universität wien

Exposé zum Dissertationsvorhaben

"The GDPR as an instrument of regulating the Digital Single Market"

Verfasser

Mag. Felix Zopf

Angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Doctor iuris)

Wien, November 2019

Studienkennzahl: UA 783 101
Dissertationsgebiet: Rechtswissenschaften
Dissertant: Felix Zopf
Matrikelnummer: 01306145
Betreuer: Univ.-Prof. Dr. Nikolaus Forgó

1. Introduction

The overall aim of this thesis is to perform an in-depth analysis of the General Data Protection Regulation[1] (GDPR) in the context of the Digital Single Market.[2] The idea of the Digital Single Market is to adapt the already existing Single Market of the EU to technological changes. The GDPR contributes to this goal in the area of data protection law. A literature review did only identify limited research on the GDPR in the context of the Digital Single Market.[3]

Jean-Claude Juncker made the Digital Single Market a priority for the whole EU Commission under his presidency (2014 – 2019).[4] Following this prioritisation in 2015, the Commission developed 'A Digital Single Market Strategy for Europe'.[5] The EU-Commission describes the Digital Single Market as the following:

> A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.[6]

This definition addresses several key principles of the EU: the fundamental freedoms of the Single Market (the free movement of goods, persons, services and capital) regulated in Arts. 26 – 66 of the Treaty on the Functioning of the European Union[7] (TFEU); the rules of fair competition in the Single Market regulated in Arts. 101 – 109 TFEU; the fundamental right of data protection laid down in Art. 8 Charter of Fundamental Rights[8] (Charter); the principle of a high level of consumer protection enshrined in Art. 38 Charter[9].

The Digital Single Market Strategy is built on three pillars:[10]

1) Better access for consumers and businesses to online goods and services across Europe.
2) Creating the right conditions for digital networks and services to flourish.
3) Maximising the growth potential of the European Digital Economy.

Data protection falls under the second pillar.[11] The Digital Single Market Strategy mentions in the area of data protection two legislative instruments:[12] The GDPR and the ePrivacy Directive[13]. The Mid-Term Review of the Digital Single Market reiterates the importance of data protection and demands the

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[2] EU-Commission, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final.

[3] E.g. Thomas Zerdick, 'Art. 1' in Eugen Ehmann and Martin Selmayr (eds), *Datenschutz-Grundverordnung 2. Auflage* (C. H. Beck 2018) mn 13; Andrej Savin, 'Regulating internet platforms in the EU - The emergence of the 'Level playing Field'' (2018) Computer Law & Security Review, 1215.

[4] See Jean-Claude Juncker, 'A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change - Political Guidelines for the next European Commission' <https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf> accessed 07 October 2019.

[5] COM (2015) 192 final.

[6] COM (2015) 192 final, 3.

[7] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

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

[9] See also Arts. 12, 114 (3), 169 TFEU.

[10] COM (2015) 192 final, 3-4.

[11] COM (2015) 192 final, 13.

[12] COM (2015) 192 final, 13.

[13] 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 L201/37.

swift adoption of the new ePrivacy Regulation[14] as replacement for the ePrivacy Directive. This has not happened yet, because the Council has not reached a general approach.[15] This means that for now the GDPR and the ePrivacy Directive are the data protection laws regulating the Digital Single Market. The GDPR was also included in the legal framework of the European Economic Area (EEA).[16] This means that the GDPR is also fully applicable in Liechtenstein, Norway and Iceland. Therefore the findings about the GDPR (at least to some extent) are also true for these countries.

The following chapters will analyse the state of the art regarding the scope of application of the GDPR, the principles of the GDPR in the Digital Single Market and the enforcement of the GDPR in more detail in order to define the research questions.

2. Scope of applicability

The scope of application of the GDPR is important in the context of the Digital Single Market, because it is a prerequisite that the GDPR is applicable in regard to the Digital Single Market to further analyse the GDPR in this context. The scope of application of the GDPR is split between the "Material scope" (Art. 2 GDPR) and the "Territorial scope" (Art. 3 GDPR).

