The (Extra-)territorial Scope Rules of the New European Data Protection Law from a Private International Law Perspective—A Model for South Africa?

Jonas Baumann
https://orcid.org/0000-0002-0939-8567
Research Associate
University of Johannesburg
jonasb@uj.ac.za

Nazreen Ismail
https://orcid.org/0000-0002-7117-0491
Lecturer, Department of Practical Business Law
University of Johannesburg
nismail@uj.ac.za

Abstract

Novel technical developments are a source for new business models and, at the same time, a challenge for legal systems and in particular data protection laws. A fundamental challenge in this respect is the delocalisation of data proceedings enabled by modern technologies. In addition, most cases related to such new data driven business models contain foreign elements. From a data protection perspective this raises numerous legal questions, related to the territorial scope of data protection instruments and their relation to the established rules and principles of private international law. The European General Data Protection Regulation (GDPR) addresses the delocalisation with extra-territorial scope rules, but the discussion on how those provisions are embedded in the legal framework of private international law has only started. This article will address those questions in context of the GDPR and the South African Protection of Personal Information Act (POPIA) from a comparative perspective. After a brief overview of the GDPR, the requirements of the territorial scope rules of Articles 3(1) and (2) GDPR will be examined. Thereafter, the doctrinal classification of these rules within the established categories of private international law and the question of whether a choice of the applicable data protection law is permitted within the legal framework of the EU will be investigated. In conclusion, the article examines the territorial scope of the POPIA and provides recommendations for an improvement of the existing rules *de lege ferenda*.

Keywords: data protection law; GDPR; POPIA; territorial scope; private international

UNISA university of south africa PRESS

Comparative and International Law Journal of Southern Africa
https://upjournals.co.za/index.php/CILSA
Volume 54 | Number 1 | 2021 | #8456 | 49 pages

https://doi.org/10.25159/2522-3062/8456
ISSN 2522-3062 (Online), 0010-4051 (Print)

law; conflict of laws; choice of law

Introduction*

Legal systems are constantly being challenged by innovative technological developments, that form the basis for new business models, products and services. Social media networks[1] like Facebook, Twitter and Instagram, internet search engines such as Google and providers of digital content like Spotify or hybrids of the aforementioned, for instance, the content network TikTok, spring to mind. These exemplify business models that emerged at the beginning of this millennium which had and are still having an extraordinary impact on the daily lives and routines of people around the world. They also illustrate how 'new' technologies challenge established legal concepts. These services use the World Wide Web as a base for their services and achieve impressive revenues and profits.[2]

These business models generate massive revenue from advertising and market research, which are gleaned to a large extent from the personal data of their users. In this respect, some economic scholars refer to two- or multi-sided markets or business models, which are characterised by the ability of the platform provider to attract at least two groups of platform-users, and to design the price-structure in such a way that one group pays more (high-price side) and charges less or nothing to the other group (low-price side).[3] In the light of these and other business models, personal data has gained undisputed economic value[4] and as a result has advanced to a new form of 'currency' for some transactions.[5]

* The authors are grateful for constructive comments from Prof Jan L Neels, Prof Eesa A Fredericks (both UJ) and Dr Andreas Sesing (Saarland University) on an earlier draft, and also for the insightful comments as provided by the anonymous peer-reviewers.

1 In detail on the characteristics of social networks: Anneliese Roos, 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) 129 SALJ 383 ff; a brief definition is also provided by Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking WP 163* (adopted on 12 June 2009) 4 f.

2 For example, Facebook announced a total revenue of USD 25.439 million and USD 11.378 million income (before tax) from operations for the first quarter of 2021 (See Facebook Inc, 'Facebook Reports First Quarter 2021 Results' <https://investor.fb.com> accessed 28 April 2021 and <https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-First-Quarter-2021-Results/default.aspx> accessed 29 April 2021).

3 Jean-Charles Rochet and Jean Tirole, 'Two-Sided Markets: An Overview' (2004) 40 (12 March 2004) <https://web.mit.edu/14.271/www/rochet_tirole.pdf> accessed 28 April 2021; Jean-Charles Rochet and Jean Tirole, 'Two-sided Markets: A Progress Report' (2006) 37 RAND Journal of Economics 664 f.; it should be noted, that the traditional notion of this term is much broader and could describe almost every market attracting to groups of clients, see only Marc Rysman, 'The Economics of Two-Sided Markets' (2009) 23 Journal of Economic Perspectives 125–129.

4 See only Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature 444 ff.

5 European Commission Staff Working Document, 'A Digital Single Market Strategy for Europe—Analysis and Evidence, SWD' (2015) 100 final 59; some scholars even suggest that data could be regarded as a currency in the legal sense, see Madalena Narciso, '"Gratuitous" Digital Content

However, these business models raise numerous legal questions, especially with regard to the law of contract and data protection law, which are discussed with reference to the term 'data as (counter-) performance'.[6]

Internet services, unlike traditional services, are provided neither locally nor personally, but solely via the internet and do not necessarily require the physical presence of the service provider in the country of the users who provide their personal data. In addition, other technologies enable data transfers between data centres around the world within seconds. The significant technological developments in the recent decades have led to a delocalisation of data processing.

Data protection laws have been implemented to protect citizens from the risks of modern data processing methods. From the legislator's perspective, the regulation of such laws become technically challenging because a territorial connection to state or union borders in regulating the processing of personal data seems to be impracticable.[7] Due to the ubiquity of the internet, most data protection cases contain foreign elements.[8] This raises the question of how such data protection rules are embedded in the framework of private international law, which is traditionally focused on the localisation of legal relationships. It is therefore facing unusual challenges[9] that should be met by the extra-territorial application of data protection laws, which are of particular relevance to avoid protection gaps.[10]

With the General Data Protection Regulation[11] (GDPR), the European legislature implemented a new data protection regime which aims to ensure a high level of data protection irrespective of the technology used for processing personal data.[12] The legislator was aware of the challenges imposed by the rapidly growing technological

Contracts in EU Consumer Law' (2017) EuCML 200; others oppose this position since data is, unlike money, unlimited and therefore not exclusive; Torsten Körber, 'Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien' (2017) ZUM 96.

6 See for example Philipp Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht' (2019) 5 ZfPW 148 ff; Axel Metzger, 'Dienst gegen Daten: Ein synallagmatischer Vertrag' (2016) 216 AcP 817 ff; Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' (2015) EuCML 218 ff.

7 cf Kai von Lewinski, 'Art 3 DS-GVO' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds), *Auernhammer DSGVO BDSG Kommentar* (7th edn, Carl Heymanns 2020) para 3.

8 In this sense also Martina Melcher, 'Es lebe das Territorialitätsprinzip?' in Susanne Lilian Gössl (ed), *Politik und Internationales Privatrecht* (Mohr Siebeck 2018) 129 f.

9 cf Marian Thon, 'Das internationale Datenprivatrecht der DS-GVO' (2020) 84 RabelsZ 25.

10 The 'data subject' is the person to whom particular information relates to (see GDPR Art 4(1) and POPIA s 1).

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

12 On the aspect of technology neutrality see GDPR Recital (15).

developments and the increase of processing activities.[13] These considerations are reflected in the design of the territorial scope rule of Article 3 GDPR, which also addresses controllers[14] and processors[15] not established within European Union (EU) territory.[16]

In South Africa, the Protection of Personal Information Act[17] (POPIA) was gazetted on 26 November 2013[18] but only came into force on 1 July 2020.[19] This Act, created a general data protection framework for the Republic and includes a provision regulating the territorial scope as set out in section 3(1)(b).[20]

This article will, after a brief general overview of the GDPR, analyse the territorial scope rules contained in articles 3(1) and (2) of the GDPR and provide extensive reference to the German literature since the discussion in Germany has reached a high academic level. Thereafter, the article will determine the classification of article 3(1) and (2) GDPR within the field of private international law by investigating the legal nature of these provisions. In addition, the paper will address the specific problem of whether a choice of the applicable data protection law is permitted under the GDPR. On the same basis the article will investigate the territorial scope rule of the POPIA with a focus on the question whether this makes provision for an extraterritorial application and how it fits in the private international law framework. In conclusion, suggestions for an enhancement of POPIA *de lege ferenda* based on a comparative approach will be proposed.

13 See GDPR Recital (6).

14 A 'controller' is the person determining the purposes and means of the processing of personal data (cf GDPR Art 4(7).

15 A 'processor' is a person processing personal data on behalf of the controller (GDPR Art 4(8)).

16 On the implications for African processors Alex Makulilo, 'The GDPR Implications for Data Protection and Privacy Protection in Africa' (2017) 1 Intl J Data Protection Officer, Privacy Officer & Privacy Couns 12 ff.

17 4 of 2013.

18 GG 37067 (26 November 2013) GN 912.

19 GG 11136 (22 June 2020) GN 43461, Proc R 21 of 2020 3.

20 The provisions of the POPIA are applicable since 1 July 2020, the compliance deadline was 1 July 2021 (see POPIA s 114(1)). Prior to the applicability of the POPIA, the protection of privacy was subject to the established common law principles, in detail Anneliese Roos, 'Data Protection Law in South Africa' in Alex Makulilo (ed), *African Data Privacy Laws* (2016 Springer) 196 ff; Anneliese Roos, 'Data Privacy Law' in Dana van der Merwe and others, *Information and Communications Technology Law* (2nd edn, LexisNexis 2016) 418 ff. At this stage it is unclear whether those principles will be upheld by the South African Courts.

The GDPR—A Brief Introduction

On 25 May 2018[21] the GDPR replaced[22] its predecessor, the Data Protection Directive[23] (DPD), which aimed to fully harmonise[24] EU member state laws. The reform primarily aimed to 'update' the framework in the light of technological developments and to minimise legal fragmentation.[25]

The Regulation provides a new legal framework for the EU data protection law. It serves to protect natural persons when their personal data is processed and aims to facilitate and support the free movement of personal data within the EU.[26]

Technically, the GDPR is a Regulation in terms of Article 288(2) of the Treaty on the Functioning of the EU (TFEU).[27] The paradigm shift to the instrument of a Regulation is evidence of the effort to lessen the differences in the level of data protection in the member states that existed despite the fully harmonising approach of the DPD.[28] Therefore, the data protection rules laid down in the GDPR form a legal regime on the level of EU secondary law, independent from the rules of the member states[29] and applies directly.[30] The DPD, a directive in terms of Article 288(3) TFEU, addressed the

21 See GDPR Art 99(2).

22 GDPR Art 94(1).

23 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

24 See only Case C-101/01 *Lindqvist* [2003] ECR I-12992 para 96; Case C-524/06 *Huber v Bundesrepublik Deutschland* [2008] ECR I-9725 para 51.

25 cf Mira Burri and Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 480–482, 489 f; Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53(3) CILSA 3–4.

26 See GDPR Art 1.

27 Consolidated version of the Treaty on the Functioning of the European Union.

28 See GDPR Recital (9). Also see Roos (n 25) 3–4 (outlining that 'legal fragmentation' and legal uncertainty resulting from new technological developments were the reasons for the replacement).

29 This has the consequence that the Regulation is (in general) to be interpreted autonomously and independently from national understandings. In the context of the GDPR: Jan-Philipp Albrecht and Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Teil 1 para 26 f.

30 Due to the legislative technique of so-called 'opening-clauses', allowing national legislation in designated fields, some authors describe the GDPR as a 'hybrid' between Regulation and Directive (Jürgen Kühling and Mario Martini, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?' (2016) EuZW 449; Wulf-Henning Roth, 'Datenschutz, Verbandsklage, Rechtswahlklauseln in Verbraucherverträgen: Unionsrechtliche Vorgaben für das Kollisionsrecht' (2017) IPRax 452; In detail on the opening clauses of the GDPR: Jürgen Kühling, Mario Martini et al, *Die DSGVO und das nationale Recht* (MV Verlag 2016) 2 ff; Marian Müller, *Die Öffnungsklauseln der Datenschutzgrundverordnung* (WWU Münster 2018) 168 ff).

member states to transpose its principles and rules into domestic law that did not apply directly in the member states. Under the DPD, domestic provisions contrary to the interpretation of the DPD needed to be interpreted in conformity with the Directive[31] or were inapplicable due to the precedent of EU law.[32] In relation to domestic data protection rules, the provisions of the GDPR are superior due to the precedence of EU Law[33] when identical matters are addressed.

After an outline of the regulatory changes by the GDPR, an overview of the enforcement mechanisms will be presented.

Evolution or Old Wine in New Bottles?

The GDPR is considered so influential that some authors have described it as the 'beginning of a new era in data protection law'.[34] From a material perspective the basic principles and rules of the EU data protection law, that were regulated in the DPD, remained almost 'untouched'.[35] The legislator upheld established concepts, especially with regard to elementary rules, such as the material scope (Article 2 GDPR) and the legality of processing (Article 6(1) GDPR). From a material perspective, the GDPR applies 'to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'[36] With regard to these provisions, the change of the legislative instrument has a rather limited impact on the interpretation of data protection rules by the ECJ, since the Court interprets EU Law autonomously and independently from member state law.[37] This also applies to data protection law.[38] The 'phenomenon' that the Court adopted the interpretation of the 'old'

31 On the interpretation in conformity with EU Directives in general Wulf-Henning Roth and Christian Jopen, 'Die richtlinienkonforme Auslegung' in Karl Riesenhuber, *Europäische Methodenlehre* (3rd edn De Gruyter 2015) para 3–38. See also in context of the DPD *Johnson v Medical Defence Union* [2007] EWCA Civ 262 para 16 and in context of Art 2(f) and 5 Directive 2002/58/EC and Art 2(h) DPD *Bundesgerichtshof*, Judgment (28 May 2020) Case No I ZR 7/16 [2020] NJW 2545 f para 50–55 'transforming' the objection rule of s 15(3) of the German Telemedia Act into a consent requirement.

32 See the leading case in this respect: Case 6/64 *Costa v E.N.E.L.* [1964] ECR 587.

33 See (n 32).

34 Jürgen Kühling and Florian Sackmann, 'Datenschutzordnung 2018—nach der Reform ist vor der Reform?!' (2018) NVwZ 681; similarly Peter Schantz, 'Die Datenschutz-Grundverordnung—Beginn einer neuen Zeitrechnung im Datenschutzrecht' (2016) NJW 1841.

