Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 41

General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues

Kristina Yuliyanova Chakarova

2019

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Kristina Yuliyanova Chakarova is a graduate of the University of Vienna School of Law, where she earned her LLM degree in European and International Business Law with distinction in 2019. She also holds a Master of Laws degree from Sofia University St. Kliment Ohridski. Her main areas of interest include data protection, intellectual property, competition and corporate law. She is currently pursuing a career as a lawyer at the law firm Schoenherr.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Kristina Yuliyanova Chakarova, General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues, Stanford-Vienna European Union Law Working Paper No. 41, http://ttlf.stanford.edu.

Copyright

Abstract

The General Data Protection Regulation ("GDPR") established the new data protection framework in the European Union and repealed the previous legal act which regulated that matter - the 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. However, the aim of the new legal act was not to revolutionise EU data protection law, but rather to eliminate the fragmentation and differences between Member State laws under the previous regime, and thereby to fully harmonise EU data protection law and remove the obstacles to flows of personal data within the Union.

The problem, however, is that the GDPR contains a significant amount of opening clauses, which enable Member States to enact their own legislation by further specifying the requirements of the regulation. In turn, these flexibilities threaten to once again fragment the EU data protection framework. In addition, the removal of the conflict of laws provisions which existed under the previous data protection regime, seems to further exacerbate the problem.

The purpose of this thesis is to answer two main questions. First, whether the amount of the opening clauses in the GDPR indeed undermines its purpose to establish a uniform data protection regime in the Union. Second, given the expected differences in national law due to the opening clauses and the lack of general applicable law rule, how could an eventual conflict of laws issue be resolved under the new data protection regime?

In order to answer these questions, Section II of this thesis starts with an overview of the opening clauses, focusing in detail on the opening clauses which are more important from a practical perspective for the day-to-day business activities of controllers and processors in the private sector. Section III examines the approach of five different Member States to the opening clauses in order to evaluate whether Member States in fact make use of the provided opportunity to enact legislation within the delegated competence, and thereby creating diverging data protection law within the Union. Finally, Section IV examines whether the GDPR provides a solution for establishing the applicable law in case provisions enacted within the opening clauses differ from one Member State to another, and if not what other solutions are there.

The conclusion of the thesis to the first question is not only that there indeed are too many opening clauses, but also that Member States actively legislate within the delegated competences, sometimes even arguably beyond them. This leads to inconsistencies in the data protection regime within the EU and thus undermines the aim of the GDPR to establish a uniform legal framework. As regards the second question, the GDPR does not provide general conflict of laws provisions which further exacerbates the issues caused by the diverging national legislation. However, the law literature provides possible solutions to the issue, such as analogy to the rules for determining lead supervisory authority, relying on general EU conflict of laws rules (e.g., Rome I Regulation), relying on national conflict of laws rules, or deriving applicable law indications from certain opening clauses. It remains to be seen whether further guidance of the European Data Protection Board or case law of the Court of Justice of the European Union would clarify the conflict of laws concerns and address problematic national provisions contrary to the GDPR.

Acknowledgements

I would like to express my special gratitude and thanks to my supervisor, Dr. Lukas Feiler, lecturer at the University of Vienna Law School, for further stoking my interest in data protection law and for providing me with insightful and invaluable guidance on this thesis.

I would also like to express my endless gratitude towards my beloved partner, Lyubomir, who is always by my side and without whom my current LL.M. endeavour would not have been possible.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ADPA	Austrian Data Protection Act
BPDPA	Bulgarian Personal Data Protection Act
CJEU	Court of Justice of the European Union
DDPA	Danish Data Protection Act
DPO	Data Protection Officer
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
GFDPA	German Federal Data Protection Act
IDPA	Irish Data Protection Act

I. Introduction

The General Data Protection Regulation (hereinafter GDPR or Regulation)[1] became directly applicable on 25 May 2018, a date perceived by many as the 'end of the world as we know it',[2] especially if we consider the media attention which was drawn to it. Nevertheless, as the European Commission fittingly remarks, the new Regulation is not a revolution, but rather an evolution.[3]

Before the GDPR, the processing of personal data in the European Union was regulated by Directive 95/46/EC[4] (hereinafter Directive) which aimed to approximate the laws of the Member States, by ensuring a high level of protection.[5] During the years of application of the Directive, that aim did not seem to be sufficiently fulfilled. To a large extent this was due to the different approaches of the Members States – some would apply the minimum standard set by the Directive combined with a laxer approach to enforcement, whereas others would enact stricter rules and thoroughly monitor compliance. The 'fragmentation of personal data protection' in the European Union has been severely criticised, especially by the companies[6] which were concerned by the deficient legal certainty and need for harmonisation in the field of personal data protection.[7]

---

[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] Thomas Stoeckle, 'GDPR – Much Ado About Nothing, or the End of the World As We Know It?' (*The Small Data Forum Podcast*, 11 June 2018) <www.smalldataforum.com/2018/06/11/gdpr-much-ado-about-nothing-or-the-end-of-the-world-as-we-know-it/> accessed 10 June 2019.

[3] European Commission, 'The General Data Protection Regulation (GDPR) is Now Applicable. Are You Ready for It?' (25 May 2018) <https://ec.europa.eu/easme/en/news/general-data-protection-regulation-gdpr-now-applicable-are-you-ready-it> accessed 10 June 2019.

[4] 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 L281/31.

[5] Directive, recital 10.

[6] For the purposes of this thesis, references to a company or companies should be considered a reference to organisations subject to the GDPR rules either as a controller, or as a processor, whatever the case may be.

[7] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' COM (2012) 011 final.

Therefore, as a more efficient legal instrument in terms of harmonisation, the EU legislator repealed the Directive and replaced it with a regulation.[8] Briefly put, the most significant difference between the two instruments is that a regulation is directly applicable in all Member States, which decreases legal fragmentation.[9] No intermediary national legislative acts have to be implemented, and as a result there is practically one single law applicable in all 28 Member States, instead of 28 different implementing national acts. The most notable downside of the Directive was that it resulted in different data protection standards throughout the Member States, as in some cases it was inconsistently and even inaccurately transposed.[10] For instance, some Member States did not follow the wording of the Directive and incorrectly extended the scope of application of their national data protection laws.[11]

Even though the GDPR repealed the Directive, it does not introduce entirely new legislation. On the contrary, the Regulation recognises and builds on the achievements and the lessons learned from the old regime, instead of introducing a fundamentally new legal framework. The GDPR's main objective is rather to overcome the inconsistencies in the levels of data protection caused by the different implementation and application of the Directive by ensuring an 'equivalent' level in all Member States.[12]

However, it seems that the EU again did not quite manage to achieve the desired level of harmonisation. This time the reason is not the nature of the legal instrument, but is instead some intentional and non-intentional omissions.

[8] Ibid.
[9] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, art 288.
[10] Jiahong Chen, 'How the Best-Laid Plans Go Awry: The (Unsolved) Issues of Applicable Law in the General Data Protection Regulation' (2016) 6(4) International Data Privacy Law 310, 315.
[11] Ibid.
[12] GDPR, recitals 9-10.