Personal data means any information relating to an identified or identifiable natural person, the data subject.[17] 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'.[18] But the processing of personal data 'in the course of an activity which falls outside the scope of Union law' and 'by a natural person in the course of a purely personal or household activity' are (among others) excluded from the GDPR.[19] This has not changed in comparison to the Data Protection Directive (DPD)[20].

The DPD was focused on the physical location of the data processing activity for its territorial application scope, either in the form of an establishment of the data controller or the location of the data processing equipment itself.[21] The physical presence of the data processing equipment for the purpose of only transporting personal data through the EU did not lead to the applicability of the DPD.[22] This was a traditional approach towards regulation in an international context as it was based on geographical locations.

The GDPR has a somewhat different approach to the territorial scope. The title of Art. 3 GDPR is "Territorial scope", but the wording seems not to fully capture its whole content. There is a distinction between controllers and processors of personal data that are established in the Union and those who

[14] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final.
[15] See <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010> accessed 07 October 2019.
[16] 'Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]' [2018] OJ L183/23.
[17] Art. 4 (1) GDPR. Legal persons are therefore not covered by the GDPR.
[18] Art. 2 (1) GDPR.
[19] Art. 2 (2) (a) and (c) GDPR.
[20] 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 [1996] OJ L281/31.
[21] Benjamin Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) International Data Privacy Law 1 <https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipz003/5475799> accessed 07 October 2019.
[22] Art. 4 (1) (c) DPD.

are not established in the Union. For controllers and processors established in the Union, the GDPR applies in the context of the activities of this establishment 'regardless of whether the processing takes place in the Union or not'.[23] Therefore, the "only" geographical link to the EU is the place of the establishment. Neither the data subject nor the processing activity must have a connection to the Union.

In the case that the controllers and processors are not established in the Union, the data subjects must be in the EU and the processing activities must relate to 'the offering of goods or services' or 'the monitoring of their behaviour as far as their behaviour takes place within the Union'.[24] These two cases can be summarised under the term "targeting criterion"[25]. The geographical link to the EU is the location of the data subjects. Additionally, specific activities related to them are required, which is a non-geographical factor.

Overall Art. 3 GDPR is a combination of geographical and non-geographical factors.[26] This means that the GDPR in regard to the applicability of data protection law applies a mixture of traditional approaches (mainly the establishment criterion for data controllers and processors) and a new factor (the targeting criterion). All in all, the GDPR is applicable to businesses acting in the Digital Single Market. Having established the applicability of the GDPR in the context of the Digital Single Market, the following chapters will analyse the GDPR in this regard in more detail.

3. Principles of the GDPR in the Digital Single Market

The GDPR is based (among others[27]) on three concepts in regard to the Digital Single Market:

1) Establishing a (more) coherent legal framework that enhances legal certainty in order to foster the development of the digital economy in the Union.[28]
2) Ensuring the free flow[29] of personal data within the EU to allow the proper functioning of the (Digital) Single Market.[30]
3) Establishing a "level playing-field" in regard to the processing of personal data to ensure that
    a. European and non-European businesses have to follow the same rules when offering services to European consumers and therefore engage in fair competition.[31]
    b. all European businesses have to follow the same rules, wherever they are located in the EU.[32]

The following subsections will go into more detail regarding these three concepts.

---

[23] Art. 3 (1) GDPR.
[24] Art. 3 (2) GDPR.
[25] The EDPB uses this terminology, EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation' <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf> accessed 28 October 2019.
[26] Art. 3 (3) GDPR (mainly) applies to public bodies and is therefore not in the focus of this work. A similar observation is made by Douwe Korff, 'The territorial (and extra-territorial) application of the GDPR' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3439293> accessed 07 October 2019.
[27] E.g. the concept of technological neutrality (recital 15 GDPR) or privacy-by-design (Art. 25 GDPR).
[28] Recital 7 and 13 GDPR.
[29] The GDPR seems to use the terms free flow and free movement of personal data interchangeable, see for this recital 3, 6, 9, 13, 16, 53, 123, 166, 70 and Art. 1, Art. 4 (24), Art. 35 (6) and Art. 51 (1) GDPR.
[30] Recital 13 GDPR.
[31] Viviane Reding, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' (4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm> accessed 07 October 2019.
[32] Recital 13 GDPR.