35 See Kühling and Martini, (n 29) 451; Kühling and Sackmann, (n 34) 681.

36 GDPR Art 2(1).

37 In general, on the autonomous interpretation of EU law: Case 283/81 *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health* [1982] ECR 3417 para 19; Sebastian A Martens, *Methodenlehre des Unionsrechts* (Mohr Siebeck 2013) 335 ff; Karl Riesenhuber, '§ 10 Die Auslegung' in Riesenhuber (n 31) para 4 ff.

38 See for example Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände —Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801 para 47.

provisions of the DPD in context of the 'new' provisions of the GDPR,[39] is therefore not surprising, since the paradigm shift regarding the change of the legislative instrument does not diminish the European origin of those interpretations.

On the other hand, the GDPR has brought clarification to certain aspects but introduced new rules, such as the Territorial Scope Rule in Article 3(2) GDPR, which raises legal uncertainty.

Enforcement Mechanisms

The GDPR aims to address public law as well as private law matters, therefore, data protection law can be classified as a cross-sectional matter.[40] The enforcement mechanisms provided by the GDPR reflect this dual approach, since the Regulation provides rules for public as well as private enforcement. In this respect, the change from a directive to a regulation, effected a higher level of harmonisation, excluding milder data protection rules and enforcement practices by certain member states.[41] Violations of GDPR provisions form the basis for actions by the independent supervisory authorities, designated non-profit organisations[42] and private persons, especially the data subject itself.[43]

Supervisory authorities play a major role in the enforcement of the GDPR and have a wide range of competences which include investigative,[44] corrective[45] as well as authorisation and advisory powers.[46] An important authoritative mechanism is fines as provided for in terms of Article 83 GDPR. The authorities can impose fines of up to €20 million or four *per cent* of the total worldwide annual turnover of the preceding financial year of a company for the infringement of designated data protection rules.[47]

39 See for example Case C-507/17 *Google LLC v Commission nationale d' l'informatique et des libertés (CNIL)* [2019] EU:C:2019:772 para 48 ff. (in context of GDPR Art 3(1)); *Planet49* (n 38) para 60 ff (in context of GDPR Art 4(11)); Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* [2020] ECLI:EU:C:2020:559 para 83 (in context of GDPR Art 4(2)) para 94 (in context of Art 45(1) GDPR), para 107 and 109 (in context of GDPR Art 57(1)).

40 On the implications of this regulatory approach for International Private and Public Law and the problems of a classification as a public law or private law matter in context of the EU Data Protection Law for example Melcher (n 8) 130 ff.

41 Burri and Schär (n 25) 489 (referring to Ireland).

42 See GDPR Art 80.

43 GDPR Art 79(1).

44 GDPR Art 58(1).

45 GDPR Art 58(2).

46 GDPR Art 58(3).

47 GDPR Art 83(5), (6).

Recent cases have shown that the data protection authorities of the member states are not hesitant to fine companies located outside the EU.[48]

In addition, Article 82 GDPR implemented a civil law claim for compensation and damages owed to any person who suffered material or non-material damages resulting from an infringement of the GDPR.

The Territorial Scope of the GDPR

In the light of the afore-mentioned enforcement mechanisms, the territorial scope of the GDPR is of particular relevance for processors since it determines whether one must comply with the strict data protection rules imposed by the Regulation. Article 3(1) GDPR pertains to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU. Article 3(2) GDPR addresses the extra-territorial application of the Regulation. According to this provision, the Regulation applies to controllers not established within the EU in the following situations, namely, the processing of personal data related to the offering of goods or services irrespective of whether a payment of the data subject is required, to such data subjects in the Union and for the purpose of monitoring the behaviour of such data subjects as long as it takes place within the EU. This extensive definition of the territorial scope of the Regulation[49] provides that all EU-related processing is addressed by the GDPR to prevent the deprivation of data subjects' rights under the Regulation by processing undertaken in third states.[50] Therefore, Article 3 GDPR seeks to introduce a level playing field, providing equal competitive conditions and data protection requirements for enterprises located within or outside the EU.[51]

48 See for example the penalty of fifty million Euro against *Google LLC* by the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés—CNIL*). See CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC' (CNIL 21 January 2019) <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> accessed 29 April 2021. This fine was upheld by the *Conseil d'Etat*, Decision (19 June 2020), Case N°430810 [2020]—*SOCIÉTÉ GOOGLE LLC*.

49 Some scholars criticise the combinatory approach of GDPR Arts 3(1) and (2) to apply the establishment as well as the market-place principle to be incompatible with the *comitas* approach, in detail Melcher (n 8) 141 ff.

50 cf GDPR Recital (23) s 1; Carlo Piltz, 'Die Datenschutz-Grundverordnung Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung' (2016) K&R 558; Bernd Schmidt, 'Art 3 DS-GVO' in Juergen Taeger and Detlev Gabel (eds), *Kommentar DSGVO – BDSG*, (3rd edn, R&W 2019) para 1.

51 Von Lewinski (n 7) para 2; see also Jan-Philipp Albrecht, 'Das neue EU-Datenschutzrecht— von der Richtlinie zur Verordnung' (2016) CR 90; Björn Steinrötter, 'Feuertaufe für die EU-Datenschutz-Grundverordnung—und das Kartellrecht steht Pate' (2018) EWS 64; Thon (n 9) 41.

After a clarification of the relation between Article 3(1) and (2) GDPR, the requirements of these provisions will be examined in detail.

The Relation between Article 3(1) and Article 3(2) GDPR

The wording of Article 3 GDPR suggests an exclusive relation between Article 3(1) and (2) GDPR and that the latter only applies in cases where no establishment of the controller is located within the EU.[52] Therefore, Article 3(1) GDPR is classified as the primary rule to determine the scope of the GDPR and only when the requirements of this provision are not met, Article 3(2) GDPR should be applied as a secondary rule.[53]

A literal interpretation of these provisions would result in the GDPR being inapplicable in cases where international corporations maintain an establishment within the EU but the relevant processing falls within the activity of an establishment outside the EU.[54] Insofar as it is submitted, Article 3(2) GDPR should be interpreted extensively to avoid protection gaps.[55]

The 'Establishment' Rule

Pursuant to Article 3(1) GDPR, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not ('establishment'-principle[56]). The European Court of Justice (ECJ) clarified the

52 Alexander Golland, 'Der räumliche Anwendungsbereich der DS-GVO' (2018) DuD 351.

53 Golland (n 52) 351 f; Stefan Hanloser, 'Art 3 DS-GVO' in Heinrich Amadeus Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht* (35th edn, CH Beck 2020) para 2 f.

54 In detail Golland (n 52) 352; Carlo Piltz, 'Art. 3' in Peter Gola (ed), *Datenschutz-Grundverordnung VO (EG) 2016/679 Kommentar* (2nd edn, CH Beck 2018), para 35 f; Piltz (n 50) 559.

55 Golland (n 52) 352; see also Lukas Feiler, Nikolaus Forgó and Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, GLP 2018) Art 3 para 7; Manuel Klar, 'Art 3 DS-GVO' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung/BDSG Kommentar* (3rd edn, CH Beck 2020) para 60.

56 The terms 'territoriality principle' and 'seat principle' are rightfully considered to be unprecise, in greater detail on the terminology Wolfgang Däubler, 'Das Kollisionsrecht des neuen Datenschutzes' (2018) RIW 406 and Thon (n 9) 32 in fn 42.

interpretation of the requirements of Article 4(1)(a) DPD[57] in several decisions.[58] This provision is referred to as the 'predecessor'[59] provision of Article 3(1) GDPR. Unlike Article 3(1) GDPR, its predecessor needed to be transposed into domestic law by the member states, which created legal uncertainty in some cases due to imprecise regulatory concepts on a national level.[60]

The reasoning of the ECJ in the *Google LLC v CNIL* judgment from 2019 suggests that Article 4(1)(a) DPD and Article 3(1) GDPR regulate identical requirements.[61] Several scholars agree that the case law of the ECJ, in the context of Article 4(1) DPD, should be used with care when interpreting Article 3(1) GDPR.[62] Others consider this adaption to be problematic due to implementation of the market-place principle by virtue of Article 3(2) GDPR.[63]

'Establishment' in the EU

The ECJ follows a 'flexible definition' regarding the interpretation of what is required of an 'establishment'.[64] The establishment is to be determined independently from the

57 DPD Art 4(1) had—as far as relevant for the purposes of this article—the following wording: 'Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; […]
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.'

58 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317 para 45 ff; Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] EU:C:2015:639 para 28 ff; Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] EU:C:2016:612 para 75 ff; Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] EU:C:2018:388 para 52 ff.

59 See the terminology used by Golland (n 52) 351.

60 See for example the criticism towards the German transposition in s 1(5) *Bundesdatenschutzgesetz* (as introduced by *Bundesgesetzblatt* I (2001) 904 ff) by Georg Borges, '§ 9 Cloud Computing mit Auslandsbezug' in Georg Borges and Jan Geert Meents (eds), *Cloud Computing* (CH Beck 2016), para 8 who criticises the fragmentary transposition and the high complexity of the domestic regulatory mechanism.

61 See Case C-507/17 *Google LLC* (n 39) para 48.

62 Piltz, 'Art 3' (n 54) para 8; Steinrötter (n 51) 63; Thon (n 9) 33.

63 Gerrit Hornung, 'Art. 3 DSGVO' in Spiros Simitis, Gerrit Hornung and Indra Spiecker gen Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019) para 30.

64 *Weltimmo* (n 58) para 29.

statutory seat[65] or the legal form[66] of a controller. In terms of Article 4(1)(a) DPD, the ECJ provided the definition of establishment as it 'extends to any real and effective activity, even a minimal one, exercised through stable arrangements.'[67] As a result of the retention of the wording of Recital (19) DPD in Recital (22) GDPR it is assumed that this definition was adopted by Article 3(1) GDPR.[68]

In several decisions on the DPD, the ECJ developed more detailed criteria to assess the existence of an 'establishment'. In the *Weltimmo* decision, the ECJ ruled that a single agent in a website directed to the relevant State combined with a bank account and a PO Box located in that State were sufficient to affirm an establishment.[69] The ruling was partially interpreted that the localisation of resources in a member state is not a mandatory requirement of an establishment.[70] In the *Amazon* case, the ECJ ruled that the mere accessibility of a website from a particular member state is insufficient.[71] The same applies, according to some scholars, to technical equipment (such as servers) without any human activity.[72] The ECJ also ruled that branches of social networks[73] or internet search engines[74] renting out advertising space to customers effectively and genuinely exercise activities within the member states. This was recently confirmed in *Google LLC v CNIL*, where the ECJ adopted the reasoning provided under Article

65 ibid.

66 *Weltimmo* (n 58) para 28; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 54; see also Recital (22) s 3 GDPR.

67 *Weltimmo* (n 58) para 31; *Verein für Konsumenteninformation* (n 58) para 75.

68 Daniel Ennöckl, 'Art 3 DSGVO' in Gernot Sydow, *Europäische Datenschutzgrundverordnung* (2nd edn, Nomos 2018) para 4; Stefan Ernst, 'Art. 3 DS-GVO' in Boris Paal and Daniel Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (3rd edn, CH Beck 2021), para 6; Golland, 'Der räumliche Anwendungsbereich der DS-GVO' (n 52) 352 f, 357; Klar (n 55) para 41; Piltz, 'Art. 3' (n 54) para 7 f; Piltz (n 50) 558; Kai-Uwe Plath, 'Artikel 3 DS-GVO' in Kai-Uwe Plath, *DS-GVO/BDSG* (3rd edn, Dr Otto Schmidt 2018) para 8; Peter Schantz, in Peter Schantz and Heinrich Amadeus Wolff, *Das neue Datenschutzrecht* (CH Beck 2017) para 324; Mirko Wieczorek, 'Der räumliche Anwendungsbereich Der EU-Datenschutz-Grundverordnung' (2013) 37 DuD 647; see also Dan Jerker Svantesson, 'Art 3 GDPR' in Christopher Kuner, Lee Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford 2020), sub-s C 6.

69 *Weltimmo* (n 58) para 31 ff.

70 Hanloser (n 53) para 15.

71 *Verein für Konsumenteninformation* (n 56) para 76; similar the argument in *Soriano v Forensic News LLC* [2021] EWHC 56 (QB) para 64.

72 Däubler (n 56) 407; Klar (n 55) para 46; Wieczorek (n 68) 647; a different approach is argued by Schantz, in Schantz (n 66) para 330 qualifying the mere use and operation of a server in the EU as a virtual establishment.

73 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 55; in the case *Facebook Germany GmbH* was the relevant establishment of *Facebook Inc* and *Facebook Ireland Ltd* in Germany.

74 *Google Spain* (n 58) para 49; In this case *Google Spain*—a subsidiary of *Google Inc*—was considered to be the relevant establishment in Spain even though the search engine itself was operated by *Google Inc*.

4(1)(a) DPD in the context of search engines, when interpreting Article 3(1) GDPR.[75] Such branches can be classified as an establishment, even when they are organised as subsidiary company.[76]

Processing 'in Context of the Activity' of an Establishment

Article 3(1) GDPR requires that the processing takes place 'in the context of the activity' of an establishment of the controller. A processing 'by' the establishment itself is not required.[77] In several decisions on Article 4(1)(a) DPD, the ECJ stated that this requirement cannot be interpreted restrictively.[78] In cases concerning internet search engines and social media networks, the ECJ inferred that a processing takes place in the context of the activity of an establishment when it is 'inextricably linked' to the processing of personal data by the controller within the main proceedings.[79] The court assumes such an 'inextricable link' when the service carried out by the establishment supports the profitability of the main service and when the main service itself provides the basis for the service operations of the establishment.[80] This interpretation was recently adopted by the ECJ under Article 3(1) GDPR.[81] This illustrates that the establishment rule has been extended by an extraterritorial dimension by virtue of case law.

The 'Market-Place' Rule

Article 3(2) GDPR introduces the 'market-place' principle[82] and provides that the GDPR applies in instances where the controller or processor is not established in the EU. The GDPR applies by virtue of Article 3(2) GDPR when processing activities are related to the offering of goods or services to data subjects within the EU or to the monitoring of the behaviour of such persons. This provision addresses the processing of personal data in internet cases.[83] In this context, some scholars opine that the GDPR

75 *Google LLC* (n 39) para 49 ff.

76 Recital (22) s 3 GDPR; see also *Google Spain* (n 58) para 48 f; *Weltimmo* (n 58) para 28; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 54 (all referring to Recital (19) DPD).