On the one hand, the intentional omissions seem to be caused by the inability (or unwillingness) of Member States to agree on a number of issues, as a result of which they were left as opening clauses. The latter are provisions which delegate competences to national legislators to lay down further rules in certain areas.[13] In practice, this means that Member States would be allowed and to some extent even required (as long as they want to make use of certain provisions under the GDPR) to enact national laws within these provisions. The problem, however, is that the Regulation contains such a significant amount of opening clauses, that they pose the threat of once again fragmenting the EU data protection framework.

This situation has already resulted in diverging national regimes on some important data protection matters. Whereas some of the different rules cannot reasonably be expected to cause inconveniences, there are particular areas where deviating rules are more likely to impede cross-border flow of data (e.g., age threshold for consent of children in the online world,[14] processing in the employment context,[15] freedom of expression and information,[16] etc.). Thus, the issue of legal uncertainty as to what are the exact data protection rules across different Member States arises again. In addition, similarly to the Directive, some Member States have enacted derogations which are not in line with the delegated competences, which has led to a deteriorated level of data protection in conflict with the Regulation.[17] The outlined issues not only undermine the main aim of the GDPR to ensure uniform data protection framework, but are also detrimental to its other

[13] GDPR, recital 10; Lukas Feiler, Nikolaus Forgó and Michaela Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business 2018) 30.
[14] GDPR, art 8.
[15] GDPR, arts 9(2)(b), 88(1).
[16] GDPR, art 85.
[17] See Valentina Pavel, 'European Commission Urged to Investigate Romanian GDPR Implementation' (*GDPR Today*, 3 July 2017) <www.gdprtoday.org/european-commission-urged-to-investigate-romanian-gdpr-implementation/> accessed 11 June 2019.

aims to ensure transparent and equivalent data protection and free movement of personal data within the EU.[18]

On the other hand, in the context of diverging national regimes, there is also one additional issue which needs to be addressed. Namely - the seemingly unintended omission of the GDPR - the lack of general conflict of laws rule. It is unclear whether this is a result of the initial intention of the Member States to fully harmonise the data protection regime within the EU, hence waiving the need for such guidance. However, considering the significant number of opening clauses allowing national legislators to further specify the GDPR requirements, it is surprising that the conflict of laws rules under the previous Directive were completely removed and no substitute guidance has been provided.[19] Under these circumstances, the lack of full harmonisation combined with the lack of clear rules on applicable law could pose quite a few practical challenges, to say the least.

Considering the above, the purpose of this thesis is two answer two main questions. First, whether the amount of the opening clauses in the GDPR indeed undermines its purpose to establish a uniform data protection regime in the Union. Second, given the expected differences in national law due to the opening clauses, how could an eventual conflict of laws issue be resolved?

In order to answer these questions, Section II of this thesis will provide an overview of all opening clauses and will examine in detail some of the most practically relevant opening clauses in the GDPR and potential issues arising therefrom. Section III will focus on a comparative review of the approaches of five Member States (Germany, Austria, Bulgaria, Ireland, and Denmark) as regards implementation of opening clauses in their national legislation. The purpose of the review will be to evaluate whether Member States make use of the provided opportunity to enact

[18] GDPR, recital 30.
[19] Feiler, Forgó and Weigl (n 13) 30.

legislation within the delegated competence, and thereby creating diverging data protection law within the Union. Section IV will elaborate on the lack of general conflict of laws guidance and analyse possible solutions to finding the applicable law.

II. Opening Clauses

1. Background

The Directive preceding the GDPR was adopted in a time period when cross-border transfer of data and especially digital international data flows were likely to be isolated cases. The Member States' national data protection laws varied considerably, if such had been enacted at all.[20] Therefore, the first step to an EU-wide convergence of the rules on processing of personal data was the adoption of the Directive.

Nonetheless, within a period of twenty years, in a context of rapid technological developments, where cross-border flows of personal data are becoming ever more crucial for effective business relations, the Directive turned out to be insufficient in its attempt to approximate data protection laws. The main problems stemmed from the nature of the Directive as a legal instrument which imposed a certain minimum standard of protection, and then had to be implemented through separate intermediary acts in the national legislation. On the one hand, certain Member States used the opportunity to enact data protection national laws which were more stringent and made use of less exceptions. On the other hand, others would opt for a laxer approach and make use of most of the exceptions allowed under the Directive (e.g., not to appoint a DPO). To make cross-border relations further complicated, the intermediary national acts did not always transpose the Directive properly.[21] For instance, when implementing the Directive, some

[20] Michael L. Rustad and Sanna Kulevska, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28(2) Harvard Journal of Law & Technology 349, 359.
[21] Chen (n 10) 315.

Member States incorrectly extended the scope of application of their national data protection rules.[22] It was to this background that the European Commission initiated the personal data protection reform in 2012.[23]

Given the considerably altered current context in an expanded European Union, the importance of having unified rules for processing of personal data has become crucial for the proper functioning of the internal market. Therefore, one of the main aims for the adoption of the GDPR was to achieve a harmonised EU data protection framework, i.e. 'one single set of rules for citizens and businesses'.[24] Such framework would not only provide an equivalent fundamental right to protection of personal data, but would also facilitate frequent cross-border transfers and level the field for companies active in the EU. The prospect of achieving full harmonisation seemed promising, as the old regime under the Directive, consisting of 28 different national data protection laws, was replaced by the new Regulation. In turn, this meant direct applicability of one single piece of legislation, effective in all Member States which should eliminate the differences in the implementation and application of data protection rules.

2. What are opening clauses and why are there such in the GDPR?

On a number of issues during the legislative process, the Member States could not reach a political agreement as regards what level of protection the Regulation should require.[25] Apparently, in the end they agreed to disagree, and instead left these issues as opening clauses.

[22] See Chen (n 10) 315: 'It follows that, for example, if a company established in Italy and Portugal processes personal data in its Portuguese establishment in a context of that establishment's activities, then the Italian Code would still apply according to its Section 5(1), which differs from what the Directive mandates.'
[23] European Commission, 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses' (Press Release, 25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> accessed 10 June 2019.
[24] European Commission, 'Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018' (Communication) COM (2018) 43 final.
[25] DLA Piper, 'EU General Data Protection Regulation - Background' (*DLA Piper*) <www.dlapiper.com/en/austria/focus/eu-data-protection-regulation/background/> accessed 11 June 2019.

Thus, each national legislator is allowed room for manoeuvre to enact its own rules within the opening clauses, i.e. within the scope of the delegated competence.

On the one hand, when considering the usual domestic particularities of certain areas, such as national labour laws, for instance, it could be understood why Member States would prefer more flexibility. On the other hand, it is rather astounding that no consensus could be reached as regards the age of digital consent.[26] It seems far more sensible to have the same solution on such a common matter with inevitable practical implications rather than leaving each Member State to set its own rules. Nevertheless, such agreement was not reached and now most national legislators have used the option to set a different age of online consent.[27]

Considering also the significant number of opening clauses within the Regulation, it could be argued that it did not achieve full harmonisation of data protection law within the EU and its above outlined aims are in a way undermined.