3.1. A (more) coherent legal framework

Firstly, the change of the legal instrument from a directive to a regulation is an instrument of reaching a (more) coherent legal framework. A directive demands from the Member States to transpose the legal content of the directive into national law. The transformed law only needs to achieve the result required by the directive and therefore the Member States are free to choose the way to achieve this result.[33] Whereas a regulation has only one binding text for the whole Single Market.

However, the GDPR allows Member States to further specify or change certain data protection rules.[34] These specification possibilities must be explicitly allowed by the GDPR and those parts of the GDPR are sometimes called "opening clauses" in the literature.[35] The European Commission calls them "specification clauses".[36] The possibility of further specification can be found in the title of the GDPR, as the word *General* in General Data Protection Regulation leaves space for more detailed rules. The TFEU knows only "normal"[37] Regulations in its Art. 288 (2), which have general application and are directly applicable in all Member States. The German literature describes Regulations, where the Member States can (or must) enact additional national legislation as "limping"[38] Regulations.[39] The GDPR seems to be a prominent example of such a limping Regulation. Depending upon the counting, there are up to 70 specification clauses.[40]

Secondly, the GDPR tries to ensure that the supervisory authorities (SAs) apply the law more coherently in comparison to the DPD. See for this in detail point 4.

3.2. The free flow of personal data

The EU-Commission sees the free flow of data as a priority for the Digital Single Market.[41] The EU-Commission sees 'unjustified data localisation requirements' as barriers to the free movement of data within the EU,[42] but this is not an actual definition of the free flow of data. The GDPR also does not define what 'free flow of personal data' actually means. In lack of an official definition, I would define it in the following way: the free flow of personal data is an abstract concept to describe the borderless transfer of personal data within the Single Market. The competence of the EU to enact legislation for the free movement of personal data (and the protection of individuals with regard to the processing of personal data) stems from Art. 16 TFEU.

Data protection is – as already mentioned under section 1. – a fundamental right. However, data protection laws need not only to guarantee the fundamental right of data protection, but also a variety of different fundamental rights.[43] Among these fundamental rights is the freedom to conduct a business laid down in Art. 16 Charter. Secondary legislation regarding the free flow of personal data

[33] See Markus Kotzur, in Rudolf Geiger, Daniel-Erasmus Khan and Markus Kotzur (eds), *European Union Treaties – A Commentary* (CH Beck Hart 2015) Article 288 TFEU mn 11.
[34] E.g. Arts. 6 (2), 8 (1), 88 GDPR.
[35] Eg Jan Pohle, 'Data Privacy Legislation in the European Union Member States – A Pratical Overview' (2018) Computer Law Review International, 97.
[36] European Commission, 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018' COM (2018) 43 final; see also <www.europarl.europa.eu/doceo/document/P-8-2018-003121-ASW_EN.html> accessed 07 October 2019.
[37] The TFEU never mentions a General Regulation.
[38] A limping Regulation means a Regulation that is not fully functional by its own.
[39] Eg Markus Kotzur, in Rudolf Geiger, Daniel-Erasmus Khan and Markus Kotzur (eds), *European Union Treaties – A Commentary* (CH Beck Hart 2015) Article 288 TFEU mn 9.
[40] Gerrit Hornung and Indra Spiecker, 'Einleitung' in Spiros Simitis, Gerrit Hornung and Indra Spiecker (eds), *Datenschutzrecht* (Nomos 2019) mn 226.
[41] E.g. COM (2015) 192 final, 14 f; EU-Commission, 'Building a European Data Economy' COM (2017) 9 final, 5-8.
[42] COM (2017) 9 final, 5.
[43] See Recital 4 GDPR.

has to consider both, the fundamental right of data protection and the freedom to conduct a business. This has to be kept in mind when analysing the GDPR.