77 *Google Spain* (n 58) para 52; *Weltimmo* (n 58) para 35; *Verein für Konsumenteninformation* (n 58) para 78; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 57.

78 *Google Spain* (n 58) para 53; *Weltimmo* (n 58) para 25; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 57.

79 *Google Spain* (n 58) para 56; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 60.

80 *Google Spain* (n 58) para 55 f; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 60; *Google LLC* (n 39) para 50.

81 *Google LLC* (n 39) para 49 ff.

82 See for example Albrecht (n 51) 90; Golland (n 52) 351; Schantz (n 34) 1842.

83 Niko Härting, 'Starke Behörden, schwaches Recht—der neue EU-Datenschutzentwurf' (2012) BB 462; Manuel Klar, 'Die extraterritoriale Wirkung des neuen europäischen Datenschutzrechts' (2017) DuD 534; Wieczorek (n 68) 647, 648.

provides a 'worldwide scope'.[84] The interpretation of this provision comes with significant uncertainty because no reported case law from the ECJ on the interpretation of Article 3(2) GDPR exists (as yet). A variety of interpretations has been submitted by scholars.

Offering Goods or Services to Data Subjects in the EU

Article 3(2)(a) GDPR requires that the controller offers goods or services to data subjects located within the EU. This raises three questions regarding the interpretation of those requirements. Firstly, when is a data subject located 'in the EU'; secondly, what is meant by 'goods and services'; and thirdly, what does an 'offering' of goods and services in this context require. The interpretation of this provision comes with uncertainty since case law is rarely reported and the scholarly positions are not settled in many aspects.

Data Subjects Located in the EU

The wording of Article 3(2)(a) GDPR ('data subject in the Union') suggests that the actual location of a natural person is the relevant criterion, however, the spectrum of opinions in this context is broad. The majority favours a literal interpretation and refers to the actual location as the only relevant criterion.[85] Other scholars follow more restrictive approaches. Some argue for a recourse to the domicile of a person,[86] whereas others consider the 'habitual residence' of a person to be crucial, arguing that a recourse to the actual location would render it impossible for certain service providers to recognise when the Regulation applies.[87] A fourth opinion argues to consider the actual location and the habitual residence as an alternative criteria.[88] The nationality of the data subject is not considered as a relevant factor.[89]

In the context of web services, especially with applications where the processing is governed from a third-state establishment, an overly restrictive interpretation could lead

84 Makulilo (n 16) 17; compare also Härting (n 83) 462.

85 Klar (n 55) para 64; Plath, 'Artikel 3 DSGVO' (n 68) para 13; Philip Uecker, 'Extraterritorialer Anwendungsbereich der DS-GVO' (2019) ZD 68; Thomas Zerdick, 'Art. 3 DS-GVO' in Eugen Ehmann and Martin Selmayr (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, CH Beck 2018) para 17.

86 Maxi Nebel and Philipp Richter, 'Datenschutz bei Internetdiensten nach der DS-GVO— Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf' (2012) ZD 410; Alexander Roßnagel, Maxi Nebel and Philipp Richter, 'Besserer Internetdatenschutz für Europa—Vorschläge zur Spezifizierung der DS-GVO' (2013) ZD 104.

87 Golland, 'Der räumliche Anwendungsbereich der DS-GVO' (n 50) 355 f.

88 Georg Borges, 'Internationale Anwendbarkeit der DS-GVO und Zuständigkeit der Aufsichtsbehörden' in Nikolaus Forgó, Marcus Helfrich and Jochen Schneider (eds), *Betrieblicher Datenschutz* (3rd edn, CH Beck 2019) para 128.

89 Plath (n 68) para 15; Svantesson (n 68) sub-s C 7 1; compare also GDPR Recital (14) s 1.

to the data subject losing its protection by leaving the territory of the EU.[90] For persons staying in the EU for a short period of time and not striving for social integration, the criterion of the 'habitual residence' would create a protection gap since the protection of the Regulation is designed to be independent from the place of residence.[91] Therefore, an alternative recourse on the actual stay and the habitual residence appears to be beneficial.

The Offering of 'Goods and Services'

The provision also requires that the processing activities are related to the offering of goods and services.

By referring to 'goods' and 'services' the Regulation adopted two established legal terms in the EU framework. Accordingly, scholars propose an interpretation of 'goods' in accordance with Article 28(2) TFEU.[92]

To define the term 'services' the adoption of the definition by the Service-Directive[93] and Article 57 TFEU is proposed.[94] This definition includes any self-employed economic activity which is normally provided in exchange for remuneration.[95]

Article 3(2)(a) GDPR clarifies that the application of the provision is independent of a payment by the data subject. As a result, the *Oberlandesgericht Frankfurt am Main* ruled that the terms 'goods' and 'services' are to be interpreted in an extensive manner.[96]

Based on the afore-mentioned interpretation of the term 'services', it is inferred that business models funded by advertising activity and other services that require the provision of personal data by the data subject as 'counter-performance' are addressed by this provision.[97] This leads to the outcome that the web-services provided by social media networks[98] and other two- or multi-sided internet business models can be classified as 'services' under Article 3(2)(a) GDPR.

90 Borges (n 88) para 127.
91 ibid with recourse to GDPR Recital (14) s 1.
92 Schantz, in Schantz (n 68) para 333; Wieczorek (n 68) 647.
93 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.
94 Borges (n 88) para 132; Klar (n 55) para 71 f; Plath (n 68) para 18; Schantz, in Schantz (n 68) para 333; von Lewinski (n 7) para 13; Wieczorek (n 68) 647; Zerdick (n 85) para 18.
95 See the definition of Art 4(1) Directive 2006/123/EC.
96 *Oberlandesgericht Frankfurt am Main*, Judgment (6 September 2019) Case No 16 U 193/17 [2019] ZUM-RD 82.
97 Schantz, in Schantz (n 68) para 333; see also von Lewinski (n 7) para 14.
98 Borges (n 88) para 132; Alexander Roßnagel, Maxi Nebel and Philipp Richter, 'Was bleibt vom europäischen Datenschutzrecht?—Überlegungen zum Ratsentwurf der DS-GVO' (2015) ZD 456; Schantz, in Schantz (n 68) para 333.

The ‘Offering’ of Goods and Services

The question of which requirements are to be placed in an ‘offering’ in terms of Article 3(2)(a) GDPR is of considerable relevance for the application of the GDPR. The interpretation of this requirement is partly addressed by Recital (23) GDPR which states that the mere accessibility of a website or the use of a general language or currency is not sufficient to assume an ‘offering’. This Recital refers in large parts to the criteria developed by the ECJ in the *Hotel Alpenhof and Pammer* decision where the Court provided criteria to determine whether a professional ‘directs’ his business activity to a member state[99] in terms of Article 15(1)(c) Brussels I Regulation[100] which has been adopted under Article 6(1)(b) Rome I Regulation[101] and Article 17(1)(c) Brussels I*bis* Regulation[102].[103] The subjective intention of the controller is therefore the decisive criteria for an ‘offering’ in this sense.[104] This intention must become apparent in some way as it requires objective circumstances to be taken into account.[105] In the English case of *Soriano v Forensic News LLC*,[106] the court ruled that the mere fact of offering shipping to the UK is not sufficient in this context.

The majority of scholars argue that the requirements of ‘offering’ and ‘directing’ are comparable[107] and propose to adopt the aforementioned ECJ case-law to clarify the term ‘offering’.[108] The *European Data Protection Board* provided a catalogue of criteria specially designed for the application of Article 3(2)(a) GDPR which are based on the

99 See Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Heller* [2010] ECR I-12570 para 76 ff.

100 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

101 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

102 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

103 Francesca Ragno, ‘Article 6’ in Franco Ferrari (ed), *Concise Commentary on the Rome I Regulation* (2nd edn, Cambridge 2020) para 10, 102, 113.

104 Golland (n 52) 356; Schantz, in Schantz (n 68) para 334; Zerdick (n 85) para 19.

105 cf Zerdick (n 85) para 19.

106 (n 71) para 66.

107 Borges (n 88) para 136; Maja Brkan, ‘Data Protection and Conflict-of-Laws: A Challenging Relationship’ (2016) 2 EDPL 338; Golland (n 52) 356; Carlo Piltz, ‘Der räumliche Anwendungsbereich des europäischen Datenschutzrechts’ (2013) K&R 297; Schantz (n 34) 1842; Zerdick (n 85) para 19. This conclusion has already been indicated by the ECJ case law in the context of DPD Art 4(1)(a), where the court had already used the term ‘orientates’; see *Google Spain* (n 58) para 60.

108 Golland (n 52) 356; Jan D Lüttringhaus, ‘Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21. Jahrhunderts’ (2018) 117 ZVglRWiss 63; Piltz (n 107) 297; Schantz (n 34) 1842; Zerdick (n 85) para 19; see also Borges (n 88) para 137 ff who considers further circumstances to be relevant.

criteria developed in *Hotel Alpenhof and Pammer*.[109] This approach is welcomed since it avoids contradictions between the interpretation of Article 3(2)(a) GDPR and the provisions of the Brussels I*bis* and the Rome I Regulation with reference to the criteria developed by the ECJ.[110] Article 6(1)(a) Rome I Regulation and Article 17(1)(c) Brussels I*bis* Regulation differ from Article 3(2)(a) GDPR which does not require a contract to be concluded.[111]

Monitoring of Data Subjects in the EU

The GDPR also applies to the processing by a controller not established in the EU who monitors the behaviour of data subjects in the EU.[112]

The term 'monitoring' is not defined by the Regulation but some remarks on its interpretation are provided in a Recital.[113] The rule explicitly addresses internet-services[114] and, according to Recital (24) GDPR, should apply when the internet-activity of a data subject is tracked in such a way that the controller is able to create a personal profile of this particular person; especially when the profile serves to make decisions about the particular data subject or to analyse or predict its preferences, behaviours and attitudes. Therefore, all services using cookies to trace a particular user in order to provide personalised advertisements to the user are addressed.[115]

The degree of intensity of the 'monitoring' is disputed as some authors hold that the use of any application to provide personalised advertisement is sufficient[116] whereas others argue for a more restrictive interpretation indicating that a certain 'surveillance' would

109 EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) from 12 November 2019, Version 2.1, 17 f (European Data Protection Board, 12 November 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf> accessed 29 April 2021.

110 cf the references (n 105).

111 Golland (n 52) 356; Klar (n 55) para 66; Piltz (n 54) para 28; Piltz (n 50) 559; Uecker (n 85) 68 f.

112 GDPR Art 3(2)(b).

113 GDPR Recital (24).

114 Klar (n 55) para 92; Zerdick (n 85) para 20; see also Uecker (n 85) 69 f emphasising that the rule does not exclusively apply to online cases.

115 Borges (n 88) para 147; Jens Eckhardt, 'EU-DatenschutzVO—Ein Schreckgespenst oder Fortschritt?' (2012) CR 196; Härting (n 83) 462; Klar (n 55) para 98; Piltz (n 50) 559; Wieczorek (n 58) 648; Zerdick (n 85) para 20.

116 Schantz (n 34) 1842; Wieczorek (n 68) 648.

be required.[117] Others emphasise that 'monitoring' means the knowledge-profit resulting from the collection and assembly of data.[118]

Furthermore, it is required that such tools are used to monitor the behaviour of data subjects in the EU as long as it takes place within this territory. Scholars submit that the GDPR therefore applies to all enterprises established in third states that collect information about EU citizens for economic purposes.[119] This applies, in particular, to social media providers[120] and providers of digital content[121] that use cookies[122] or other analytical tools to track users and provide personalised advertisements.

The (Unclear) Role of the Representative in Terms of Article 27 GDPR

In order to examine the full concept of the extra-territorial application of the GDPR, the legal consequences for the controllers and processors of such an application need to be examined. Where Article 3(2) GDPR applies, controllers and processors shall designate a representative in the EU.[123] The representative is a natural or juristic person established in the EU, designated in writing by the controller or processor, who represents the controller or processor regarding their respective obligations under the GDPR.[124]

The functions and the legal status of the representative are controversial. Article 27(4) GDPR provides that the representative serves as a contact point for supervisory authorities and data subjects for all questions relating to processing operations and compliance with the GDPR. Some scholars identify the establishment of a contact point in the EU to be the *ratio legis*.[125] Others submit that Article 27 GDPR also serves the

117 Manuel Klar, 'Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts—Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen' (2013) ZD 109 at 113; more liberal probably, Klar (n 55) para 95 who states clearly that systematic and broad surveillance activity is not required; compare *Soriano v Forensic News LLC* (n 71) para 68, where the court indicated that a connection between the monitoring and the claim is required.

118 Borges (n 88) para 149.

119 Brkan (n 107) 340.

120 See, for example, regarding Facebook the findings in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 34 ff; see also Twitter, 'Our Use of Cookies and Similar Technologies' <https://help.twitter.com/en/rules-and-policies/twitter-cookies> accessed 29 April 2021.

121 For example, Spotify, 'Spotify Cookie Policy' (15 July 2019) sub 2 <https://www.spotify.com/za/legal/cookies-policy/> accessed 29 April 2021.

122 Cookies can be defined as 'text files which the provider of a website stores on the website user's computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour' (see the definition of the ECJ in Case C-673/17 *Planet49* (n 38) para 31).

123 GDPR Art 27(1).

124 See GDPR Art 4(17).

125 Kai-Uwe Plath, 'Artikel 27 DSGVO' in Plath (n 68) para 1.

purpose to establish an additional liability subject besides the controller or processor.[126] Accordingly, it is argued that the representative is a separate 'object of obligation and enforcement' alongside the controller or processor.[127] On the other hand, the prevailing opinion rejects any liability of the representative for infringements of the GDPR by the represented entity.[128] This is supported by a systematic argument since Article 79 and 82 GDPR do not provide for passive legitimation of the representative.[129]

This is cause for legal uncertainty, until either the European legislature or the ECJ clarifies the legal position on potential liability of the representative in this context.

Article 3 GDPR in the Scope of Private International Law

The following subsection of this article will investigate the legal nature of Article 3 GDPR from a private international law perspective and assess whether a choice of the applicable data protection law is permitted under the GDPR.