3. Challenges posed by the opening clauses

Diverging national regimes inevitably lead to fragmentation of data protection laws and legal uncertainty. One of the negative implications arising therefrom is lack of predictability as regards the exact rights and obligations of the key stakeholders within a cross-border personal data transfer. In practice, for controllers and processors this means, inter alia, additional burden in terms of time and costs for identifying and applying the relevant foreign national provisions. Companies should in any case diligently examine whether or not the national rules of a particular Member State further specify or preclude GDPR's provisions.[28] This situation is further exacerbated by the

[26] GDPR, art 8.
[27] Olivia Tambou, 'Opening Remarks to the E-Conference on the National Adaptations of the GDPR' (*Blogdroiteuropéen*, 4 June 2018) <https://blogdroiteuropeen.com/2018/06/04/opening-remarks-to-the-e-conference-on-the-national-adaptations-of-the-gdpr-by-olivia-tambou/> accessed 11 June 2019.
[28] Paul Voigt and Axel Von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer International Publishing AG 2017) 223.

inconveniences caused by the lack of conflict of laws rules which will be addressed in Section IV of this thesis.

Another downside is inconsistency regarding enforceable rights which might have negative effects especially on data subjects. Particularly detrimental implications might have differentiating rules as regards exceptions to data subjects' rights,[29] processing and freedom of expression and information,[30] representation of data subjects by not-for-profit organisations,[31] etc. Ultimately, diverging national data protection regimes constitute an impediment to efficient free flow of personal data and business relations within the EU.

4. Different types of opening clauses

To begin with, for the purposes of illustrating the scope of the issue regarding the numerous occasions on which the GDPR allows Member States to further legislate, this thesis would enumerate all 69 provisions with opening clauses, exhaustively indicated by Dr. Lukas Feiler:[32]

	Article of the GDPR	Main subject	Text of the opening clause
Chapter I General provisions			
1.	Article 4(7)	Defining a controller	'(…) [W]here the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.'

[29] GDPR, arts 14(5)(c)-(d), 17(1)(e), 17(3)(b)-(c), 22(2)(b), 23(1).
[30] GDPR, art 85.
[31] GDPR, art 80.
[32] The following table is based on Lukas Feiler, 'Öffnungsklauseln in der Datenschutz-Grundverordnung - Regelungsspielraum des österreichischen Gesetzgebers' (2016) 5 jusIT <https://lesen.lexisnexis.at/_/oeffnungsklauseln-in-der-datenschutz-grundverordnung-regelungssp/artikel/jusit/2016/5/jusIT_2016_05_093.html> accessed 15 June 2019.

2.	Article 4(9)	Public authorities which receive personal data	'However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients (…) .'
Chapter II Principles			
3.	Article 6(1)(c) in conjunction with (2)	Processing for compliance with a legal obligation	'Processing shall be lawful only if and to the extent that at least one of the following applies: (c) processing is necessary for compliance with a legal obligation to which the controller is subject;' 'Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) (…) of paragraph 1 (…) .'
4.	Article 6(1)(e) in conjunction with (2)	Processing for compliance with a task carried out in the public interest or in the exercise of official authority	'Processing shall be lawful only if and to the extent that at least one of the following applies: (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;' 'Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 (…) .'
5.	Article 6(4)	Processing for a purpose other than that for which the personal data have been collected	'Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law (…) .'

6.	Article 8	Child's consent in relation to information society services	'Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.'
7.	Article 9(2)(a)	Restrictions for providing consent for processing of special categories of personal data	'Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;'
8.	Article 9(2)(b)	Processing in the field of employment and social security and social protection law	'Paragraph 1 shall not apply if one of the following applies: (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;'
9.	Article 9(2)(g)	Processing based on substantial public interest	'Paragraph 1 shall not apply if one of the following applies: (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law (…) ;'
10.	Article 9(2)(h) in conjunction with (3)	Processing for the purposes of health care or occupational medicine	'Paragraph 1 shall not apply if one of the following applies: (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law (…) ;'

11.	Article 9(2)(i)	Processing for the purposes of public health	'Paragraph 1 shall not apply if one of the following applies: (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law (…) ;'
12.	Article 9(2)(j)	Processing for the purposes of archiving, scientific or historical research or statistics	'Paragraph 1 shall not apply if one of the following applies: (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law (…) ;'
13.	Article 9(4)	Conditions and restrictions for processing of genetic, biometric and health data	'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.'
14.	Article 10	Processing personal data relating to criminal convictions and offences	'Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law (…) .'
Chapter III Right of the data subject			
15.	Article 14(5)(c)	Derogations from the information right of the data subject	'Paragraphs 1 to 4 shall not apply where and insofar as: (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject (…);'

16.	Article 14(5)(d)	Derogations from the information right of the data subject	'Paragraphs 1 to 4 shall not apply where and insofar as: (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.'
17.	Article 17(1)(e)	Erasure for compliance with a legal obligation	'[T]he personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;'
18.	Article 17(3)(b)	Derogations from the right to erasure	'Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;'
19.	Article 22(2)(b)	Authorising automated individual decision-making, including profiling	'Paragraph 1 shall not apply if the decision: (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;'
20.	Article 23	Restrictions of the data subjects' rights	'Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 (…) .'
Chapter IV Controller and processor			
21.	Article 26(1)	Responsibilities of join controllers	'They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation (…) by means of an arrangement between them unless, and in so far as, the respective responsibilities of the

			controllers are determined by Union or Member State law to which the controllers are subject.'
22.	Article 28(3)	Processing by a processor governed by a legal act	'Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to (…) .'
23.	Article 28(3)(a)	Processing by a processor based on a legal requirement	'[P]rocesses the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject (…);'
24.	Article 28(3)(a)	Legal prohibition for the processor to inform the controller of the legal requirement	'(…) [I]n such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;'
25.	Article 28(3)(g)	Legal storage requirement for processors	'[A]t the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;'
26.	Article 28(4)	Processing by a sub-processor governed by a legal act	'Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other

			processor by way of a contract or other legal act under Union or Member State law (…).'
27.	Article 29 and Article 32(4)	Derogation of processor's obligation to process data only on controller's instructions	'The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.' 'The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'
28.	Article 35(10)	Derogation from the requirement to carry out impact assessment	'Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.'
29.	Article 36(5)	Legal requirement for consulting the supervisory authority	'(…) Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.'
30.	Article 37(4)	Additional cases where assignment	'(…) [T]he controller or processor or associations and other bodies representing categories of controllers or processors may

		of a DPO is obligatory	or, where required by Union or Member State law shall, designate a data protection officer.'
31.	Article 43(1)	Accredited certification bodies	'Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:'
Chapter V Transfers of personal data to third countries or international organisations			
32.	Article 49 (1)(d) in conjunction with (4)	Transferring personal data in a third country based on a public interest	'The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.'
33.	Article 49(1)(g)	Transferring personal data in a third country from a register intended to provide public information	'[T]he transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.'
34.	Article 49(5)	Legal limitations to transferring specific categories	'In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation.'

