an EU establishment of the processor, that entity is an EU establishment of the controller only if stipulated in a contract. Hence, the requirement to confer obligations on the sub-processor enshrined in Article 28(4) of the GDPR is inapplicable, albeit the processor with an EU establishment must still abide by the Regulation.[146]

Article 3(2)(a) of the GDPR and the targeting criterion

Although the EDPB devotes a significant portion of its guidelines to Article 3(2) of the GDPR, the reasoning in this regard requires less commentary than the reasoning regarding Article 3(1) of the GDPR. Indeed, the guidelines on Article 3(2)(a) and (b) of the GDPR are mainly uncontroversial in substance, albeit sometimes unclear as discussions about different criteria are mixed.[147] Articles 3(1) and (2) of the GDPR are alternative as opposed to cumulative bases for determining the Regulation's applicability. However, in a lexical construction, there are situations where both Article 3(1) and 3(2) of the GDPR can be invoked against a controller or processor that is not in the Union when the data is processed. As the Regulation applies pursuant to Article 3(2) of the GDPR to the processing of personal data 'by a controller or processor not established in the Union' there is nothing precluding the Regulation from being applicable also under that provision in case the controller or processor with a main establishment in a third country has an EU establishment.[148] However, even if Article 3(2) of the GDPR could apply, Article 3(1) thereof takes president since the express reference to an establishment 'of' a controller or a processor overrides the silence in Article 3(2) of the GDPR on the matter, and the former provision applies more broadly to data processing beyond 'targetting' or 'monitoring'. For the sake of system-coherency, Article 3(2) of the GDPR should have mirrored the wording of Article 3(1) of the GDPR and stated that the Regulation applies to processing of personal data of data subjects who are in the Union, *unless the data is processed by a controller or pro-*

142 See section 'A system-coherent concept of "controller"'.

143 EDPB guidelines (n 1) 12.

144 See sections 'A system-coherent concept of "controller"' and "A system-coherent concept of "processor"'.

145 See section 'A system-coherent concept of "processor"'.

146 Lexically, Article 28(4) of the GDPR does not hinder such a construction, but the 'controller' should arguably be subject to the GDPR without a need to apply Article 3 thereof.

147 See eg EDPB guidelines (n 1) 15.

148 See section 'Article 3(1) of the GDPR and an EU establishment "of" the controller or processor'.

cessor in the Union, or in the context of the activities of an establishment in the Union of the controller or processor.

As recognized in the EDPB guidelines, the fact that the Regulation shall pursuant to Article 3(2) of the GDPR apply to any data subject in the Union and not only to EU citizens, is consistent with the fundamental rights to data protection enshrined in Article 8 of the EU Charter.[149] When it comes to Article 3(2)(a) GDPR, 'the offering of goods or services' implies that the data subjects are 'targeted' by a 'commercial offer'. Indeed, the GDPR should apply neither if the invitation is directed to third countries, nor if a trader reaches out to a global market without targeting a market specifically in the Union. Far from all goods or services accessible online are offered to data subjects in the Union specifically.[150] Furthermore, the Regulation can be invoked only by a data subject or in relation to that individual. Hence, three interrelated criteria must be met for the GDPR to apply under Article 3(2)(a) thereof. It applies when a commercial offer is *directed to a market* in the Union and involves the processing of personal data of *identified or identifiable* individuals who are *in the Union* at a particular time.

When it comes to the *targeting of a market* in the Union, the EDPB is right to take into account the preliminary ruling in joined Cases C–585/08 and C–144/09, concerning the *forum* in consumer law cases.[151] Article 15(1)(c) of Regulation 44/2001 ('the Brussels I Regulation') that was the subject of the investigation applies when a trader 'pursues commercial or professional activities in the Member State'.[152] Lexically, 'commercial or professional activities' embraces a broader range of activities than the 'offering of goods or services'. However, the words 'goods' and 'services' have been interpreted extensively in EU law and encompass virtually any commercial offer, which in turn constitutes an invitation to engage in an economic transaction expressed in the course of 'commercial or professional activities'. In its guidelines, the EDPB pays heed to the fact that Article 3(2)(a) of the GDPR, stipulates that goods and services can be offered irrespective of whether a 'payment' is required.[153] In a systematic analysis, this concept of commercial offers tallies with the market definitions in competition law and relates to the debate on whether personal data can be considered a 'payment'.[154]

More importantly, the EDPB discusses the factors that should according to the Court of Justice in joined Cases C–585/08 and C–144/09, *inter alia* be taken into consideration when determining whether or not a commercial offer has been directed to a national market.[155] For instance, the language, currency, and TLD used by the online trader can provide useful information about the targeting of a market. Then again, the fact that commercial offers are directed to a national market within the Union does not *per se* afford any data subject in the Union the right to invoke the GDPR against the online trader.