The GDPR has the goal to assure the free movement (flow) of personal data.[44] The GDPR blocks Member States from restricting or prohibiting the free movement of personal data within the Union for reasons connected with the protection of natural persons with regard to the processing of personal data.[45] The GDPR assumes that different implementations of the DPD had a negative impact on the free flow of data.[46] Taken this assumption into consideration, the idea of fostering the free movement of personal data and the fact that the GDPR is a limping Regulation, because of the specification clauses, seems contradictory. The GDPR also sees this problem and limits the application scope of a particular specification clause[47] to non-cross-border processing activities.[48] However, the GDPR does not seem to address the problem for any other specification clause.

Additional problems for the free flow of personal data arise, when personal data and non-personal data are mixed in one dataset (mixed dataset). The Regulation for the free flow of non-personal data[49] complements the rules of the GDPR regarding the free flow of data and provides a framework to reduce data localisation requirements for non-personal[50] data. The GDPR applies to mixed datasets that are 'inextricably linked'.[51] Considering the problem of inextricably linked mixed datasets, regulation for the free flow of non-personal data is also relevant for this thesis.

3.3. Level playing-field

Levelling the playing-field means that the same rules apply to everybody,[52] and it is part of an effort to provide a framework for fair competition. One of the goals of the GDPR is 'to ensure a "level playing-field" as to between businesses based in the EU and businesses based outside the EU, but doing business on the European market'.[53] The same is true for businesses within different Member States.[54] The concept of a "level playing-field" is related to different areas throughout this thesis (e.g. the territorial scope, specification clauses) and is therefore important for this thesis.

4. Enforcement of the GDPR

As mentioned under point 3.1., the GDPR wants to establish a (more) coherent legal framework. There are two enforcement related aspects of this: 1) A (more) consistent application of the GDPR for single businesses by the competent SAs. 2) A (more) consistent application of the GDPR as a whole by the different SAs in the EU.

---

[44] See Arts. 1 and 51 (1) and recitals 6, 13, 53 and 123 GDPR.
[45] Art. 1 (3) GDPR.
[46] See Recital 9 GDPR.
[47] Art 9 (4) GDPR regarding the processing of genetic data, biometric data or health data.
[48] Recital 54 GDPR.
[49] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.
[50] Non-personal data is all the data that is not personal data, see Art. 3 (1) Regulation 2018/1807 and Art. 4 (1) GDPR.
[51] Art. 2 (2) of the Regulation for the free flow of non-personal data. See also EU-Commission, 'Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union' COM(2019) 250 final, 7-10.
[52] E.g. Viviane Reding, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' (4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm> accessed 07 October 2019.
[53] Dan Svantesson, 'Commentary on Art. 3 GDPR' in Christopher Kuner and other (eds), *Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)* (2018) 3.
[54] Recital 13 GDPR.

4.1. Supervisory authorities

The main enforcement agencies of the GDPR are the SAs, this has not changed between the DPD and the GDPR. But the GDPR has much more detailed rules on the SAs, especially regarding the cooperation between the different SAs in the EU[55] in order to foster a (more) consistent application.

As a standard rule, each SA has the competence to perform the tasks assigned to it and exercise the powers conferred on it only 'on the territory of its own Member State'.[56] This applies for data controllers and processors in the same manner and covers

> in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, (…) processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory.[57]

In the standard case, the scope of each SA´s jurisdiction is quite wide and can potentially overlap with the jurisdiction of other SAs.