		of personal data in a third country	
Chapter VI Independent supervisory authorities			
35.	Article 51(3) in conjunction with Article 68(4)	Rules when there is more than one supervisory authority in a Member State	'Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.'
36.	Article 52(4)	Ensuring that the supervisory authority is provided the necessary resources	'Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.'
37.	Article 52(5)	Ensuring that the supervisory authority chooses its own staff	'Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.'
38.	Article 52(6)	Ensuring that the supervisory authority is subject to financial control	'Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.'
39.	Article 54(1)(a) in junction with Article 51(1)	Establishing a supervisory authority for monitoring and	'Each Member State shall provide by law for all of the following: (a) the establishment of each supervisory authority'. 'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the

		application of the Regulation	application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').'
40.	Article 54(1)(b) in conjunction with Article 53(2)	Providing the qualifications and eligibility conditions for members of the supervisory authority	'Each Member State shall provide by law for all of the following: (b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;' 'Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.'
41.	Article 54(1)(c) in conjunction with Article 53(1)	Providing the procedure for appointing members of the supervisory authority	'Each Member State shall provide by law for all of the following: (c) the rules and procedures for the appointment of the member or members of each supervisory authority;' 'Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by: (…).'
42.	Article 54(1)(d) in conjunction with Article 53(3)	Providing the duration of the term of the members of the supervisory authority	'Each Member State shall provide by law for all of the following: (d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, (...);' 'The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.'
43.	Article 54(1)(e)	Providing whether members of the supervisory	'Each Member State shall provide by law for all of the following: (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment.'

		authority can be reappointed	
44.	Article 54(1)(f) in conjunction Article 52(3), Article 53(3) and (4)	Providing the obligations and other employment conditions of the members of the supervisory authority	'Each Member State shall provide by law for all of the following: (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.' 'Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.' 'The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.' 'A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.'
45.	Article 54(2)	Duty of professional secrecy of the member of the supervisory authority	'The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers.'
46.	Article 55(3) in conjunction with recital 20	Entrusting the supervision of data processing operations of	'Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.' 'It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial

		courts to specific bodies	system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.'
47.	Article 57(1)(c)	Advisory functions of the supervisory authority vis-à-vis the national parliament and other institutions	'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;'
48.	Article 58(1)(f)	Providing conditions for obtaining access to premises of the controller and the processor	'Each supervisory authority shall have all of the following investigative powers: (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.'
49.	Article 58(3)(b)	Opinions of the supervisory authority to other institutions and the public	'Each supervisory authority shall have all of the following authorisation and advisory powers: (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;'
50.	Article 58(4)	Providing judicial remedy and due process against the	'The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process,

		supervisory authority	set out in Union and Member State law in accordance with the Charter.'
51.	Article 58(5)	Providing powers to the supervisory authority to bring infringements before the judicial authorities	'Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.'
52.	Article 58(6)	Providing additional powers to the supervisory authorities	'Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.'
53.	Article 59	Determining other authorities which receive the annual activity report of the supervisory authority	'Each supervisory authority shall draw up an annual report on its activities (…). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law.'
Chapter VII Cooperation and consistency			
54.	Article 62(3)	Rules for conferring powers on other Member State's supervisory authorities	'A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, (…).'
55.	Article 62(3)	Permitting other Member State's supervisory	'A supervisory authority may (…) in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to

		authorities to exercise investigative powers pursuant to that other Member State's law	exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority.'
Chapter VIII Remedies, liability and penalties			
56.	Article 80(2)	Providing the NPOs right to lodge complaint independently of a data subject's mandate	'Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.'
57.	Article 83(7)	Rules on whether administrative fines could be imposed on public authorities	'(…) [E]ach Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.'
58.	Article 83(8)	Providing effective judicial remedy and due process for imposing administrative fines	'The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.'

59.	Article 83(9)	Providing equivalent legal remedies where the Member State's legal system does not provide for administrative fines	'Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities.'
60.	Article 84	Providing penalties for infringements which are not sanctioned pursuant to Article 83	'Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented.'
Chapter IX Provisions relating to specific processing situations			
61.	Article 85(1)	Reconciling the right to personal data protection with the right to freedom of expression and information	'Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.'
62.	Article 85(2)	Processing for journalistic, academic, artistic	'For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from (…) if

		or literary purposes	they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.'
63.	Article 86	Processing and public access to official documents	'Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.'
64.	Article 87	Processing of the national identification number	'Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application.'
65.	Article 88	Processing in the context of employment	'Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context (…) .'
66.	Article 89(2)	Derogations when processing for scientific or historical research purposes or statistical purposes	'Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 (…) .'
67.	Article 89(3)	Derogations when processing for archiving purposes	'Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 (…) .'

		in the public interest	
68.	Article 90(1)	Regulation of the exercise of the powers of the supervisory authority vis-à-vis professional secrecy holders	'Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy (…) where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy.'
69.	Article 91(2)	Setting up an independent supervisory authority for churches and religious associations	'Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.'

As evidenced by the table above, the GDPR's opening clauses not only are numerous, but they also differ from each other in their characteristics. For instance, they differ in how much margin for manoeuvre they afford to Member States, as well as in their potential impact to cross-border processing of personal data.

First, as regards the margin for manoeuvre, the EU legislator's approach regarding the delegated competences is not the same for each provision. Depending on the specific provision, the opening clause may allow national legislator either to: 1) further specify, 2) supplement, or 3) replace provisions of the GDPR.[33] National legislators should carefully consider these

[33] Voigt and von dem Bussche (n 28) 222.

particularities when making use of the opening clauses. Incorrect implementation may not only lead to exceeding the delegated competence, but also to contradictions with other provisions and fundamental principles of the GDPR.

Second, as regards their impact, the opening clauses differ in their potential to cause conflict between different Member States' laws and thus become an obstacle to the free flow of data within the Union. On the one hand, provisions which are of predominantly national significance are less likely to cause inconveniences and legal uncertainty for companies, especially the ones operating cross-border. For instance, the opening clauses in Chapter VI and Chapter VII of the GDPR regarding the establishing, powers, staff, and other procedural requirements concerning the supervisory authorities could not reasonably be expected to be problematic in that regard. The same is true for most of the opening clauses in Chapter IX of the GDPR which governs the remedies, liability, and penalties.

In contrast, there are many opening clauses which would be very relevant in the day-to-day business activities of companies, in particular as regards the ones which operate in different Member States. Inconsistencies in the GDPR implementing acts is a matter of which such businesses should be particularly aware. Simply put, this means that companies should know these differences and adapt their processing operations to the respective national peculiarities, if and to the extent necessary. Such provisions which could be considered particularly important for the daily business activities from a practical standpoint are, for instance, most of the opening clauses in Chapter II, Chapter III, Chapter IV, and Chapter IX governing the principles, rights of the data subjects, controllers and processors, and specific processing situations, respectively. For example, a provision which has already caused quite a lot of questions for cross-border processing is the opening clause under Article 8(1) of the GDPR which allows Member States to determine different

age thresholds for children's digital consent. Provisions like that would definitely pose compliance issues for companies. Therefore, the first step to avoiding GDPR infringements is awareness regarding the important areas with opening clauses which are likely to come up in practice.