True, the Brussels I Regulation implicitly has bearing on personal data since it concerns consumer contracts.[156] Only an identifiable consumer can invoke the procedural rights under Article 15(1)(c) thereof. However, the EDPB is right to abstract the reasoning regarding the targeting of an *identified or identifiable person* in the Union from the criteria for targeting a market under international private law.[157] According to the EDPB, the Regulation should apply only where individuals are *intentionally targeted*. Conversely, it does not apply when data subjects are inadvertently or incidentally targeted.[158] This alludes to an 'objective intent', which is a well-known concept in competition law, meaning that the intention is ascertained from the behaviour of a legal entity, as opposed to the state of mind of individuals.[159] Furthermore, the reasoning corresponds to the distinction made in competition law between active and passive sale.[160] Such an effort to approximate the civil law protection of personal data with the legal framework for competition law interventions against eg online platforms is welcome.[161]

Finally, the temporal and spatial aspects of a data subject *being in the Union* are far from unproblematic. Naturally, a person who visits a place online under the

149 EDPB guidelines (n 1) 14–15. See also the Recital thereof.

150 Compare with M Gawronski (ed), *Guide to the GDPR* (Wolters Kluwer, Zuidpoolsingel the Netherlands, 2019) 19.

151 Joined Cases C–585/08 and C–144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmH v oliver*, ECLI:EU:C:2010:740 ('*Pammer and Alpenhof*').

152 Regulation (EU) 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, 2012 OJ L351/1.

153 EDPB guidelines (n 1) 16. See also Case C–109/92 *Stephan Max Wirth v Landeshouptstadt Hannover*, ECLI:EU:C:1993:916.

154 See decision of the Federal Court of Karlsruhe of 23 June 2020—KVR 69/19—vindicating that the decision of the German competition authority regarding abuse of market dominance by Facebook can be enforced.

155 EDPB guidelines (n 1) 17–18.

156 See Case C–191/15 *Amazon EU* (n 78).

157 Compare with Articles 77–81 of the GDPR. See also Article 22 of the GDPR.

158 EDPB guidelines (n 1) 15.

159 See eg PA Perinetto, 'Intent and Competition Law Assessment: Useless or Useful Tool in the Quest for Legal Certainty' (2019) 1 European Competition Law 153.

160 See eg Commission Notice, *Guidelines on Vertical Restraints*, OJ C131/1, 19 May 2010.

161 Compare with Commission report by Crémer, de Montjoye, and Schweitzer (n 35).

TLD of a Member State or .eu should not be considered being in the Union unless he or she is also physically present in a Member State. It makes sense that an individual residing in a Member State that stays in a third country for weeks cannot enjoy the rights specified in the GDPR, but if the person leaves the Union for some hours, it is less obvious. For instance, an Irish citizen who receives a tailored commercial offer on the way to the UK, can invoke the GDPR only if proving that he or she was 'targeted' before crossing the border. Some more clarifications in these regards would have been expected in the EDPB guidelines. Perhaps the burden of proof should be relaxed, so that the GDPR applies as soon as a person is mainly in the Union during a relevant day or week, or shifted to the legal entity seeking to be exculpated? Alternatively, the place of residence could after all be a criterion under the GDPR? It would tally with the importance of residence for procedural rights under Article 15(1)(c) of the Brussel I Regulation. As mentioned with regard to the liability for individuals that process personal data for private purposes beyond the scope of Article 2(2)(c) of the GDPR, there is no Union concept of 'domicile'. However, that is less of a problem when it comes to the right for data subjects to enforce the GDPR against controllers or processors headquartered in third countries. In parity with the reference in Article 15(1)(c) of the Brussel I Regulation to the consumer's domicile as defined in the legal systems of the Member States, a reference in Article 3(2) of the GDPR to the data subject's domicile as defined in the domestic laws, would ensure access to justice for people in the EU. Conversely, a person that is not residing in the Union may have difficulties to enforce the rights anyhow.