The Classification of Article 3 GDPR in Private International Law

The classification of the legal nature of Article 3 GDPR in the established categories of private international law is discussed controversially. Regarding the predecessor, Article 4 DPD, the discussion was relatively settled as indicated below, before addressing the latter question in context of Article 3 GDPR.

The Legal Nature of Article 4 DPD—The 'Predecessor'

Under Article 4(1)(a) DPD, the applicability of the member state data protection law depended primarily on whether the processing was carried out in the context of the activities of an establishment of the controller in that member state. The provisions of Article 4(1) DPD also regulated the extra-territorial application of the directive which depended on international public law or the use of equipment situated in the EU.

This provision had two functions. Firstly, it determined the relationship between European and third-state data protection laws; secondly, it ascertained which member state data protection law was applicable in the event of a dispute.[130] The latter function was required due to the legal nature of the DPD, as a directive in terms of Article 288(3)

126 Stefan Hanloser, '27 DS-GVO' in Wolff (n 53) para 1; Carlo Piltz, 'Art. 27 DS-GVO' in Gola (n 54) para 8, 10; such a purpose is rejected by Markus Lang, 'Art. 27 DS-GVO' in Taeger (n 50) para 2.

127 Hanloser (n 126) para 10.

128 Däubler (n 56) 411; Jürgen Hartung, 'Art 27 DS-GVO' in Kühling (n 55) para 24; Gerrit Hornung, 'Art 27 DSGVO' in Simitis (n 63) para 31; Lang (n 110) para 66; Christopher Millard and Dimitra Kamarinou, 'Art 27 GDPR' in Kuner (n 68) sub-s C 8; Plath (n 125) para 8.

129 Hornung (n 128) para 32.

130 Brkan (n 107) 326; Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* Opinion of AG Saugmandsgaard Øe from 2.6.2016 para 110; different the description of Case C-230/14 *Weltimmo*, Opinion of AG Cruz Villalón from 25.6.2015 para 23.

TFEU, which retained legislative power in the field of data protection law with the member states and did not provide for a full harmonisation, even though this had been intended.[131] With regard to its legal nature, the provision as well as the domestic provisions to transpose its requirements into domestic law,[132] were classified as a conflict-of-laws rule by the majority,[133] including the ECJ.[134] Others classified Article 4 DPD as an overriding mandatory provision[135] whereas others assumed that the provision would deal with requirements of international public law.[136]

Classifying the Legal Nature of Article 3 GDPR—The 'Newcomer'

Article 3(1) and (2) GDPR contain rules comparable to Article 4 DPD. According to its heading, the provision deals with the territorial scope of the Regulation for controllers and processors with an establishment within the EU as well as external controllers in special circumstances. After an overview of the discussion on the legal nature of Article 3 GDPR, the effect of this Article in the framework of private international law will be examined.

Conflicting Approaches: Overriding Mandatory Provision Versus Conflict of Law-rule

In contrast to the fairly consistent classification of Article 4 DPD, a multitude of opinions are introduced in respect of the legal nature of Article 3 GDPR.

Some scholars assume the GDPR would not contain a general conflict-of-laws provision.[137]

Others classify Article 3 GDPR as an overriding mandatory provision.[138] Brkan even proposes to clarify the legal nature of Article 3 GDPR as an overriding mandatory

131 See (n 24).

132 In context of s 1(5) *Bundesdatenschutzgesetz* (2001) for example Eva Beyvers and Tilman Herbrich, 'Das Niederlassungsprinzip im Datenschutzrecht—am Beispiel von Facebook—Der neue Ansatz des EuGH und die Rechtsfolgen' (2015) ZD 558; Borges, '§ 9 Cloud Computing mit Auslandsbezug' (n 60) para 12.

133 See only Borges (n 60) para 10 f; Brkan (n 107) 326; Philip Laue, 'Öffnungsklauseln in der DS-GVO—Öffnung wohin?' (2016) ZD 464; Piltz, 'Art. 3' (n 54) para 44; Roth (n 30) 451; *Weltimmo* Opinion of AG Cruz Villalón (n 130) para 23; see also Case C-191/15 *Verein für Konsumenteninformation* Opinion of AG Saugmandsgaard Øe (n 130) para 108.

134 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (n 58) para 51.

135 Carlo Piltz, 'Rechtswahlfreiheit im Datenschutzrecht?' (2012) K&R 643 f.

136 Björn Steinrötter, 'Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern—uneinheitliche Spruchpraxis oder bloßes Scheingefecht?' (2013) MMR 694.

137 Brkan (n 107) 341; Laue (n 133) 464; Wieczorek (n 68) 648.

138 Däubler, 'Das Kollissionsrecht des neuen Datenschutzes' (n 56) 406; Wolfgang Däubler, 'Art. 3 DSGVO' in Wolfgang Däubler, Peter Wedde, Thilo Weichert and Imke Sommer, *EU-DS-GVO und BDSG Kompaktkommentar* (2nd edn Bund 2020) para 2; Hornung, 'Art. 3 DSGVO' (n 63) para 70; Klar (n 55) para 105; Piltz, 'Art. 3' (n 54) para 44; Schmidt (n 50) para 35.

provision *de lege ferenda* in a new Article 3(5) GDPR.[139] The opposing opinion qualifies Article 3 GDPR as a conflict-of-laws rule,[140] while most of the scholars support a classification as a unilateral conflict of laws rule.[141] On this basis, Melcher[142] and Thon[143] argue to design Article 3 GDPR *de lege ferenda* as a multilateral conflict-of-laws provision which focuses on the 'market-place' principle as a connecting factor. Others identify Article 3 GDPR *de lege lata* as a *lex protectionis datorum* and, therefore, not merely a unilateral but a multilateral conflict-of-laws rule.[144]

Determining the Regulatory Content of Article 3 GDPR

In the light of these diverging opinions, a more detailed analysis regarding the classification of Article 3 GDPR in the traditional categories of private international law is required.

After an outline of the existing exclusive legal relationship of conflict-of-law and overriding mandatory provisions, the legal nature of Article 3 GDPR in the scope of private international law will be examined in detail.

Demarcation Between Conflict-of-Law, Overriding Mandatory Provisions and Procedural Rules

In private international law, the application of conflict-of-laws rules and the special connection of overriding mandatory provisions are seen as two different types of rules.[145] In addition, a distinction needs to be made about procedural rules. Such rules typically address the procedural aspects of litigation and arbitration, such as provisions indicating the jurisdiction in international cases.[146]

In terms of the Rome I Regulation, overriding mandatory provisions are defined as provisions being so crucial for safeguarding a country's public interest that they are applicable to any situation falling within their scope, irrespective of the law applicable

139 Brkan (n 107) 336, 341.

140 Hanloser (n 53) para 7.

141 Jonas Sebastian Baumann, 'The Provision of Personal Data as a Form of Payment in E-commerce Contracts: Determining the Applicable Data Protection and Contract Law in the Legal Framework of the European Union' (LLM Diss, University of Johannesburg 2018) 44; Borges (n 88) para 18; Christian Gomille, 'Datenschutzrechtlicher Löschungsanspruch gegen Suchmaschinenbetreiber—Anmerkung zu OLG Frankfurt am Main, Urteil vom 6.9.2018-16 U 193/17' (2019) ZUM-RD 86; Lüttringhaus (n 108) 72; Melcher (n 8) 138; Thon (n 9) 39 ff.

142 Melcher (n 8) 143 ff.

143 Thon (n 9) 59 f.

144 Martin Schmidt-Kessel, 'Article 9' in Franco Ferrari (n 103) para 51.

145 See Christian von Bar and Peter, Mankowski, *Internationales Privatrecht Band 1* (2nd edn, CH Beck 2003) s 4 para 99.

146 See for example the provisions of the Brussels I*bis* Regulation (which do not apply to arbitral matters (see Art 1(2)(d))).

according to the provisions of the relevant Regulation.[147] On an abstract level, overriding mandatory provisions are substantive rules that are connected with an express or latent one-sided conflict-of-laws rule specifically related to them.[148]

This definition shows that overriding mandatory provisions contain substantive regulative content and are therefore classified as substantive rules.[149] Provisions only stating a legal consequence in the field of conflict-of-laws can therefore not be qualified as overruling mandatory provisions.[150] Accordingly, the classification of a provision as a substantive or a conflict rule is decisive for the classification of the very same provision as an overriding mandatory or conflict-of-laws provision.

Substantive and conflict-of-law provisions have different functions. Conflict-of-laws rules are provisions that determine the applicable legal system in an internationally linked situation,[151] whereas substantive rules solve material legal questions.[152] The doctrinal qualification of a particular provision as a conflict-of-laws provision or a substantive provision can be complex, especially with regard to provisions determining the scope of a particular Act or Regulation. In this respect, Schurig submitted a procedure for such a classification based on the different functions of substantive rules and conflict-of-law provisions by interpretation of the provision in question.[153]

Accordingly, the regulatory content of geographically limited provisions must be assessed. Provisions are considered to have a substantive nature when addressing the applicability of two domestic regulatory regimes, one including and one excluding the provision in question.[154] A conflict-of-laws nature is considered for provisions conclusively defining the scope of application of an Act in a way that, outside the scope of these rules, the matter is addressed by a foreign legal system.[155]

147 See Art 9(1) Rome I Regulation.

148 Jan Kropholler, *Internationales Privatrecht* (Mohr Siebeck 2006) 109; Von Bar (n 145) s 4 para 12.

149 Stephan Lorenz, 'Einleitung zum internationalen Privatrecht' in Wolfgang Hau and Roman Poseck (eds), *BeckOK BGB* (57th edn, CH Beck 2021) para 49; Melcher (n 8) 131; similar Gerhard Kegel and Klaus Schurig, *Internationales Privatrecht* (9th edn, CH Beck 2004) 155; see also Kropholler (n 148) 108 ff ('*materielle Normen*').

150 In terms of the Rome I Regulation, for example, the coexistence of Art 9 and 23 would not make any sense when the priority of special conflict-of-laws rules could also be justified under recourse to Art 9 Rome I Regulation. The same applies to art 16 and 27 Regulation (EC) No 864/2007 (Rome II Regulation).

151 Kropholler (n 148) 103; Von Bar (n 145) s 4 para 1; see also Klaus Schurig, *Kollisionsnorm und Sachrecht* (Duncker & Humblot 1981) 64

152 Von Bar (n 145) s 4 para 1; Schurig (n 151) 64.

153 In detail Schurig (n 151) 58 ff.

154 ibid 64.

155 ibid 64.

This procedure, which is referred to as *Alternativentest*[156] (alternative test), is also applied to determine the legal nature of Article 3 GDPR.[157]

The Regulatory Content of Article 3 GDPR

In order to apply the afore-mentioned procedure to Article 3(1) and (2) GDPR, it must be determined whether the provisions regulate the applicability of the GDPR in relation to other EU legislation or whether they regulate the application of the GDPR conclusively and whether matters outside the scope of these rules are addressed by another legal system.

Article 2 and 3 GDPR, regulating the scope of application, follow a specific regulatory technique. The substantive law question, when the GDPR is applicable in relation to other Acts, is addressed by Article 2 GDPR which regulates the material scope. Article 2(1) GDPR positively determines the material scope of the Regulation and Article 2(2) GDPR negatively excludes the application in certain cases. The provision also regulates the relation to other EU data protection legislation, as illustrated by Article 2(3) and (4) GDPR. Article 3(1) and (2) GDPR, on the other hand, regulate the territorial scope and both provisions provide the legal consequence that the Regulation 'applies'. From this, some authors conclude that *de lege lata* data protection law does not provide for a system of conflict-of-law provisions[158] but the legal order of Article 3(1) and (2) GDPR is typical for unilateral conflict-of-laws rules. Unilateral conflict-of-law rules only regulate the applicability of their own regulatory system.[159] In addition, Article 3 GDPR has a function in determining the applicable data protection law in international cases. It provides that either the requirements for an application of the GDPR are met, and if not, the data protection laws of a third state may be applicable.[160] In contrast, multilateral conflict-of-law provisions are characterised by the fact that their legal consequence is to declare a special legal system independent from its origin.[161] Article 3(1) and (2) GDPR do not refer to the application of another legal system and can therefore not be classified as a multilateral conflict-of-laws rule.

Since Article 3 GDPR does not provide a legal consequence in relation to other Regulations or Acts, the solitary function of the provision is to regulate the application of the GDPR in international situations by using already established and new connecting factors.[162] Therefore, Article 3 GDPR does not address a problem on the substantive level and cannot be qualified as a substantive rule. In addition, Article 3 GDPR does

156 Kegel (n 149) 57

157 Melcher (n 8) 138; Thon (n 9) 40.

158 See also Philip Uecker, *Extraterritoriale Regelungshoheit im Datenschutzrecht* (Nomos 2017) 205; also compare Wieczorek (n 68) 648.

159 Kegel (n 149) 301; Kropholler (n 148) 106; Lorenz (n 149) para 45; von Bar (n 145) s 1 para 17.

160 Thon (n 9) 40.

161 Kegel (n 149) 301; Lorenz (n 149) para 45; Von Bar (n 145) s 1 para 17.

162 Baumann (n 141) 44; compare also Melcher (n 8) 138; Thon (n 9) 40.

also not regulate procedural matters, since this provision does not address jurisdictional matters.[163] In this respect, the GDPR introduced special procedural rules to determine the *forum*.[164] Therefore, the legal consequence of Article 3 GDPR is limited to determine the applicability of the GDPR itself on a conflict-of-laws level, introducing the legal consequence of a unilateral conflict-of-laws in terms of the traditional understanding.

The classification as a unilateral conflict-of-laws provision reflects that Article 3 GDPR regulates the scope of public and civil law provisions. Public international law mainly utilises unilateral conflict-of-law provisions and the classification of Article 3 GDPR, as such a rule results in a regulatory symmetry between private and public international law.[165]

Furthermore, Article 3(1) GDPR, which links to the processing in the context of the activity of an establishment, uses a connecting factor already known from the conflict-of-laws rule contained in Article 4(1) DPD.[166] Article 3(2) GDPR uses connecting factors, such as, the actual location of a person, the 'offering' of services and goods as well as 'monitoring'. In doing so, it is assumed that the 'offering' is comparable to the connecting factor of 'directing' as provided for in Article 6(1)(b) Rome I Regulation and that the principles developed by the courts are transferable.[167] The adoption of the content of such connecting factors constitutes another argument in favour of the classification as a conflict-of-laws provision.