Taking into account the above distinction, in the following paragraphs of Section II.4, this thesis will analyse certain opening clauses, which are more relevant from a practical perspective for the day-to-day business activities of controllers and processors in the private sector, and their potential impact on cross-border relations, without aiming to exhaustively examine all of the opening clauses in the GDPR.

4.1. Lawfulness of processing

Member States may enact legislation which further specifies the grounds to process personal data in order to comply with a legal obligation, for performing a task in the public interest or when exercising the official authority of the controller.[34] The rationale of this opening clause is that Member States should be given the autonomy to maintain or adapt their national laws which require processing of personal data.

However, the broad wording of this opening clause could have cross-border implications, some of which problematic. For example, controllers would have different sources of legal obligations and thus diverging grounds to collect personal data. This may not be of major concern as regards typical legal obligations which are expected to be found in each Member State, such as accounting and auditing duties. At the same time, this might have some unintended effects. For instance, due to the lack of further clarification regarding the 'legal obligation' of the controller, Member States might simply decide to create any obligation as they wish[35] or to maintain long

[34] GDPR, art 6, recital 10.
[35] European Digital Rights, 'Proceed With Caution: Flexibilities in the General Data Protection Regulation' (*EDRi*, 5 July 2016) 6 <https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf> accessed 11 June 2019.

outdated rules which do not take into account the data minimisation principle. In order to ensure transparency and avoid implementing conflicting legislation, the international non-profit association EDRi suggested that Member States be required to publish the relevant legal obligations and to inform the Commission and the European Data Protection Board (hereinafter EDPB or Board).[36]

4.2. Child's consent in relation to information society services

As simple as this looks at first, apparently it was not within the realm of possible for EU countries to agree on the appropriate age of consent for processing of personal data in the Internet. As a result, Article 8(1) of the GDPR lays down only the minimum standard of 16 years of age and then allows national legislators to lower it to no less than 13 years.

This provision has already caused a lot of questions regarding its practical implementation in the online world. Given the lack of territoriality in the internet, it is not clear how a controller is supposed to observe these different age thresholds. For instance, a controller, situated in a Member State which has set the age of digital consent on 14 years, may provide information services (e.g., opening of an e-mail account) to a data subject in another Member State where the age is set at 16 years. In this case, how could controllers ensure that they are obtaining a valid consent by customers from different Member States? One solution may be to collect additional information in order to determine the applicable age threshold for the data subject. Setting aside the additional burden for businesses, in this situation it could be argued that collecting such information may be contrary to the data minimisation principle. This particular case is additionally exacerbated by the lack of guidance as to which would actually be the applicable law in such a conflict of laws situation (elaborated further in Section IV).

[36] Ibid 7.

In practice, the preferred solution by most online service providers is to set an age of digital consent at 16 years in order to avoid obtaining consent which may turn out to be invalid. While this may be a reasonable solution from a business perspective, it might unjustifiably restrict data subjects, who are below 16 years but above the age threshold applicable for them, from exercising their rights. This result is contrary to the objective of the GDPR to provide consistent level of data protection and to facilitate free flow of personal data.

4.3. Processing of special categories of personal data

Firstly, Article 9(2)(a) of the GDPR allows Member States to further restrict the possibilities for processing of special categories of personal data. They are allowed to enact legislation which prohibits collection of sensitive data, regardless of whether the data subject has consented to it or not. Thus, even if data subjects have provided their explicit consent, it would not be a valid ground for processing of sensitive data, and hence a personal data infringement.

Secondly, Article 9(2)(b) of the GDPR allows for derogations from the general prohibition for processing sensitive data for employment and social security purposes. Such deviations require suitable safeguards and balancing against the fundamental rights of the data subjects in order to be enacted.[37] This is one of the key opening clauses from a practical standpoint. It could be reasonably be assumed that most Member States would make use of it, as it enables national legislators to reconcile their domestic labour law particularities with EU data protection rules. For instance, even before the GDPR some national legislators would prohibit collecting data for religious beliefs, whereas others would require its collection for certain purposes.[38]

[37] GDPR, recital 52.
[38] European Digital Rights (n 35) 10.

Both of the provisions described above should not be expected to cause inconveniences, as they would usually concern processing of personal data in a solely domestic context.[39] However, this may not be the case for multinational companies which operate in more than one country within the EU.[40] For instance, an HR intragroup transfer of databases with employees' personal data might turn out to be quite challenging. In such a case, companies have to consider the differences in each national legislation, as it may turn out that an HR department in one MS is not permitted to process certain sensitive data which, however, is lawfully processed by an HR department in another MS.

4.4. Processing of genetic data, biometric data or data concerning health

Another opening clause with potentially considerable practical implications is the possibility to introduce additional conditions and limitations regarding genetic data, biometric data or data concerning health.[41] It is, admittedly, reasonable to provide a margin of manoeuvre when processing these types of data.

It should be noted, however, that there are certain areas where diverging national legislation may per se be fairly problematic. To that point, genetic research usually presupposes transnational cooperation and processing of personal data.[42] This is due to the fact that meaningful scientific results require substantial international amounts of data.[43] Accordingly, the research might be conducted in one country, whereas the data might be collected in others.[44] In this regard the GDPR expressly states that implementing legislation should 'not hamper the free flow of personal data'.[45]

[39] Ibid.
[40] Ibid.
[41] GDPR, art 9(4).
[42] Kart Pormeister, 'Genetic Research and Applicable Law: The Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-Border Genetic Research' (2018) 5(3) Journal of Law and the Biosciences 706, 708.
[43] Ibid.
[44] Ibid.
[45] GDPR, recital 53.

It is therefore crucial to consider the national particularities and potential conflict of laws issues which may arise in such cross-border scientific research.

4.5. Processing of personal data relating to criminal convictions and offences

The rules on processing of personal data relating to criminal convictions and offences or related security measures are separated from the rules on special categories of data and are laid down in Article 10 of the GDPR. The approach of the Regulation is to prohibit the processing of such data, except in the following two cases: 1) it is conducted under the control of an official authority, or 2) it is explicitly authorised by EU or national law.[46] It is somewhat peculiar that the legal text does not provide any uniform EU-wide applicable general cases, making diverging national legislation inevitable. This approach may also have undesired outcomes, especially if a Member State has intendedly or not failed to lay down rules authorising the processing of such data. For instance, an employer may not be able to initiate its own internal investigation regarding potential fraud incident by an employee.[47] This would be the case if the relevant national legislation does not explicitly authorise processing of personal data relating to criminal convictions and offences in such a context, and therefore such data could be processed only under the control of official authority.[48] Therefore, differences and potential shortfalls of national legislations should be expected.