Article 3(2)(b) of the GDPR and the monitoring criterion

As stated in the EDPB guidelines, the concept of 'monitoring' encompasses a broad range of activities such as behavioural advertisement, geo-localization, online tracking, personalized services, CCTV, surveys, profiling, studies, and reporting on health status.[162] Furthermore, the EDPB considers the two criteria that the Regulation applies only to data subjects who 'are' in the Union and to their 'behaviour' in the Union, to be *cumulative*.[163] However, these criteria are rather tautologous. Because it is possible to monitor the behaviour of a person in the Union only if the person *is* in the Union, and it adds truly little information that the Regulation applies only with regard to the behaviour of a person in the Union. When a data subject in the Union is monitored, the Regulation applies without further inquiries.

Evidently, the wording of Article 3(2)(b) of the GDPR brings the same questions to the fore about the concept of 'data subjects who are in the Union' as those addressed in the context of Article 3(2)(a) thereof. Perhaps even more so since the data subject often has no knowledge of the time for the monitoring. Shall the GDPR apply to the entire processing activity if a data subject was in the Union at some point during the monitoring, or only to the processing of data that took place when the person was in the Union? If eg an institute established in the USA is tracking the behaviour of German citizens online in order to make projections about the outcome of a general election in Germany, the GDPR applies when reading Article 3(2)(b) of the GDPR verbatim only when the individuals are in the Union. By contrast, information collected at a time when the data subject is in a third country, escapes the scope of the GDPR. Arguably, such a construction of the fundamental rights to data protection tends to make them haphazard. Legal rights shall be foreseeable, as opposed to subject to chance. Hence, there are legitimate concerns about the criteria in Article 3(2)(b) of the GDPR. In fact, a data subject's place of residence appears to be a more relevant fact than the place where a person happens to be at a given time. However, the EDPB guidelines are silent on the matter also in these regards.

Finally, a controller or processor that escapes the scope of Article 3(1) of the GDPR but is caught by Article 3(2) of the GDPR, may need to appoint a *representative* in the Union pursuant to Article 27 of the GDPR, primarily in order to safeguarding the access to justice for all the data subjects in the Union.[164] Such a 'representative' acting professionally in the Union should either be a self-employed person with an 'establishment' in the Union, or work for an undertaking with an establishment in the Union.[165] If so, the Regulation seems to apply to the controller or processor pursuant to Article 3(1) of the GDPR. However, it would be a catch 22 to make the Regulation applicable

162 EDPB guidelines (n 1) 20. Mere use of cookies is captured by the GDPR, compare with Case C–40/17 *Fashion ID* (n 66).

163 EDPB guidelines (n 1) 19.

164 See section 'Article 3(1) of the GDPR and an EU establishment "of" the controller or processor'.

165 Article 4(17) of the GDPR. See also section 'A controller or a processor in the Union and the concept of establishment' and 'Article 3(1) of the GDPR and an EU establishment "of" the controller or processor'.

under Article 3(1) of the GDPR by a detour over Article 3(2) of the GDPR when the former provision is *prima facie* inapplicable.[166] More to the point, it is incompatible with the rule of law to make the Regulation applicable to processing activities beyond the scope of Article 3(2) of the GDPR by considering a representative appointed under Article 27 of the GDPR an establishment of the controller or processor.[167]

Conclusions

There is no such a thing as 'extraterritorial applicability' of the GDPR. Instead, a *genuine link* to the Union is required for the Regulation to apply if the controller or processor is headquartered in a third country. Such a link is established if the data is processed in the context of the activities of an establishment of the controller or processer in the Union pursuant to Article 3(1) of the GDPR. Indeed, the Regulation can be invoked in every EU Member State where the controller or processor has an establishment. If Article 3(1) of the GDPR does not apply, the regulation may still be invoked pursuant to Article 3(2) of the GDPR if the targeted or monitored data subjects are in the Union. Unless the Regulation applies pursuant to Articles 3(1) or (2) of the GDPR, the Union's data protection standards can apply to controllers or processors that are not in the Union only by virtue of public international law or private commitments.