Article 3 GDPR as a Unilateral Conflict-of-law Rule

Although the GDPR pursues important goals regarding the social and economic organisation within the EU,[168] Article 3 GDPR cannot be classified as an overriding mandatory provision as matters of substantive law are not addressed. The application of general principles of private international law leads to the conclusion that the territorial scope rule of Article 3(1) and (2) GDPR constitutes a unilateral conflict-of-laws rule.[169]

163 *Soriano v Forensic News LLC* (n 71) para 46.

164 See GDPR Art 79(2). GDPR Recital (147) clarifies in this respect, that the Brussels I*bis* Regulation shall not prejudice the application of the jurisdiction rules introduced by the GDPR. Further, GDPR Recital (145) indicates that the subject may choose the *forum*, if more than one court could assume jurisdiction based on GDPR Art 79(2).

165 In detail on this aspect Thon (n 9) 50 f.

166 cf Borges (n 88) para 17; Schantz, in Schantz (n 68) para 324.

167 See the references in (n 95).

168 See Klar (n 55) para 105; Piltz 'Art. 3' (n 54) para 45.

169 See the references in (n 125).

The GDPR, therefore, introduces a special conflicts rule in terms of Article 23 Rome I Regulation[170] preceding the conflict rules of the Rome I Regulation within the scope of the GDPR in a contractual context.[171] In delictual cases, Article 3 GDPR supersedes in its scope the conflict-of-laws rules of the member states since the Rome II Regulation is not applicable.[172]

Contractual Choice of the Applicable Data Protection (Civil) Law

Another aspect arising from a private international law perspective lies in the permissibility of a choice of law under the GDPR. In this regard, it is unclear whether a contractual choice of law includes a valid choice of the applicable data protection regulations.

Subsequently, the legal framework and the practical relevance of choice of law clauses will be elaborated upon before examining whether the applicable data protection law can be determined by a choice of law in contracts.[173]

Legal Framework and Practical Relevance of Choice of Law Clauses

A choice of the applicable data protection law can only be considered in private law relations since authorities and other public law entities are not permitted to evade the applicable law via a choice of law.[174] Between private persons on the other hand, a choice of law is permitted as a result of contractual freedom.[175]

Pursuant to Article 3(1) Rome I Regulation, the parties can choose the law applicable to the contract within the scope of this Regulation and the freedom of choice of law is mainly restricted by the provisions of the Rome I Regulation.[176]

170 Special conflict-of-law provisions in terms of Art 23 Rome I Regulation can be both unilateral and multilateral conflict-of-law provisions, see Ulrich Magnus, 'Art. 23 Rom I-VO' in Staudinger, *Kommentar zum bürgerlichen Gesetzbuch (Internationales Vertragsrecht II)* (Sellier De Gruyter 2016) para 17.

171 Melcher (n 8) 139.

172 Data Protection cases are excluded via Art 1(2)(g) Rome II Regulation; see only Ivo Bach, 'Art 1 Rom II-VO' in Gerald Spindler and Fabian Schuster (eds), *Recht der elektronischen Medien* (4th edn, CH Beck 2018) Rn 9; Brkan (n 107) 332; Lüttringhaus (n 108) 75.

173 The legal problems of an *ex post* choice of law regarding delictual claims will be excluded from the analysis.

174 Hornung, 'Art. 3 DSGVO' (n 63) para 70.

175 See Case C-184/12 *Unamar v Navigation Maritime Bulgare* [2013] EU:C:2013:663 para 49; Case C-135/15 *Republik Griechenland v Nikiforidis* [2016] EU:C:2016:774 para 42; in detail on contractual freedom in EU Law Jan D Lüttringhaus, *Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt* (2018 Mohr Siebeck) 113 ff.

176 See for example Art 6(2) Rome I Regulation.

Prominent social media networks[177] and providers of digital content[178] incorporated choice of law clauses in their terms of use which evidences the high practical relevance of this matter. In this context, studies concluded that such clauses are often designed to favour the provider.[179]

Choice of the Applicable Data Protection Law

The following section will provide an overview on the possibility of a choice of the applicable data protection law in context of the DPD. Thereafter, the ECJ decision of the *VKI v Amazon* case will be investigated to determine whether the ECJ explicitly or tacitly clarified the possibility of a choice of law in the field of data protection law. Then, the state of discussion under the GDPR will be presented and it will be discussed whether a choice of law should be permitted in this new regulatory framework.

State of Discussion on the Data Protection Directive

Regarding the legal situation under the DPD the possibility of a choice of law was a controversial issue as neither the Rome I Regulation, the DPD nor the domestic data protection frameworks[180] expressly excluded a choice of law in the field of data protection law.

In certain cases, a choice of law regarding private law data protection rules was considered admissible by some German courts[181] and supported by scholars.[182] Others

177 See for example the Facebook, 'Terms of Service' (20 December 2020) sub 4.4 <https://www.facebook.com/legal/terms?ref=pf> accessed 29 April 2021 (law of the residence of the user applies for EU consumers); see also Twitter, 'Terms of Service' for users living outside the European Union, EFTA States, or the United Kingdom, including such users living in the United States (18 June 2020) sub 6 <https://twitter.com/en/tos#intlTerms> accessed 29 April 2021 (choice of the law of the State of California) and TikTok, 'Terms of Service' for users outside US, EEA, the United Kingdom, Switzerland or India (February 2021) sub 11 <https://www.tiktok.com/legal/terms-of-use?lang=en> accessed 29 April 2021 (choice of law in favour of the laws of Singapore).

178 The service Spotify, for example, has a very differentiated choice of law system depending on which country the service is provided for, see Spotify, 'Terms and Conditions of Use' (13 February 2019) sub 24.1 <https://www.spotify.com/za/legal/end-user-agreement/#s24> accessed 29 April 2021.

179 See the findings of Michael Rustad and Thomas Koenig, 'Wolves of the World Wide Web: Reforming Social Networks' Contracting Practices' (2014) 49 Wake Forest LR 1511 (in context of social networks).

180 See for example s 1(5) of the German *Bundesdatenschutzgesetz* (2001), s 3 of the Austrian *Datenschutzgesetz* (2000) (as introduced by *Bundesgesetzblatt* I No 165/1999), s 5 of the UK Data Protection Act 1998 or s 4 of the Dutch *Wet bescherming persoonsgegevens* (as introduced by *Staatsblad* (6.7.2000), 302) all which did not address the matter within their scope rules.

181 *Landgericht Berlin*, Judgment (6 March 2012) Case No 16 O 551/10 [2012] ZD 278; *Kammergericht*, Judgment (24 January 2014) Case No 5 U 42/12 [2014] ZD 416.

182 Steinrötter (n 136) 693; also see Sven Polenz, 'Die Datenverarbeitung durch und via Facebook auf dem Prüfstand' (2012) VuR 209 and Wolfgang Ziebarth, 'Das Datum als Geisel—Klarnamenspflicht und Nutzeraussperrung bei Facebook' (2013) ZD 377 f.

considered a solution in respect of Article 6(2) S1 Rome I Regulation, as data protection regulations could be regarded as a mandatory consumer protection regulation.[183] The majority argued that a choice of the applicable data protection law is generally inadmissible.[184]

The Open Position of the ECJ in VKI v Amazon EU Sàrl

The ECJ has not explicitly addressed the question whether a choice of the applicable data protection law is permitted, even though the court had an opportunity in 2016 to share its position on the DPD in the *Amazon* case. The decision is interpreted as an implicit statement of the ECJ against the permissibility of a choice of the applicable data protection law.[185] It is argued that in this judgment, the ECJ considered a choice of law to be inadmissible regarding the contract law aspects of the case but determined the applicable data protection law referring to the DPD.[186]

The preliminary ruling of the ECJ referred to a case in Austrian Courts where the *Verein für Konsumenteninformation (VKI)*, a consumer protection organisation based in Austria, filed an action against *Amazon EU Sàrl*, a company established in Luxemburg and belonging to an international corporation that distributes goods via a website (also addressing consumers residing in Austria) to prohibit the use of several clauses utilised by *Amazon* in agreements with consumers. The clauses in dispute included a choice of law clause indicating the law of Luxemburg to be applicable.[187]

The *Oberste Gerichtshof* of Austria referred a number of questions to the ECJ.[188] In the first place, the referring court asked the ECJ how to interpret the Rome I and Rome II-Regulations to determine the law applicable to an action for an injunction in terms of Directive 2009/22[189] against the use of allegedly unlawful contractual terms. Further, the Court asked the ECJ whether a choice of law, like the one in dispute, would be

183 This result was rejected by Isabel Gläser, 'Anwendbares Recht auf Plattformverträge—Fragen des IPR bei sozialen Netzwerken am Beispiel von Facebook' (2015) MMR 703 and Piltz, 'Rechtswahlfreiheit im Datenschutzrecht?' (n 135) 642.

184 *Verwaltungsgericht Schleswig*, Decision (14 February 2013) Case No 8 B 60/12 [2013] ZD 245 f; Brkan (n 107) 333; Gläser (n 183) 703; Ingemar Kartheuser and Manuel Klar, 'Wirksamkeitskontrolle von Einwilligungen auf Webseiten—anwendbares Recht und inhaltliche Anforderungen im Rahmen gerichtlicher Überprüfungen' (2014) ZD 502; Piltz, 'Rechtswahlfreiheit im Datenschutzrecht?' (n 135) 645; Piltz (n 107) 296.

185 Alexander Golland, *Datenverarbeitung in sozialen Netzwerken* (R&W 2018) 114.

186 ibid.

187 According to the findings of the ECJ in *Verein für Konsumenteninformation* (n 58) para 30, the clause had the following wording '12. Luxembourg law shall apply, excluding the United Nations Convention on the International Sale of Goods.'

188 The questions are repeated in *Verein für Konsumenteninformation* (n 58) para 34.

189 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests.

'unfair' in terms of Article 3(1) Directive 93/13.[190] Lastly, the court asked which data protection rules are applicable by virtue of Article 4(1)(a) DPD.

After determining the applicable law to the injunction in terms of the Rome I and Rome II Regulation,[191] the ECJ provided criteria for national courts to assess whether a choice of law clause is 'unfair' in terms of Article 3(1) Directive 93/13.[192] Thereafter, the ECJ applied Article 4(1)(a) DPD in order to determine the applicable data protection law.[193] In its remarks on Article 4(1)(a) DPD, the ECJ did not refer to the choice of law clause at any point. Additionally, the ECJ summarised the question presented by the *Oberste Gerichtshof*[194] and did not repeat the exact wording of this question.[195] The *Oberste Gerichtshof* suggested that the applicable data protection law is to be determined by virtue of Article 4(1)(a) DPD 'regardless of the law that would otherwise apply', which indicates that the referring court considered the choice of law to be irrelevant in this assessment. Due to this discrepancy and since the ECJ did not address the relevance or legal effect of a choice of law during the determination of the applicable data protection law, its position on the matter remains unclear. Therefore, the *Amazon* decision does not indicate the (im)permissibility of a choice of the applicable data protection law.

The State of Discussion under the GDPR

Considering that the legal question of whether a choice of law clause extends to the civil law data protection provision was never explicitly addressed by the ECJ, the matter has not been decided by the highest relevant court. The scholarly opinions on this question under the GDPR differ from the opinions represented under the DPD and, as far as apparent, case law in this respect has not yet been reported.

190 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

191 *Verein für Konsumenteninformation* (n 58) para 35 ff.

192 ibid para 65.

193 ibid para 72 ff.

194 The *Oberste Gerichtshof* presented the following question: 'Is the processing of personal data by an undertaking which in the course of electronic commerce concludes contracts with consumers resident in other Member States, in accordance with Article 4(1)(a) of Directive 95/46, regardless of the law that would otherwise apply, subject exclusively to the law of the Member State in which is situated the establishment of the undertaking in the context of which the processing takes place, or must the undertaking also comply with the data protection rules of those Member States to which its commercial activities are directed?'.

195 See *Verein für Konsumenteninformation* (n 58) para 72: 'By Question 4(b) the referring court seeks essentially to know whether Article 4(1)(a) of Directive 95/46 must be interpreted as meaning that the treatment of personal data by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities.'

The vast majority of scholars argues that a choice of the applicable data protection law is not permitted.[196] However, Schantz suggests that a distinction be made between a deselection of the GDPR, which is regarded to be inadmissible, and a voluntary submission to the civil law regulations of the GDPR which should be permissible.[197]

The (Im)possibility of a Choice of the Applicable Data Protection Law

Even though the approach of a voluntary submission to the GDPR or a choice of law would pursue party autonomy and freedom to contract, these concepts are problematic. The approach of a voluntary submission to the civil law provisions of GDPR raises uncertainties,[198] especially regarding the determination of whether a GDPR provision should be qualified as a civil or public law provision. Further, if a choice of law would be permitted, it could lead into a frustration of the high protection standards of the GDPR since this instrument could be utilised to evade the applicability of the GDPR.[199]

Therefore, the result of the prevailing concept seems preferable in respect of the effectiveness of the protection level provided by the GDPR but the doctrinal foundation requires further discussions. Many authors who support this position, base their argument on the premise that Article 3(1) and (2) GDPR are classified as overriding mandatory provision in terms of Article 9 Rome I Regulation.[200] Article 3(1) and (2) GDPR are to be qualified as a special conflict-of-laws rule and, therefore, the argument that a choice of law is blocked by an overriding mandatory provision cannot be relied upon.

Since Article 3 GDPR is to be qualified as a special conflict-of-laws provision, the Rome I Regulation does not apply within the scope of Article 3(1) and (2) GDPR. The basic rule of 'freedom of choice' as contained in Article 3(1) Rome I Regulation does

196 Baumann (n 141) 48; Däubler (n 56) 406; Däubler (n 138) para 2; Golland (n 185) 114; Hornung, 'Art 3 DSGVO' (n 63) para 70; Klar (n 55) para 105 f; Piltz, 'Art 3' (n 54) para 42, 46; Schmidt (n 50) para 35; Schmidt-Kessel (n 144) para 59; Svantesson (n 68) sub-s C.2.; Thon (n 9) 41 f; see also Lüttringhaus (n 108) 74 (in context of the liability rule of GDPR Art 82).