4.6. Exceptions to the right to information where personal data have not been obtained from the data subject

One of the cornerstones of data subjects' rights is the right to be informed of the existence of the processing operation, its purposes and other information necessary to ensure fair and

[46] GDPR, art 10.
[47] Feiler, Forgó and Weigl (n 13) 196.
[48] Ibid.

transparent processing. In practice, this is usually done via a privacy notice which provides the information required by the Regulation. The proper exercise of this right to information is a crucial basis of the fundamental right of personal data protection. Any limitations and exceptions to this right should be very cautiously implemented.

Noteworthy examples for derogations of the right to information are stipulated in Article 14(5) of the GDPR. The exceptions provided therein are applicable where controllers have not collected the personal data directly by the data subjects, but from another source. The result of these exceptions is that, subject to the specified conditions, the data subject's right to information does not apply. While Article 14(5)(a) is quite straightforward, the rest of the clauses are more complex. Potentially problematic are the provisions under Article 14(5)(c) and 14(5)(d). The first exempts controllers when the obtaining or disclosure of the information is explicitly required by EU or national law. The second lifts the information duty when the personal data are supposed to remain confidential due to a professional or statutory secrecy obligation.

The broad wording of these provisions conceivably allows national legislators to provide unjustifiably far-reaching exceptions to an essential right of data subjects, ultimately keeping them in the dark as to who and for what purposes is processing their personal data.[49] It is therefore essential for Member States to take into account that such derogations must be implemented narrowly as a general rule.[50]

4.7. Restrictions to data subjects' rights

Under Article 23 of the GDPR, data subjects' rights could be restricted by Union or national law. Such measures could be implemented for the purposes specified in the provision which

[49] European Digital Rights (n 35) 16.
[50] Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/679' (29 November 2017 revised on 11 April 2018) WP 260, 28 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025> accessed 11 June 2019.

include, inter alia, national security, defence, prosecution of criminal offences, general public interest, protection of the data subject or the freedoms of others, breaches of ethics for regulated professions, enforcement of civil laws claims, etc. Although this legal text does not differ considerably from the Directive,[51] the concerns for the broad formulation of the delegated competencies, commented in Section II.4.6 above, are even more relevant here.

Nevertheless, it is should be noted that Article 23(1) of the GDPR explicitly requires that any implemented national restriction is balanced against the fundamental rights of the concerned individuals and is necessary and proportionate. Any restrictions should be narrowly applied and in compliance with the additional specific requirements under Article 23(2) of the GDPR.

Misuse of the broad discretion provided to Member States may lead to various undesired implications.[52] For instance, considerable discrepancies in the data subjects' rights in different Member States would be contrary to the aim of creating equivalent level of data protection within the EU. Another potential undesired consequence would be if a national law turns out to be exceeding the delegated competence and is therefore cancelled by the Court of Justice of the European Union (hereinafter CJEU).[53]

4.8. Designation of the data protection officer

One the most discussed novelties of the GDPR was the introduction of the data protection officer (DPO) as a mandatory requirement. Article 37(1) of the GDPR provides the three EU-wide applicable cases where appointment of a DPO is imperative.

[51] Directive, art 13(1).
[52] European Digital Rights (n 35) 21.
[53] Ibid.

As evidenced by the ambiguous wording of two of the mandatory cases[54] and by the opening clause,[55] which allows national legislators to lay down further mandatory cases, the Member States did not quite agree on this matter. To some extent this is due to the differences in data protection standards within the EU which existed during the previous regime under the Directive. As with other privacy law matters, some countries had a laxer approach, whereas others had already implemented a standard which was very close to or even stricter than the requirements of the Regulation. For instance, German companies long before the entry into force of the GDPR have been required to assign a DPO if they have at least 10 employees processing personal data which involves IT systems.[56] Considering the three cases where the GDPR provides for mandatory appointment,[57] it is clear why Germany might have insisted for additional requirements, or at least for an opening clause. Even though vague, the GDPR requirements could still be reasonably assumed to require a significantly higher threshold triggering the obligation to appoint a DPO.

Albeit quite discussed, the opening clause under Article 37(4) of the GDPR does not have the potential to hinder cross-border relations. The risk is even further mitigated by the possibility to voluntary appoint a DPO[58] or to assign one single DPO within a group of companies.[59] These options seem to be preferred by some international companies in their attempt to ensure compliance with the GDPR, in particular when due to the broad wording[60] companies are not certain if they must appoint a DPO for their business units within different Member States.

[54] GDPR, arts 37(1)(b)-(c).
[55] GDPR, art 37(4).
[56] Axel Spies, 'Germany Enacts GDPR Implementation Law' (*Lexology*, 6 June 2018) <www.lexology.com/library/detail.aspx?g=5f6cf3a2-56de-4484-beba-d6b20047e452> accessed 11 June 2019.
[57] GDPR, art 37(1).
[58] GDPR, art 37(4).
[59] GDPR, art 37(2).
[60] GDPR, arts 37(1)(b)-(c).

4.9. Representation of data subjects by NGOs

An interesting option for the data subjects is provided for in Article 80 the GDPR. The first paragraph of this article allows individuals to mandate an NGO to lodge a complaint on their behalf. More specifically, a data subject can mandate: 1) the right to lodge a complaint with a supervisory authority, 2) the right to appeal the acts of a supervisory authority before a court, 3) the right to sue a controller or a processor in a court, and 4) the right to receive compensation for damages.

The second paragraph provides another option for NGOs - to lodge complaints *independently* if they consider that data subjects' rights have been infringed by processing which non-compliant with the GDPR. Practically, this means that non-for-profit organisations could exercise the data subject's rights even without being authorised. Nevertheless, the rights which NGOs can exercise on their own initiative are narrowed down. They are only entitled to the first three enumerated rights, and not to claim damages on behalf of the data subject.

However, both of the above mentioned options could be exercised only and to such extent as provided for by Member State law. Therefore, whether or not NGOs are able to represent data subjects with the rights accorded in Article 80(1) and (2) of the GDPR, would depend entirely on domestic law. Leaving full discretion to Member State as to the existence of these rights is unsettling. It will again inevitably leave to inconsistent level of data protection in the EU, in particular as regards enforcement.[61] While some data subjects would be afforded the full range of rights to be represented by NGOs, others would not be, and this will be entirely dependent on the particularities of their national law.

[61] European Digital Rights (n 35) 49.

4.10. Supervisory powers and imposing administrative fines

Another vastly discussed matter in the new regime are the administrative fines. Setting the maximum threshold at 20 000 000 EUR or 4 % of last year's total global annual turnover of the entire group of undertakings (whichever is higher), the European Union makes a statement that it takes personal data protection very seriously.[62]

The GDPR has left it to the national supervisory authorities to determine the exact amount of the fines within this broad range. However, it is not entirely at their discretion, as authorities have to take into account the criteria laid down in the GDPR.[63] These criteria could be divided into two categories – one general and a number of specific criteria.