When it comes to the basic concepts of 'controller' and 'processor', the EDPB guidelines are premised on the false assumption that a distinction can be made between a 'formal' and 'factual' approach. There is always a formal side to legal requirements and yet the black letter law must be interpreted and applied in a purposeful way when taking all factual circumstances into consideration. Indeed, the construction of 'controller' and 'processor' in EU law is properly understood only in the light of the teleology and system-coherency of the Union legal order that ultimately the Court of Justice is required by the Member States to safeguard pursuant to the EU Treaties.

Since the processor processes data 'on behalf' of the controller, the controller and processor must be two different legal entities. A formalized principal–agent relationship should be required for making a legal entity a 'processor'. Furthermore, the EU establishment 'of' the controller or processor that is required for the Regulation to apply pursuant to Article 3(1) of the GDPR, must be a separate, albeit affiliated, legal entity. It may be an entity in the same corporate group, or an affiliated entity in a group of undertakings that processes data under the immediate control of the determining body or beyond that control. In its guidelines, the EDPB suggests that any legal entity involved in an activity that is 'inextricably linked' to the processing activity would be an establishment of the controller or processer. Evidently, that is an error in logic since most interdependent processing activities are unintended. Instead, a *collaboration* akin to a principal–agent relationship in accordance with general principles of civil law or administrative law is required for the GDPR to apply under Article 3(1) thereof.

In addition to the mysteries surrounding the proposed affiliation-criterion, the EDPB defines the 'context of activities' that is required pursuant to Article 3(1) of the GDPR in terms of 'revenue-raising'. However, also this assumption is rather unconsidered. Evidently, the Regulation applies to non-commercial data processing, and even if personal data is processed in the course of trade, the result of an activity is too unpredictable a criterion. Indeed, the nature of the processing activity as opposed to the shifting results of the activity should be decisive. Tentatively, the GDPR should apply only when the EU establishment *contributes to the achievement of the goals of a given processing activity*.

In the EDPB guidelines, it is suggested that the processor shall not be considered an EU establishment of the controller and *vice versa*. Such a categorical approach sits uncomfortably with the *in concreto* analysis advocated by the EDPB itself. More to the point, it may bring normative inconsistencies in its train. However, the need to treat these entities as a Cinderella result from the fact that the construction of the criteria in Article 3(1) of the GDPR advocated by the EDPB is erroneous in the first place. If any activity that is 'inextricably linked' to a processing activity would define an EU establishment of the processor, it is difficult not to classify a controller in the Union among those establishments. By contrast, the controller is unlikely to be an EU establishment of a legal entity that processes data on its behalf if a collaboration akin to a principal–agent relationship is required. Conversely, it would be an anomaly not to consider an appointed processor in the Union an EU establishment of a third country controller. Indeed, a system-coherent approach is required by the methodological source code of EU law.

In its guidelines on Article 3(1) of the GDPR, the EDPB suggests that an 'employee' who is in a Member

166 Articles 13–14 of the GDPR; and Recital 80 thereof.

167 See section 'Data protection, the rule of law and the "methodological source code" of EU law'.

State could constitute an 'establishment' in the Union of a controller or a processor in a third country. However, the employer is normally responsible for the employees' professional data processing and the vicarious liability makes the place where the employee processes the data immaterial. If the controller or processor is headquartered in a third country, the employee's activity escapes the scope of the GDPR unless the data is processed in the context of the activities of an EU establishment. By contrast, if the natural person processes data in her or his capacity as a self-employed person, the applicability of the GDPR depends on the location of the person's fixed establishment. Furthermore, if an individual processes data for private purposes beyond the scope of Article 2(2)(c) of the GDPR, the place for the processing activity determines the applicability of the Regulation. Hence, when it comes to natural persons, the territorial scope of the regulation depends on whether the data is processed in his or her capacity as an employee, self-employed person or private person.

Finally, when it comes to Article 3(2) of the GDPR, the EDPB guidelines are less controversial and more apt. Particularly, the construction of Article 3(2)(a) is convincing. In addition, the reasoning regarding Article 3(2)(b) is credible, albeit the distinction between being in the Union and behaving in the Union is strained. Having said that, clarifications regarding the spatial and temporal aspects of being in the Union are conspicuously absent, perhaps because of the need for separate guidelines on the matter. It cannot be emphasized enough that EU law must be interpreted and applied in both a teleological and systematic way. In that connection, the 'domicile' of data subjects could perhaps be an aspect to take into account. Indeed, more clarifications regarding the meaning of being in the Union would be welcome.

doi:10.1093/idpl/ipab012
Advance Access Publication 2 June 2021