197 Schantz, in Schantz (n 68) para 342 f.

198 The GDPR allows such a submission (on a contractual basis) in the context of the transfer of personal data to third states. Such a transfer is permitted under the requirements of GDPR Art 44 ff, inter alia, when based on standard data protection clauses (GDPR Art 46(2)(c). Those clauses as adopted by the European Commission are to be incorporated into a contract between the data exporter and the importer and constitute obligations with regard to the processing of personal data and contain a third-party beneficiary clause in favour of the data subject. Regarding the clauses adopted by Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, the data importer is required to process data in accordance with the mandatory data protection principles as set out in Appendix 2 of the decision (clause 5(b)), which were formed based on the DPD.

199 See only Däubler (n 138) para 2.

200 Däubler (n 56) 406; Hornung (n 63) para 70; Klar (n 55) para 105 f; Schmidt (n 50) para 35; also see Piltz (n 54) para 44, 46; also compare Svantesson, (n 68) sub-s C 2 ('mandatory nature').

not apply and the GDPR does not implement a provision explicitly permitting a choice of law within its scope.[201] Since this problem was already discussed under the DPD and the GDPR, it does not conclusively solve this matter. One could assume that a choice of the applicable data protection law should not be permitted. Also, the extensive extra-territorial scope rule of Article 3(2) GDPR and the change to the legislative instrument of the Regulation which envisages a high degree of harmonisation due to its direct application in all member states, militate against the permission of a choice of law. In addition, a choice of law would also endanger one of the main purposes of the Regulation, which is according to Article 1(1) GDPR the protection of information related to natural persons.[202] Further, the rationale of Article 3 GDPR, to implement a level playing field, would be frustrated if a choice of law would be permitted.[203] Others identify the avoidance of forum shopping as a rationale of Article 3 GDPR,[204] which would be an additional argument against the permissibility of a choice of law.

Therefore, a restriction of party autonomy of the data subject in the field of choice of law is required and can be based on the systematic argument that the GDPR does not contain a corresponding provision that allows a choice of law within the scope of the Regulation. This result is also supported by previous policy considerations.

Interim Conclusion

A choice of the applicable data protection law is not permissible under the new GDPR. Therefore, choice of law clauses do not determine the applicable data protection law, instead the GDPR applies directly in all member states when the requirements of Article 3 are met.

Potential Regulatory Impacts for South Africa

The POPIA is the first South African Act implementing a general framework for data protection law and is of significant relevance for the development of data protection standards in the Republic. Whilst drafting this Act, extensive reference was made to international data protection instruments[205] as well as the DPD.[206] Many provisions

201 Baumann (n 141) 48; Thon (n 9) 42; also see the argument of Kartheuser and Klar (n 184) 502 (in context of the DPD).

202 Also compare the reasoning of Golland (n 185) 114 referring to Art 16 TFEU and Art 8 of the Charter of Fundamental Rights of the European Union.

203 Thon (n 9) 41 f.

204 Albrecht (n 51) 90; Steinrötter (n 51) 64.

205 Namely the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data from 23 September 1980 and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108/1981 from 28 January 1981.

206 See for example the references on those frameworks in the reform debate (SALRC, Issue Paper 24 (Project 124) (2003) sub. 1.2.13 ff and sub 6.1.7 ff; SALRC, Discussion Paper 109 (Project 124) (October 2005) sub.1.2.13 ff; SALRC, Project 124 Privacy and Data Protection Report (2009), sub 1.2.13 ff and sub. 4.1.11 ff). On the genesis of the POPIA in greater detail Roos, 'Data Protection Law

contained in the POPIA serve as evidence that the DPD served as a model for its wording and systematisation.[207] The historical connection between the POPIA and the European data protection law provides a solid basis for a legal comparison with the GDPR. Therefore, 'the wheel does not have to be re-invented' when attempting to understand, interpret and apply the POPIA, as much can be learnt and adopted from the EU's data protection laws as well as relevant case law.

An examination of the territorial scope rule of the POPIA and its classification in terms of private international law will be presented before potential amendments of this Act concerning its (extra)territorial scope will be analysed.

The Territorial Scope of the POPIA

The territorial scope of the POPIA is addressed in section 3(1)(b) and applies to the processing of personal information,

> 'where the responsible party is
>
> (i) domiciled in the Republic; or
>
> (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.'

This provision determines the applicability of the POPIA based on a distinction between responsible parties domiciled and not domiciled in the Republic. The recourse on the use of automated or non-automated means 'in the Republic' suggests a territorial approach since a connection to the territory of the Republic of South Africa is required in all cases.[208] As deduced from this provision, processing activity must regularly be connected to the territory of South Africa in order to apply the POPIA, which is quite a challenging requirement as the processing of personal information crosses borders easily via the internet and by using other technological means such as cloud services.[209] In the reports of the *Law Reform Commission*, on the reform of data privacy law in

in South Africa' (n 20) 201 ff; see also on the Data Protection Bill 2009: Alex Makulilo, *Protection of Personal Data in Sub-Saharan Africa* (Dr iur Thesis, University of Bremen 2012) 400 ff.

207 See Yvonne Burns and Ahmore Burger-Smidt, *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018) 8: '[…] it becomes clear that the South African legislature relied heavily on the principles and objectives of the 1995 Directive in drafting the POPI Act.'

208 Some South African scholars indicate an 'extraterritorial reach' of the South African data protection law, see Lukman Adebisi Abdulrauf, 'Data Protection in the Internet: South Africa', in Dário Moura Vincente and Sofia de Vasconcelos Casimiro (eds), *Data Protection in the Internet* (2020 Springer) 367.

209 Elizabeth De Stadler and Paul Esselaar, *A Guide to the Protection of Personal Information* Act (Juta 2015) 6.

South Africa, this regulatory approach was not discussed in greater detail.[210] Nevertheless, the proposed bill of the *SALRC* introduced the regulatory mechanism as adopted by Section 3(1)(b) of the POPIA.[211] This approach is comparable to the regulatory concept of Article 4(1)(a) and (c) DPD which contained comparable rules and followed, in essence, the territoriality principle.[212]

The Concept of 'Domicile' under the POPIA

Unlike the DPD and the GDPR, section (3)(1)(b) of the POPIA distinguishes on the basis of the requirement of 'domicile' of the responsible party and thereby utilises an established private international law term,[213] since the POPIA does not provide an autonomous definition. In international data protection cases, the responsible party is mostly a juristic person. According to South African case law, a company is domiciled at the place of its registered office.[214] Some scholars indicate a broader notion of company domicile in terms of the POPIA as it is submitted that the Act applies when the responsible party has a place of business in South Africa, even if the head office is situated outside the Republic.[215]

Due to this terminological difference to Article 3(1) GDPR an extra systematic reference to ECJ case law appears to be excluded, since the Constitutional Court does not support such reference when it 'displace[s] the express meaning of the legislation'.[216] Therefore, it seems unlikely that South African courts will deviate from

210 The discussion on the scope of the proposed legislation focussed on other aspects, such as the incorporation of juristic persons into the personal scope of the Act, see SALRC, *Issue Paper 24 (Project 124)* (2003) sub-s 1.3 ff; SALRC, *Discussion Paper 109 (Project 124)* (October 2005) sub-s. 3.1 ff; SALRC, *Project 124 Privacy and Data Protection Report* (2009), sub-s 3.1 ff.

211 See s 3 of the proposed bill in the SALRC, *Project 124 Privacy and Data Protection Report* (2009), Annex C which had the following wording: 'This Act applies to the processing of personal information entered in a record, using automated or non-automated means, by or for a responsible party -
(a) domiciled in the Republic of South Africa; or
(b) which is not domiciled in South Africa, using automated or non-automated means situated in South Africa, unless those means are used only for forwarding personal information, provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.'

212 Ulrich Damann and Spiros Simitis, *EG-Datenschutzrichtlinie Kommentar* (Nomos 1997) Art 4 para 2 f, 6.

213 In detail on the concept of domicile in South African Private International Law: Richard Frimong Oppong, *Private International Law in Commonwealth Africa* (Cambridge 2013) 32 ff; Christopher F Forsyth, *Private International Law* (5th edn, 2012 Juta) 132 ff.

214 *Bisonbord Ltd v K Braun Woodworking Machinery (Pty) Ltd* 1991 (1) SA 482 (AD) 489C; *Sibakhulu Construction (Pty) Ltd v Wedgewood Village Golf Country Estate (Pty) Ltd* 2013 (1) SA 191 (WCC) 199E-G.

215 De Stadler (n 209) 6.

216 *Competition Commission of South Africa v Media 24 (Pty) Limited* 2019 (5) SA 598 (CC) 655 para 185 (in context of the interpretation of section 8(c) Competition Act (89 of 1998)—addition by the authors).

the established definition of domicile and adopt the broad interpretation of the ECJ of the term 'establishment'.

Application of the POPIA in Context of Responsible Parties not Domiciled in the Republic

In cases where the responsible party is not domiciled within the Republic, the POPIA applies by virtue of section 3(1)(b)(ii) when such a responsible party makes use of automated or non-automated means in the Republic. The inclusion of automated as well as non-automated means of processing under the scope of the Act expresses the technology neutral regulatory approach of the POPIA.[217] The distinction between automated and non-automated means was recommended by the *Law Reform Commission* based on the concept of Article 3 DPD in order to address electronic and digital means of processing.[218]

The means referred to in the provision are presumably used to either enter the personal information into a record or to process the personal information.[219] The wording of section 3(1)(b)(ii) of the POPIA suggests that not even an attribution criterion regarding the use of means in the Republic by a responsible party is required. An interpretation based on the wording of section 3(1)(b)(ii) of the POPIA could, therefore, extend the (extra)territorial scope significantly, since every processing, even by devices of the data subjects located in the Republic, would lead to the application of the POPIA.

In section 3(4) of the POPIA 'automated means' are defined as 'any equipment capable of operating automatically in response to instructions given for the purpose of processing information.' In this context, the POPIA does not provide further guidance on the extent of the meaning of 'automated means' besides the highly abstract definition in section 3(4).[220] Section 3(1)(b)(ii) of the POPIA only clarifies that the Act is not applicable when information is only routed through the Republic.[221] In the context of Article 3 (1) DPD, the ECJ interpreted the passus 'wholly or partly by automatic means' in the *Lindqvist* case, which addressed the uploading of personal data to a website, as operations that are at least partly performed automatically.[222] In a similar vein, scholars

217 Similar Abdulrauf (n 208) 358 ('[T]he POPI Act, in its provisions, does not discriminate between processing of personal information electronically and manually'). Such an approach was also recommended by the SALRC, *Project 124 Privacy and Data Protection Report* (SALRC 2009), sub-s 3.3.5 ff.

218 SALRC, *Project 124 Privacy and Data Protection Report* (SALRC 2009), sub-s 3.3.9.

219 De Stadler (n 209) 6.

220 In other provisions, eg the definition of 'personal information' in s 1 POPIA, the Act provides a (non-exhaustive) list of examples illustrating which cases are certainly addressed.

221 Burns (n 207) 6.

222 *Lindqvist* (n 24) para 26. In the British case *Law Society and Others v Kordowski* [2011] EWCH 3185 (QB) para 84, 163, the court even assumed a 'processing' of personal data by the website-host when content generated by third parties is published.

assume that personal information processed by internet service providers and social network providers is to be classified as processing via automated means and, therefore, covered by the POPIA.[223] Even the use of cookies could be qualified as the use of 'automated means' in the Republic, when stored on a device located within the Republic.

The term 'non-automated means' is not defined in the POPIA but scholars state under reference to the material scope rule of section 3(1)(a) of the POPIA that it relates to manually recorded information or data.[224] In this respect, section 3(1)(a) of the POPIA restricts the material scope of the Act when recorded personal information is processed by non-automated means. In such cases, the Act only applies if this information forms part of a 'filing system'[225]. Since this provision addresses the material scope of the POPIA, the latter restriction also restricts the territorial scope of the Act in terms of section 3(1)(b) of the POPIA.

With regard to operations, including numerous processing of personal data, it was held in the British case of *Johnson v Medical Defence Union*[226] that singular manual processing steps cannot evade the application of data protection laws when one or more processings are performed via automatic means. This reasoning should be adapted under POPIA in the light of the 'European roots' of this distinction[227] and reflects the technology neutral approach.

The technology neutral approach of the POPIA and the potentially extensive interpretation of 'automated means' in the Republic that comes along with this regulatory technique provide for a 'extraterritorial dimension' of the POPIA. This is surprising since section 3(1)(b)(ii) of the POPIA makes reference to the 'use of automated or non-automated means in the Republic', a criterion commonly associated with a territorial approach.

The Classification of Section 3(1)(b) of the POPIA in South African Private International Law

An analysis on how section 3(1)(b) of the POPIA is embedded in South African private international law follows. South African private international law makes a distinction

223 Abdulrauf (n 208) 358.

224 Burns (n 207) 183.

225 In s 1, the POPIA defines 'filing system' as 'any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.' On the comparable definition of DPD Art 2(c) for example Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551 para 52–62.

226 [2007] EWCA Civ 262 para 30–32.

227 See (n 218).

between unilateral and multilateral conflict-of-laws rules.[228] Unilateral conflict-of-laws rules indicate the applicability of their own legal system in international cases.[229]

Section 3(1)(b) only addresses the question of the applicability of the POPIA and does not regulate a substantive legal question or procedural matters. Identical to provisions in other Acts that have been qualified as unilateral conflict-of-law provisions,[230] section 3(1) provides the legal consequence that '[t]his Act applies'. This indicates that section 3(1)(b) of the POPIA should be classified as a unilateral conflict-of-laws provision. This result is also supported by the similar regulatory technique as utilised in Article 4(1)(a) and (c) DPD, a conflict-of-laws rule and the fact that the provision refers to the 'domicile', an established connecting factor in private international law.