The first one requires that the imposed fine is 'effective', 'proportionate' and 'dissuasive'.[64] Depending on the specific circumstances, a fine may not even be imposed at all. Instead, the national authorities could decide to impose a corrective measure such as warning, ordering compliance with a data subject's request, ordering suspension of data flows to a third country, and others.[65] There are also the options to impose only a fine or to cumulatively impose a fine and corrective measures.

The second category of criteria are more specific and detailed. According to the Article 83(2) of the GDPR, the national authorities must take into account various circumstances concerning the infringement, inter alia, the following: 1) the nature, gravity and duration, 2) whether it was intentional or negligent, 3) mitigating actions undertaken to limit the damage caused to data subjects, 4) degree of cooperation with the authority, 5) categories of affected personal data, and others. As evidenced by the extensive enumeration of criteria, the Regulation tries to provide

[62] GDPR, arts 83(5)-(6).
[63] GDPR, arts 83(1)-(2).
[64] GDPR, art 83(1).
[65] GDPR, arts 58(2)(a)-(h), (j).

sufficient guidance to the national authorities to be able to determine the appropriate fine and/or corrective measures. Even though the criteria for this determination are not subject to an opening clause, they could still be perceived as providing broad discretion to Member States, in particular to the national supervisory authorities.

Considering also the lack of minimum threshold for administrative fines, national supervisory bodies are given enough room for judgement and could be flexible when assessing the specific circumstances of the case. Such an approach should be seen as rather positive, as it should contribute to avoiding unnecessary harsh and disproportionate sanctions. Of course, this would hold true only if the freedom of discretion is not abused in practice (e.g., by imposing disproportionately low or high fines within the broad range set by the GDPR).

Nevertheless, the Regulation leaves one particular issue entirely open for the Member States. Namely, the delegated competence to decide whether or not their national public authorities could be imposed administrative fines, and if yes – to what extent.[66] Therefore, some countries could decide to exempt all of their public authorities (e.g., municipalities, universities, etc.) from administrative fines for data protection infringements. As an opening clause, this potential derogation seems in the less problematic category. However, eliminating sanctions for the public sector should be well thought out as it may have negative implications, especially if it is misused and leads to lower data protection standards for the public sector. Still, insofar as this matter has mostly domestic dimensions, it should not be causing cross-border inconveniences.

4.11. Processing and freedom of expression and information

Member States are allowed to deviate from the Regulation's rules in order to balance the competing fundamental rights – personal data protection and freedom of expression and

[66] GDPR, art 83(7).

information (including processing for journalistic purposes and the purposes of academic, artistic or literary expression).[67] If considered necessary for this purpose, national legislators could exclude the application of almost all GDPR provisions.[68]

A noteworthy exemption is the opening clause regarding the rights of the data subject. For instance, derogations from the rights to information and access to personal data[69] and the right to be forgotten[70] would be essential, in particular, for journalistic purposes. Personal data protection should not hinder informative and objective quality media. To reduce to the absurd, if an investigative journalist is not exempted from obligations, such as to provide privacy notices and to erase personal data, of course, we cannot talk about freedom of expression and information whatsoever.

The freedom of expression is an essential element of every democratic society. Member States are, therefore, allowed a very broad discretion whether and to what extent to apply the rules of the GDPR. At the same time, national legislators should strike a balance between the competing rights, and not give preference to one or the other. In that endeavour, national legislators should give regard to recital 153 of the GDPR. Journalism, in particular, should remain informative and capable of serving the public interest, while the right to personal data protection should not be undermined or abused by unnecessary exceptions.

In an exceptional case of reference to applicable law, recital 153 of the GDPR also clarifies that whenever derogations differ '(…) the law of the Member State to which the controller is subject should apply'. Even though useful, this guidance raises some questions. For instance, what if a publication in a Member State with a laxer approach to invading the privacy of celebrities is

[67] GDPR, art 85(1).
[68] GDPR, art 85(2).
[69] GDPR, art 13-15.
[70] GDPR, art 17.

published in an online website directed to other Member States with more stringent rules, or if these celebrities are residents of the latter state?[71] The indication of applicable law is rather insufficient, especially in an online environment.[72] In order to avoid serious conflicts of laws, guidelines by the EDPB on the application of this provision would be necessary.[73]

4.12. Processing of the national identification number

Under Article 87 of the GDPR the Member States are allowed to specify the requirements for processing of national identification numbers or other identifiers which are generally applicable. If they choose to make use of this option, Member States must give regard to the rights and freedoms of individuals, by ensuring that processing of such identifiers is conducted only under appropriate safeguards. While this provision is clear and straightforward, it should be bore in mind, especially in cross-border data flows, that national particularities might apply.

4.13. Processing in the context of employment

For the most part, employment laws are outside the scope of EU's law-making competence.[74] It is therefore rational that Member States are allowed to strike their own balance between competing rights under domestic labour law and personal data protection.[75]

In addition to Article 9(2)(b) of the GDPR (commented in Section II.4.3 above) regulating special categories of employees' personal data, Article 88 of the GDPR also contains an opening clause concerning employment law. It provides a comprehensive discretion to '(…) provide for

[71] European Digital Rights (n 35) 51.
[72] Ibid.
[73] Ibid.
[74] Detlev Gabel and Tim Hickman, 'Chapter 17: Issues Subject to National Law – Unlocking the EU General Data Protection Regulation' (*White & Case LLP*, 5 April 2019) <www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection> accessed 11 June 2019.
[75] Ibid.

more specific rules to ensure the **protection** of the rights and freedoms in respect of the processing **of employees' personal data** in the employment context (…)'.[76]

Further, the GDPR lists in a non-exhaustive way the purposes for which Member States are allowed to deviate. For instance, national legislation may provide for more specific rules on recruitment, the performance and termination of an employment contract, management, planning and organisation of work, health and safety and work, and others.[77] As this is not a conclusive list, Member States can also lay down rules for purposes which are not explicitly listed in the provision.

These deviations from the GDPR could be introduced not only by law, but also by collective agreements (including 'work agreements').[78] Any provisions adopted under this opening clause should include safeguard measures which guarantee the employees' human dignity, legitimate interests and fundamental rights.[79]

Given the typical substantial differences of labour law amongst Member States,[80] the extensive use of this opening clause would be understandable and even desirable in a national context. Ultimately, it provides the necessary flexibility for countries to adapt their domestic labour framework and traditions to the new EU data protection regime.

As a result, multinational companies, in particular, have to consider the particularities of each national data protection and labour law legislation (and potential conflict of laws issues), in order to avoid fines under the GDPR.[81]

[76] GDPR, art 88(1) (emphasis added).
[77] Ibid.
[78] GDPR, art 88(1), recital 155.
[79] GDPR, art 88(2).
[80] Voigt and von dem Bussche (n 28) 224.
[81] Ibid 225.

III. Comparative analysis of different EU Member States' approaches to opening clauses

As illustrated above, the opening clauses in the GDPR are numerous and may lead to considerable divergences in Member States' data protection rules. Therefore, compliance with EU data protection law requires not only observance of the GDPR, but also identifying and adhering to national law provisions.