In the case of "cross-border processing"[58] of personal data, the SA of the "main establishment"[59] (or the single establishment) of the data controller or processor becomes the "lead supervisory authority"[60] (lead SA) and is in general the responsible SA. However, another SA is still competent 'if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'.[61] Art. 60 of the GDPR has detailed rules for the cooperation of the lead SA and the "supervisory authority concerned"[62], which has some connection with the data controller or processor. The system of lead SAs helps the consistent application of the GDPR for single businesses. The downside of this system is that it can only work for those who are established in the EU as a "main establishment" is needed.[63] None of the data controllers or processors falling under Art. 3 (2) GDPR therefore have a lead SA, which reduces the effectiveness of this system.

In addition to the system of lead SAs, the consistency mechanism of the European Data Protection Board (EDPB) provides assistance in a (more) unified application of the GDPR in general.[64] The EDPB issues an opinion in cases regarding certain implementation acts of one SA and cases regarding any matter of general application or producing effects in more than one Member State.[65] A binding decision has to be adopted regarding the system of lead SAs and if one SA does not follow an opinion of the EDPB.[66] The consistency mechanism in general seems a good instrument to foster a unified application of the GDPR. But the huge downside of the implementation of this system in the GDPR is the fact that only applies to SAs and not to other authorities concerned with the enforcement of the GDPR, as explained in more detail in the following sections.

---

[55] This includes in general the SAs of the EEA countries, but the SAs of the three EEA countries do not have the right to vote on the board, see Art. 1 (a) of the Decision of the EEA Joint Committee.
[56] Art. 55 (1) GDPR.
[57] Recital 122 GDPR.
[58] Defined in Art. 4 (23) GDPR.
[59] Defined in Art. 4 (16) GDPR.
[60] Defined in Art. 56 (1) GDPR.
[61] Art. 56 (2) GDPR.
[62] For the definition see Art. 4 (22) GDPR.
[63] Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority', WP 244 rev.01 (2017) 10, officially endorsed by the EDPB on 25 May 2018.
[64] See Arts. 63 – 67 GDPR.
[65] Art. 64 (1) and (2) GDPR.
[66] Art. 65 (1) GDPR.

4.2. Right to an effective judicial remedy

The GDPR provides for an effective judicial remedy against a legally binding decision of a supervisory authority and for data subjects against a controller or processor, if the data subject considers their rights have been infringed.[67] The Charter requires such an effective judicial remedy.[68] Courts are not part of the EDPB and therefore not subject to the consistency mechanism. This reduces the overall effectiveness of the consistency mechanism.

There is an additional problem depending on the national law: the two different judicial remedies can create two "branches" of enforcement, when the remedy against a decision of a SA ends up in a different court system than the remedy against the controller or processor. This may lead to problems, if contradictory decisions are made by the courts.

4.3. Enforcement by other authorities

Data protection law can also be enforced by other authorities: First, there is the idea that a violation of data protection law can be a form of abuse of market power.[69] Second, a violation of data protection law can be seen as an unfair commercial practice[70].[71] This brings two new groups of stakeholders to the table in regard to the enforcement of data protection: competition authorities and those concerned[72] with the enforcement of unfair commercial practice.

This situation creates an additional threat to the coherent application of the GDPR as the issues are similar to the courts raised under point 4.2.: Competition authorities and those concerned with the enforcement of unfair commercial practice are not part of the EDPB and therefore not subject to the consistency mechanism. Contradictory decisions between the SAs on the one hand and competition authorities and those concerned with the enforcement of unfair commercial practice on the other are also possible.

5. Research questions and outline

5.1. Research questions

The overall aim of this thesis is to perform an in-depth analysis of GDPR in the context of the Digital Single Market:

1. To whom is the GDPR applicable in the context of the Digital Single Market?
2. How does the system of specification clauses interact with the principles of the GDPR in conjunction with the Digital Single Market?
3. Who is enforcing the GDPR in the context of the Digital Single Market and to which extend is there a coordination between the different enforcement bodies?

[67] Arts. 78 (1) and 79 (1) GDPR.

[68] Art. 47 Charter; recital 4 and 141 GDPR.