Potential Amendments of the POPIA

On the first sight, the technology neutral approach equips the POPIA to safeguard the right to privacy of data subjects even in the light of modern technological means, including data-driven businesses. Nevertheless, the lack of case law as well as a guidance note by the Information Regulator unleashes legal uncertainty when interpreting the territorial scope rule of section 3(1)(b) of the POPIA. It is, for example, unclear whether section 3(1)(b)(i) or (ii) of the POPIA applies in cases where the responsible party is (formally) domiciled outside the Republic but manages subsidiary companies within the Republic, thereby providing services (economically) related to the main service as provided by the legal entity abroad. One might classify this problem as being purely academic since POPIA will apply either way. However, this example illustrates that the utilisation of a connecting factor relying on company law classifications could be problematic in certain cases. Scholars try to circumvent this by applying an extensive interpretation of 'domicile' which requires a place of business in the Republic.[231] The European data protection framework excluded the corporate structure of controllers as a relevant factor in the determination of the territorial scope utilising the flexible concept of establishment.[232] With the GDPR, the EU entered into a 'new era' of (extra-)territorial data protection regulation, explicitly establishing the

228 Forsyth (n 213) 7; in detail on the types of conflict-of-law rules in the South African legal system Jan Neels, 'An Experiment in the Systematization of South African Conflicts Rules' in Sebastian Omlor (ed), *Weltbürgerliches Recht—Festschrift für Michael Martinek zum 70. Geburtstag* (CH Beck 2020) 531 ff.

229 Forsyth (n 213) 9; Neels (n 228) 531.

230 See s 4(1) National Credit Act (34 of 2005) that is also classified as a unilateral conflict-of-laws provision, see Jan Neels, 'Consumer Protection Legislation and Private International Law' (2010) Obiter 125 f.

231 See De Stadler (n 209) 6.

232 See (n 66).

market-place principle as provided in Article 3(2) GDPR. This concept was recently adopted by the United Kingdom in the UK-GDPR[233] for the post-Brexit period.

The aforementioned 'extraterritorial dimension' of the POPIA also raises practical problems in contacting a responsible party not domiciled in the Republic. The only legal consequence established by the POPIA lies in the application of the Act by virtue of section 3(1)(b)(ii). For instance, in a situation where a responsible party not domiciled within the Republic cannot be contacted, this would constitute a practical obstacle in claiming for compliance with the data subject's rights. Such a request could then factually not be communicated. The same applies to attempts by the Information Regulator to contact such an entity, who may be prevented from initiating or executing enforcement measures. The recent developments in the European data protection framework as well as the revealed practical threat to the enforcement of the POPIA could be reason enough to consider a reform of the POPIA in light of its extra-territorial reach.

Furthermore, a reform process would be a chance to clarify South Africa's position on choice of law in the field of data protection law. This paper has outlined the application of omnibus data protection frameworks in the private sector and raises a number of legal questions from a private international law perspective. Since the POPIA does not address whether a choice of law in data protection law is permitted and the classification of section 3(1)(b) POPIA as unilateral conflict-of-laws provision does not automatically exclude the possibility of such a choice, a similar discussion on this aspect, as in the European legal framework could arise.

In the Preamble to the POPIA, the drafters of the Act clarified that the Act seeks to regulate the aspects of processing personal information 'in harmony with international standards'. In order to keep up with this goal, it appears to be beneficial to constantly evaluate the regulatory mechanisms of the POPIA in light of international 'state of the art'. Since the regulatory mechanism of section 3(b) of the POPIA can be traced back to 2009,[234] more than a decade ago, it appears beneficial to evaluate the option of remodelling this provision based on the concepts for territorial scope rules as introduced by the GDPR. This could lead to an amendment of the POPIA which would provide more legal certainty in international cases and could lead to other beneficial effects. Furthermore, a reform could strengthen the chances for South Africa to obtain an adequacy decision by the European Commission which would provide for free data flow between the Republic and Europe without the requirement of any further

233 See UK-GDPR Art 3(1) and (2).

234 See the Protection of Personal Information Bill s 3(b), as presented by the Portfolio Committee on Justice and Constitutional Development (National Assembly), after consideration of the Protection of Personal Information Bill [B 9—2009] and the similar provision recommended by the SALRC (n 211).

authorisation.[235] This could be of economic significance.[236] With such a decision the European Commission, inter alia, needs to take into account the existence and effectiveness of data protection legislation as well as supervision in a third state.[237] In this context, Roos recently suggested a number of amendments to POPIA in order to comply with the data protection standard as provided by the GDPR.[238]

Reshaping Section 3(b) of the POPIA in the Light of European Principles

In the first place, the South African legislature should evaluate whether a retention of the connecting factor of the 'domicile' is preferable. By utilising a formulation in orientation on Article 3(1) GDPR referring to the 'processing in the context of the activities of an establishment', a basis to adopt the ECJ case law via extra-systematic reference could be provided. Since the ECJ has established guidelines on the interpretation on this provision and its predecessor,[239] this could enhance the territorial scope of the POPIA with a stronger extra-territorial focus that will mitigate the risk that the courts may develop an autonomous definition of the term 'domicile' in terms of the POPIA deviating from the established private international law concept.

Alternatively, the drafters could consider adapting the market-place principle as provided for in Article 3(2) GDPR and implement a rule recognising new connecting factors. Such a rule could *de lege ferenda* be implemented as section 3(1)(c)(i) and (ii) of the POPIA and could be formulated as follows:

> (c) This Act also applies to the processing of personal information of data subjects, who are located in the Republic, by a responsible party or operator not domiciled within the Republic, where the processing activities are related to:
>
> (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Republic; or
>
> (ii) the monitoring of their behaviour as far as their behaviour takes place within the Republic.

235 GDPR Art 45(1). In detail on POPIA from an adequacy perspective Roos (n 25) 8–31.

236 See for example the economic evaluation of the European Parliament concerning the data flow to the US European Parliament resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)), OJ C 76/82 from 28.2.2018 sub-s F, G.

237 See GDPR Art 45(2)(a) and (b); on the reasoning required in such decisions by the EC Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 para 79–98 (regarding the Safe Harbor principles); on the legal standard required by the non-EU legal system for an adequacy decision Case C-311/18 *Data Protection Commissioner* (n 39) para 168 ff (in context of the EU-US Privacy Shield).

238 Roos (n 25) 31 f.

239 See the cases referenced in (n 58).

Such a rule would ensure that the POPIA applies to responsible parties domiciled outside South Africa, even if they offer services and goods to persons in South Africa, without reference to means located within the Republic. This would disconnect the process of determining the application of the POPIA to a certain extent from corporate law criteria or highly complex technological procedures and introduce an objective assessment of the business model and practices of the responsible party. Article 3(2) GDPR could serve as an example to provide legal practitioners with additional sources for the interpretation of the proposed rule, such as the academic discussion on the requirements of Article 3(2) GDPR and future decisions of the ECJ. This should be welcomed since the Act explicitly seeks to establish conditions in harmony with international standards.[240] Such a rule would also include responsible parties (established or using means located) in South Africa as well as entities established outside the Republic who would then benefit from a level playing field with regard to the applicable data protection standard.

A third possibility would be the adoption of the combined approach of the 'establishment' and the 'market-place' principle as provided by Article 3(1) and (2) GDPR. The drafters would then have to carefully evaluate the impact of such an extensive extra-territorial concept.[241] An approach that could result in an extensive extra-territorial application of the POPIA by accumulating an extensive interpretation of the term 'establishment' in conjunction with another extra-territorial scope rule. Such a cumulation could result in an application of the POPIA to cases that might be more closely connected with another country and a foreign data protection regime.

Implementation of the Concept of Representation

With regard to responsible parties not domiciled within the Republic, the drafters should consider implementing an obligation to designate a representative within the Republic. A concept comparable to the one implemented by Article 27 GDPR is alien to the POPIA. In South African law, the implementation of such a concept would be a policy decision. In any case, the requirement of representation would come with certain advantages compared to the *status quo*. *De lege lata*, the POPIA does not introduce any legal consequences besides the application of the Act where the responsible party is not domiciled within the Republic. Practically, this could result in an 'enforcement vacuum', when the Information Regulator seeks to contact such responsible parties or even intends to initiate enforcement measures. A representative would provide a contact point for the supervisory authorities as well as the data subjects. In addition, a clarification could avoid legal uncertainty by defining whether the representative is a potential addressee of civil law claims and authoritative measures based on infringements of the POPIA committed by the represented responsible party. Under the

240 POPIA s 2(b).

241 See on the criticism regarding the *comitas* approach (n 49).

GDPR, this aspect of the representation is subject to a controversial discussion. Such an allocation of liability would be a policy decision as it could facilitate the enforcement of the POPIA against parties not domiciled in the Republic but would impose significant liability risks on the representative rendering this position less attractive. In any case, the implementation of a compulsory representation would strengthen the level of protection provided by the POPIA.

Explicit Exclusion of a Choice of Law in the POPIA

The POPIA, like the DPD and the GDPR, does not explicitly address the question whether a choice of law is permitted regarding the applicable data protection law. In South African private international law, the instrument of a choice of the proper law by contracting parties is recognised by the South African courts.[242] Therefore, a clarification with regard to the possibility of a choice of the proper data protection law is also required within the South African regulatory framework. A regulation explicitly addressing the question of the possibility of a choice of law in South African data protection law would provide legal certainty. Considering the purposes of the POPIA, as outlined in section 2, it would be surprising if the South African drafters would conclude that such a choice of law should be permitted. In addition, it is unclear to which extent provisions of the POPIA are to be qualified as overriding mandatory provisions. Therefore, the POPIA could be amended by including section 3(1)(d) that could be formulated as follows: '(d) irrespective of a choice of law'.

This open formulation would also clarify that a choice of law is not permitted regarding delictual claims[243] which would exclude any possibility to evade the application of the Act by a choice of law. In conjunction with the existing formulation of section 3(1) of the POPIA ('This Act applies to the processing of personal information'), the suggested amendment would indicate that a choice of law of the parties with regard to other legal fields would, in general, remain valid. This amendment would be the least invasive solution regarding the parties' freedom to contract.

Conclusion

The challenges imposed by emerging business models, based on the possibilities provided by modern data processing technologies can be addressed by extra-territorial scope rules. This article demonstrates that EU data protection law offers a modern concept in this regard. With Article 3(1) and (2) GDPR, the EU provided a regulatory framework aiming to tackle the problem of delocalisation of data processing, with an

242 *Standard Bank of South Africa Ltd v Efroiken and Newman* 1924 AD 171 at 185; *Guggenheim v Rosenbaum* (2) 1961 (4) SA 21 (W) 31; *Improvair (Cape) (Pty) Ltd v Establissements Neu* 1983 (2) SA 138 (C) 145; *Laconian Maritime Enterprises Ltd v Agromar Lineas Ltd* 1986 (3) SA (D) 509 at 525.

243 See for example the claim pursuant to s 99(1) of the POPIA.

extensive interpretation of the ‘establishment’ combined with rules for extra-territorial application. This is the first step to ensure a high level of data protection for data subjects located within the EU. Certain aspects of the requirements of such rules are strongly disputed, causing legal uncertainty. On the other hand, several decisions of the ECJ in the context of Article 4 DPD provide guidance for the interpretation thereof.

This investigation has also shown that the territorial scope rules of Article 3(1) and (2) GDPR can be embedded in the framework of private international law as unilateral conflict-of-law rules. A choice of the applicable data protection law is not permitted in the context of the GDPR. This serves the purpose of a high level of protection for data subjects and to prevent the evasion of the standard provided by the GDPR.

With regard to the status quo of South African data protection law, this article demonstrates that the POPIA provides for extra-territorial application. This could result in the application of the POPIA in numerous international cases, related to the processing of personal information by data-driven businesses. Nevertheless, a potential reform could lead to the adoption of a concept providing established principles for the application of (extra)territorial scope rule and to ‘move closer’ to the European standard. In this respect, three options for the legislature to harmonise the territorial scope of the Act based on the regulatory technique of Article 3 GDPR are offered.

With an amendment of the POPIA, the South African legislature could also significantly improve the protection of the rights of South African data subjects by facilitating communication and enforcement of the POPIA regarding responsible parties not domiciled within the Republic by implementing a holistic concept of representation. This would close a regulatory gap arising from the extra-territorial dimension of section 3(1)(b) of the POPIA. The drafters could also address the uncertain legal position on the possibility of a choice of law in the field of data protection law. In this respect, the drafters would have an opportunity to create a more advanced regulatory system than the GDPR, since this question has also remained unaddressed in the Regulation.

References

Acquisti A, Taylor C and Wagman L, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature <https://doi.org/10.1257/jel.54.2.442>

Albrecht JP, 'Das neue EU-Datenschutzrecht—von der Richtlinie zur Verordnung' (2016) Computer und Recht (CR) <https://doi.org/10.9785/cr-2016-0205>

Albrecht JP and Jotzo F, *Das neue Datenschutzrecht der EU* (Nomos 2017).

Baumann JS, 'The Provision of Personal Data as a Form of Payment in E-commerce Contracts: Determining the Applicable Data Protection and Contract Law in the Legal Framework of the European Union' (LLM Diss, University of Johannesburg, 2018).

Beyvers E and Herbrich T, 'Das Niederlassungsprinzip im Datenschutzrecht—am Beispiel von Facebook—der neue Ansatz des EuGH und die Rechtsfolgen' (2015) Zeitschrift für Datenschutz (ZD).

Borges G and Meents JG (eds), *Cloud Computing* (CH Beck 2016).

Brkan M, 'Data Protection and Conflict-of-Laws: A Challenging Relationship' (2016) 2 EDPL <https://doi.org/10.21552/EDPL/2016/3/8>

Burns Y and Burger-Smidt A, *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018).

Burri M and Schär R, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy <https://doi.org/10.5325/jinfopoli.6.2016.0479>

Dammann U and Simitis S, *EG-Datenschutzrichtlinie Kommentar* (Baden-Baden Nomos 1997).

Däubler W, 'Das Kollissionsrecht des neuen Datenschutzes' (2018) Recht der internationalen Wirtschaft (RIW).

Däubler W, Wedde P, Weichert T and Sommer I, *EU-DS-GVO und BDSG Kompaktkommentar* (2nd edn, Bund 2020).

De Stadler E and Esselaar P, *A Guide to the Protection of Personal Information Act* (Juta 2015).

Eckhardt J, 'EU-DatenschutzVO—Ein Schreckgespenst oder Fortschritt?' Computer und Recht (CR).

Ehmann E and Selmayr M (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, CH Beck 2018).

Eßer M, Kramer P and Von Lewinski K (eds), *Auernhammer DSGVO BDSG Kommentar* (7th edn, Carls Heymanns 2020).

Feiler L, Forgó N and Weigl M, *The EU General Data Protection Regulation (GDPR): A Commentary* (1st edn, GLP 2018).

Ferrari F (ed), *Concise Commentary on the Rome I Regulation* (2nd edn, Cambridge 2020) <https://doi.org/10.1017/9781108596633>

Forgó N, Helfrich M and Schneider J (eds), *Betrieblicher Datenschutz* (3rd edn, CH Beck 2019).

Forsyth CF, *Private International Law* (5th edn, Juta 2012).

Gläser I, Anwendbares Recht auf Plattformverträge—Fragen des IPR bei sozialen Netzwerken am Beispiel von Facebook' *Zeitschrift für IT-Recht und Digitalisierung* (MMR 2015).

Gola P (ed), *Datenschutz-Grundverordnung VO (EG) 2016/679 Kommentar* (2nd edn, CH Beck 2018).

Golland A, 'Der räumliche Anwendungsbereich der DS-GVO' *Datenschutz und Datensicherheit* (DuD 2018) <https://doi.org/10.1007/s11623-018-0955-8>

Golland A, *Datenverarbeitung in sozialen Netzwerken* (R&W 2018).

Gomille C, 'Datenschutzrechtlicher Löschungsanspruch gegen Suchmaschinenbetreiber—Anmerkung zu OLG Frankfurt am Main, Urteil vom 6.9 2018–16 U 193/17' 2019 Zeitschrift für Urheber- und Medienrecht—Rechtsprechungsdienst (ZUM-RD).

Gössl SL (ed), *Politik und Internationales Privatrecht* (Mohr Siebeck 2018).

Hacker P, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht' (2019) 5 Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW).

Härting N, 'Starke Behörden, schwaches Recht—der neue EU-Datenschutzentwurf' 2019' Betriebs-Berater (BB).

Hau W and Poseck R (eds), *BeckOK BGB* (57th edn, CH Beck 2021).

Kartheuser I and Klar M, 'Wirksamkeitskontrolle von Einwilligungen auf Webseiten—Anwendbares Recht und inhaltliche Anforderungen im Rahmen gerichtlicher Überprüfungen' (2014) Zeitschrift für Datenschutz (ZD).

Kegel G and Schurig K, *Internationales Privatrecht* (9th edn, CH Beck 2004).

Klar M, 'Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts—Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen' (2013) Zeitschrift für Datenschutz (ZD).

Klar M, 'Die extraterritoriale Wirkung des neuen europäischen Datenschutzrechts' (2017) Datenschutz und Datensicherheit (DuD) <https://doi.org/10.1007/s11623-017-0826-8>

Körber T, 'Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien' (2017) Zeitschrift für Urheber- und Medienrecht (ZUM).

Kropholler J, *Internationales Privatrecht* (Mohr Siebeck 2006).

Kühling J and Buchner B (eds), *Datenschutz-Grundverordnung/BDSG Kommentar* (3rd edn, CH Beck 2020).

Kühling J and Martini M, 'Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?' (2016) Europäische Zeitschrift für Wirtschaftsrecht (EuZW).

Kühling J and Martini M, Heberlein J, Kühl B, Nink D, Weinzierl Q and Wenzel M, *Die DSGVO und das nationale Recht* (MV Verlag 2016).

Kühling J and Sackmann F, 'Datenschutzordnung 2018—nach der Reform ist vor der Reform?!' (2018) Neue Zeitschrift für Verwaltungsrecht (NVwZ).

Kuner C, Bygrave LA and Docksey C (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford 2020) <https://doi.org/10.1093/oso/9780198826491.001.0001>

Langhanke C and M Schmidt-Kessel, 'Consumer Data as Consideration' (2015) EuCML.

Laue P, 'Öffnungsklauseln in der DS-GVO—Öffnung Wohin?' (2016) Zeitschrift für Datenschutz (ZD).

Lüttringhaus JD, 'Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21 Jahrhunderts' (2018) 117 Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss) <https://doi.org/10.1628/978-3-16-155766-8>

Lüttringhaus JD, *Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt* (Mohr Siebeck 2018).

Makulilo AB, *Protection of Personal Data in sub-saharan Africa* (Dr iur Thesis, University of Bremen 2012).

Makulilo AB (ed), *African Data Privacy Laws* (Springer 2016) <https://doi.org/10.1007/978-3-319-47317-8>

Makulilo AB, 'The GDPR Implications for Data Protection and Privacy Protection in Africa' (2017) 1 Intl J Data Protection Officer, Privacy Officer & Privacy Couns.

Martens SA, *Methodenlehre des Unionsrechts* (Mohr Siebeck 2013).

Metzger A, 'Dienst gegen Daten: Ein synallagmatischer Vertrag' (2016) 216 Archiv für die civilistische Praxis (AcP) <https://doi.org/10.1628/000389916X14752235857843>

Moura VD and de Vasconcelos CS (eds), *Data Protection in the Internet* (Springer 2020).

Müller M, *Die Öffnungsklauseln der Datenschutzgrundverordnung* (WWU Münster 2018).

Narciso M, '"Gratuitous" Digital Content Contracts in EU Consumer Law' (2017) EuCML.

Nebel M and Richter P, 'Datenschutz bei Internetdiensten nach der DS-GVO—Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf' (2012) Zeitschrift für Datenschutz (ZD).

Neels JL, 'Consumer Protection Legislation and Private International Law' (2012) Obiter.

Omlor S (ed), *Weltbürgerliches Recht – Festschrift für Michael Martinek zum 70' Geburtstag* (CH Beck 2020).

Oppong RF, *Private International Law in Commonwealth Africa* (Cambridge 2013) <https://doi.org/10.1017/CBO9781139031288>

Paal BP, and Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (3rd edn, CH Beck).

Piltz C, 'Rechtswahlfreiheit im Datenschutzrecht?' (2012) Kommunikation & Recht (K&R).

Piltz C, 'Der räumliche Anwendungsbereich des europäischen Datenschutzrechts' (2013) Kommunikation & Recht (K&R).

Piltz C, 'Die Datenschutz-Grundverordnung Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung' (2016) Kommunikation & Recht (K&R).

Plath K-U (ed), *DS-GVO/BDSG Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG* (3rd edn, Dr Otto Schmidt 2018).

Polenz S, 'Die Datenverarbeitung durch und via Facebook auf dem Prüfstand' (2012) Verbraucher und Recht (VuR).

Riesenhuber K (ed), *Europäische Methodenlehre* (3rd edn, De Gruyter 2015) <https://doi.org/10.1515/9783110332070>

Rochet JC and Tirole J, 'Two-Sided Markets: An Overview' (2004) 40 (12 March 2004) <https://web.mit.edu/14.271/www/rochet_tirole.pdf> accessed 28 April 2021.

Rochet JC and Tirole J, 'Two-sided Markets: A Progress Report' (2006) 37 RAND Journal of Economics <https://doi.org/10.1111/j.1756-2171.2006.tb00036.x>

Roos A, 'Privacy in the Facebook Era: a South African Legal Perspective' (2012) 129 South African Law Journal.

Roos A, 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected Content Principles' (2020) 53(3) Comparative and International Law Journal of Southern Africa <https://doi.org/10.25159/2522-3062/7985>

Roßnagel A, Nebel and Richter P, 'Besserer Internetdatenschutz für Europa—Vorschläge zur Spezifizierung der DS-GVO' (2013) Zeitschrift für Datenschutz (ZD).

Roßnagel A, Nebel and Richter P, 'Was bleibt vom Europäischen Datenschutzrecht?—Überlegungen zum Ratsentwurf der DS-GVO' (2015) Zeitschrift für Datenschutz (ZD).

Roth WH, 'Datenschutz, Verbandsklage, Rechtswahlklauseln in Verbraucherverträgen: Unionsrechtliche Vorgaben für das Kollisionsrecht' Praxis des Internationalen Privat- und Verfahrensrechts (2017) 37(5) IPRax.

Rustad ML and Koenig TH, 'Wolves of the World Wide Web: Reforming Social Networks' Contracting Practices' (2014) 49 Wake Forest Law Review.

Rysman M, 'The Economics of Two-Sided Markets' (2009) 23 Journal of Economic Perspectives <https://doi.org/10.1257/jep.23.3.125>

Schantz P, 'Die Datenschutz-Grundverordnung—Beginn einer neuen Zeitrechnung im Datenschutzrecht' (2016) Neue Juristische Wochenschrift (NJW).

Schantz P and Wolff HA, *Das neue Datenschutzrecht* (CH Beck 2017).

Schurig K, *Kollisionsnorm und Sachrecht* (2017 Duncker & Humblot 1981) <https://doi.org/10.3790/978-3-428-44825-8>

Simitis S, Hornung G and Döhmann I (eds), *Datenschutzrecht* (1st edn, Nomos 2019).

Spindler G and Schuster F (eds), *Recht der elektronischen Medien* (4th edn, CH Beck 2018).

Staudinger J (founder), *Kommentar zum Bürgerlichen Gesetzbuch (Internationales Vertragsrecht II)* (Sellier De Gruyter 2016).

Steinrötter B, 'Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern—Uneinheitliche Spruchpraxis oder bloßes Scheingefecht?' (2013) Zeitschrift für IT-Recht und Digitalisierung (MMR).

Steinrötter B, 'Feuertaufe für die EU-Datenschutz-Grundverordnung—und das Kartellrecht steht Pate' (2018) Europäisches Wirtschafts- und Steuerrecht (EWS).

Sydow G (ed), *Europäische Datenschutzgrundverordnung* (2nd edn, Nomos 2018).

Taeger J and Gabel D (eds), *Kommentar DSGVO—BDSG* (3rd edn, R&W 2019).

Thon M, 'Das internationale Datenprivatrecht der DS-GVO' (2020) 84 RabelsZ <https://doi.org/10.1628/rabelsz-2020-0003>

Uecker P, *Extraterritoriale Regelungshoheit im Datenschutzrecht* (Nomos 2017) <https://doi.org/10.5771/9783845288000>

Uecker P, 'Extraterritorialer Anwendungsbereich der DS-GVO' (2019) *Zeitschrift für Datenschutz* (ZD).

Van der Merwe D, Roos, A Pistorius T, Eiselen S and Nel S, *Information and Communications Technology Law (*2nd edn, LexisNexis 2016),

Von Bar C and Mankowski P, *Internationales Privatrecht Band 1* (2nd edn, CH Beck 2003).

Wieczorek M, 'Der räumliche Anwendungsbereich Der EU-Datenschutz-Grundverordnung' (2013) 37 *Datenschutz und Datensicherheit* (DuD) <https://doi.org/10.1007/s11623-013-0268-x>

Wolff HA and Brink S (eds), *BeckOK Datenschutzrecht* (35th edn, CH Beck 2020).

Ziebarth W, 'Das Datum als Geisel—Klarnamenspflicht und Nutzeraussperrung bei Facebook' (2013) Zeitschrift für Datenschutz (ZD).

Cases

European Court of Justice (ECJ)

Case 6/64 *Costa v E.N.E.L.* [1964] ECR 587.

Case 283/81 *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health* [1982] ECR 3417.

Case C-101/01 *Lindqvist* [2003] ECR I-12992.

Case C-524/06 *Huber v Bundesrepublik Deutschland* [2008] ECR I-9725.

Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Heller* [2010] ECR I-12570.

Case C-184/12 *Unamar v Navigation Maritime Bulgare* [2013] EU:C:2013:663.

Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317.

Case C-230/14 *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] EU:C:2015:639.

Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] EU:C:2016:612.

Case C-135/15 *Republik Griechenland v Nikiforidis* [2016] EU:C:2016:774.

Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] EU:C:2018:388.

Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551.

Case C-507/17 *Google LLC v Commission nationale d' l'informatique et des libertés (CNIL)* [2019] EU:C:2019:772.

Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801.

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* [2020] ECLI:EU:C:2020:559.

French Courts

Case No 430810 [2020] *Conseil d'Etat*, Decision (19 June 2020) – *SOCIÉTÉ GOOGLE LLC.*

German Courts

Case No I ZR 7/16 *Bundesgerichtshof*, Judgment (28 May 2020) [2020] *Neue Juristische Wochenschrift* (NJW) 2540.

Case No 16 O 551/10, [2012] *Landgericht Berlin*, Judgment (6 March 2012) *Zeitschrift für Datenschutz* (ZD) 276.

Case No 8 B 60/12 *Verwaltungsgericht Schleswig*, Decision (14 February 2013) [2013] *Zeitschrift für Datenschutz* (ZD) 245.

Case No 5 U 42/12 [2014] *Kammergericht*, Judgment (24 January 2014) *Zeitschrift für Datenschutz* (ZD) 412.

Case No 16 U 193/17 *Oberlandesgericht Frankfurt am Main*, Judgment (6 September 2019) [2019] *Zeitschrift für Urheber- und Medienrecht – Rechtsprechungsdienst* (ZUM-RD) 79.

South African Courts

Bisonbord Ltd v K Braun Woodworking Machinery (Pty) Ltd 1991 (1) SA 482 (AD).

Competition Commission of South Africa v Media 24 (Pty) Limited 2019 (5) SA 598 (CC).

Improvair (Cape) (Pty) Ltd v Establissements Neu 1983 (2) SA 138 (C).

Laconian Maritime Enterprises Ltd v Agromar Lineas Ltd 1986 (3) SA (D) 509.

Sibakhulu Construction (Pty) Ltd v Wedgewood Village Golf Country Estate (Pty) Ltd 2013 (1) SA 191 (WCC).

Standard Bank of South Africa Ltd v Efroiken and Newman 1924 AD 171 at 185; *Guggenheim v Rosenbaum* (2) 1961 (4) SA 21 (W).

UK Courts

Johnson v Medical Defence Union [2007] EWCA Civ 26.

Law Society and Others v Kordowski [2011] EWCH 3185 (QB).

Soriano v Forensic News LLC [2021] EWHC 56 (QB).

Legislation

European Union

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37 as amended by Directive 2009/136/EC [2009] OJ L 337/37.

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [2006] OJ L 376/36.

Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests [2009] OJ L 110/30.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

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

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

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

EU Member States and the UK

Bundesdatenschutzgesetz (2001) (Germany).

Datenschutzgesetz 2000 (Austria).

Telemedia Act (Germany).

UK Data Protection Act 1998 (UK).

United Kingdom General Data Protection Regulation (UK).

Wet Bescherming Persoonsgegevens (Netherlands).

South Africa

Competition Act 89 of 1998.

National Credit Act 34 of 2005.

Protection of Personal Information Act 4 of 2013.

Government Notices

GG 37067 (26 November 2013) GN 912.

Proclamation No R 21 in GG 11136 (22 June 2020) GN 43461.