[69] E.g. Wolfgang Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (2016) GRUR Int., 639; Samson Y. Esayas, 'Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law' (2018) International Data Privacy Law, 181; Giuseppe Colangelo and Mariateresa Maggiolino, 'Data accumulation and the privacy–antitrust interface: insights from the Facebook case' (2018) International Data Privacy Law, 224.

[70] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L149/22.

[71] Catalina Goanta and Stephan Mulders, ''Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media' (2019) EuCML, 136.

[72] The Unfair Commercial Practices Directive does not harmonize the enforcement, see Art. 11.

5.2. Outline of the dissertation

Part I: Introduction

Part II: Scope of applicability

Part III: Principles of the GDPR in the Digital Single Market

Part IV: Enforcement of the GDPR

Part V: Summary

5.3. Timeline

WiSe 2019/20: signing of the Dissertationsvereinbarung; writing Part II

SoSe 2020: finishing Part II; writing Part III

WiSe 2020/21: finishing Part III; writing Part IV; Seminar im Dissertationsfach

SoSe 2021: finishing Part IV; writing Part I and V; final corrections

WiSe 2021/22: Defensio

6. Relevant literature

Albrecht J and Jotzo F, 'Das neue Datenschutzrecht der EU' (Nomos 2017)

Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority', WP 244 rev.01 (2017)

Azzi A, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation' (2018) JIPITEC, 126

Colangelo G and Maggiolino M, 'Data accumulation and the privacy–antitrust interface: insights from the Facebook case' (2018) International Data Privacy Law, 224

Ehmann E and Selmayr M (eds), *Datenschutz-Grundverordnung 2. Auflage* (C. H. Beck 2018)

Esayas S, 'Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law' (2018) International Data Privacy Law, 181

EU-Commission, 'Impact Assessment', SEC (2012) 72 final

– – 'A Digital Single Market Strategy for Europe' COM (2015) 192 final

– – 'Building a European Data Economy' COM (2017) 9 final

– – 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final

– – 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018' COM (2018) 43 final

Feiler L and Forgó N, *EU-Datenschutz-Grundverordnung* (Verlag Österreich 2017)

Geiger R, Khan D-E and Kotzur M (eds), *European Union Treaties – A Commentary* (CH Beck Hart 2015)

Goanta C and Mulders S, ''Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media' (2019) EuCML, 136

Gola P (ed), *Datenschutz-Grundverordnung 2. Auflage* (C. H. Beck 2018)

Gömann M, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) Common Market Law Review, 567

Greze B, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) International Data Privacy Law 1 <https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipz003/5475799> accessed 07 October 2019

Hörnle J, 'Juggling more than three balls at once: multilevel jurisdictional challenges in EU Data Protection Regulation' (2019) International Journal of Law and Information Technology, 142

Juncker J-C, 'A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change - Political Guidelines for the next European Commission' <https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf> accessed 07 October 2019

Kerber W, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (2016) GRUR Int., 639

Kindt E, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) Computer Law & Security Review, 729

Korff D, 'The territorial (and extra-territorial) application of the GDPR' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3439293> accessed 07 October 2019

Kuner C and other (eds), *Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)* (2018)

Kühling J and Buchner B (eds), *Datenschutz-Grundverordnung 2. Auflage* (C. H. Beck 2018)

Knyrim R (ed), *Der DatKomm - Praxiskommentar zum Datenschutzrecht* (Manz 2019)

Pohle J, 'Data Privacy Legislation in the European Union Member States – A Pratical Overview' (2018) Computer Law Review International, 97

Reding V, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' (4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm> accessed 07 October 2019

Savin A, 'Regulating internet platforms in the EU - The emergence of the 'Level playing Field'' (2018) Computer Law & Security Review, 1215

Simitis S, Hornung G and Spiecker I (eds), *Datenschutzrecht* (Nomos 2019)

Sydow G (ed), *Europäische Datenschutzgrundverordnung 2. Auflage* (Nomos Manz Dike 2018)

Wagner J and Benecke A, 'National Legislation within the Framework of the GDPR' (2016) 2 European Data Protection Law Review, 353