Many Member States have already adopted new or amended their existing legislation.[82] On the one hand, national legislators are aiming to align their existing laws with the Regulation in order to avoid conflicting rules. The diligent conduct of this endeavour would involve amending not only data protection laws, but also other laws which are closely connected with processing of personal data such as employment, social security, accounting and others.

On the other hand, many Member States are using the chance to make use of the opening clauses. Therefore, the new or amended national data protection laws usually include provisions which further specify, supplement or modify the GDPR, where the latter allows it. However, the approach of Member States regarding implementation of the opening clauses differs significantly. National legislators with long-standing data protection traditions are trying to make the most of the delegated competences in order to reconcile EU and domestic data protection law. At the same time, other countries are adopting a rather modest approach and do not make extensive use of the provided discretion.

The practical implications of the opening clauses could be better comprehended if considered in the light of the actual national implementing legislation. Therefore, Section III of this thesis will continue with a comparative review of the data protection acts of five Member State, all of which

[82] International Association of Privacy Professionals, 'EU Member State GDPR Implementation Laws and Drafts' (*IAPP*) <https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/> accessed 11 June 2019.

have adopted their different approach to the opening clauses, as follows: Germany, Austria, Bulgaria, Ireland, and Denmark.

Without aiming to be exhaustive, the review will be focused on five key areas with opening clauses: 1) processing of employees' personal data, 2) processing of special categories of personal data, 3) restrictions to data subjects' rights, 4) digital age of consent, and 5) appointment of a DPO. As all of these provisions are significant from a practical standpoint and mostly concern common business activities, companies which carry out cross-border processing should expect and be aware of the inconsistencies across Member States in the EU. Effective compliance programs would require identifying the differences and adapting personal data processing operations to the respective national peculiarities at least in these five areas, and of course – in any other relevant area for the specific case.

1. Germany

Germany has a long-established tradition in data protection law, contributing also the first formal act on data protection worldwide – the Hessian Data Protection Act from 1970.[83] The first Federal Data Protection Act was introduced seven years later in 1977.[84] During its long history, data protection law has evolved to a complex system where all sixteen of the German states have separate data protection acts and many sectorial laws supplement the legal framework.[85] Considering the complexity, adaptation to the GDPR rules seemed challenging.[86]

[83] Christian Geminn, 'The New Federal Data Protection Act – Implementation of the GDPR in Germany' (*Blogdroiteuropéen*, June 2018) 1 <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 June 2019.
[84] Ibid.
[85] Ibid 2.
[86] Ibid.

Nevertheless, the new national data protection law - the German Federal Data Protection Act[87] (hereinafter GFDPA) - was published in July 2017, well ahead of the entry into force of the GDPR.[88] A good example, not followed by the majority of the EU Member States.[89]

Although quite lengthy at first look with its 85 Articles, a considerable part of the provisions in the GFDPA actually are not concerned with the opening clauses. The German legislator has chosen to implement in its new data protection law also Directive (EU) 2016/680[90] which accounts for nearly half of the provisions (Article 45 to Article 84 of the GFDPA). Still, Germany has introduced a lot of provisions within the scope of the opening clauses.

1.1. Processing of employees' personal data

As explained in Section II.4.3 and II.4.13 above, the GDPR allows for comprehensive deviations in an employment context,[91] including exemptions from the general prohibition for processing of special categories of personal data.[92] The German legislator makes an extensive use of the discretion provided by these opening clauses.

Processing purposes

Article 26 of the GFDPA specifies the rules for collection and use of employees' personal data.[93] First, the provision provides a general permission for processing of employees' data, if

[87] Bundesdatenschutzgesetz vom 30 Juni 2017, BGBl I S 2097, available in German at <www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html> accessed 11 June 2019.
[88] Geminn (n 83) 1.
[89] International Association of Privacy Professionals (n 82).
[90] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (hereinafter Directive (EU) 2016/680).
[91] GDPR, art 88.
[92] GDPR, art 9(2)(b).
[93] Lennart Schüßler and Natallia Karniyevich, 'Germany Is the First EU Member State to Enact New Data Protection Act to Align With the GDPR' (*Bird & Bird*, July 2017) <www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr> accessed 11 June 2019.

required for hiring, carrying out or termination of the employment contract. The provision expressly mentions that collective agreements could serve as a legal ground to process HR data.[94]

The provision stipulates that employees' personal data could be processed also for the purpose of detecting criminal offences.[95] However, such processing must be based on documented factual indications which justify the suspicion that the particular employee has committed a crime, and the legitimate interests of the data subject do not outweigh such investigation.[96]

Consent

Further, the German act provides guidance on the validity of consent as a basis for processing personal data within an employment relation. Usually, the enforceability of consent in such a context is problematic due to the imbalance between the position of an employee and an employer. As a result, it is highly likely that such consent would not be considered 'freely' given and, hence, invalid. However, the GFDPA clarifies the situations where consent would be an appropriate and lawful basis for processing personal data.

Article 26(2) the GFDPA outlines two general criteria for assessing validity: 1) the employee's level of dependence, and 2) the circumstances under which consent was given. Further, the German legislator provides two inexhaustive examples where consent could be considered freely given: 1) when the employee receives a legal or economic advantage from the processing of these data, or 2) the employee and the employer are pursuing the same interests.[97] Consent must be provided in a written form, except when due to special circumstances another form would be

[94] Ibid.
[95] GFDPA, art 26(1).
[96] Ibid.
[97] GFDPA, art 26(2).

appropriate.[98] Also, the employer must inform the employee for the purposes of the processing and the right to withdraw consent in text form.

The approach of the German legislator to explicitly lay down criteria for the validity of an employee's consent should be supported as a positive step. It reduces legal uncertainty (at least within the national jurisdiction) for a matter which frequently comes up in practice.

Special categories of personal data

The German legislator implements the opening clause on special categories of personal data for employment-related purposes. Article 26(3) of the GFDPA allows employers to process sensitive data (e.g., religious beliefs, health data, trade union membership, etc.) if this is necessary to comply with labour law, social security and social protection law. Such processing is also subject to a balancing test, requiring that the employee's legitimate interest are not overriding the interest of the controller.

Categories of employees

It is also interesting to note that the GFDPA provides a broad definition of employees for the purposes the act.[99] It includes, inter alia, dependent employed workers, including temporary workers, persons undergoing rehabilitation, volunteers, persons working at home, applicants for employment, persons whose employment has been terminated, and others. The extensive definition of employees should also be positively asserted as a helpful approach to overcoming potential legal uncertainties.

[98] Ibid.
[99] GFDPA, art 26(8).

1.2. Special categories of personal data

Article 22 of the GFDPA specifies further the requirements of Article 9(2)(b), (g), (h), (i), and (j) of the GDPR on processing of special categories of personal data.[100] The provision makes a distinction between public bodies or private bodies and provides more exceptions for the processing conducted by the public sector.

Private bodies are permitted to process sensitive data, for instance, when this is necessary for preventative medicine, assessment of working capacity, medical diagnosis, on the basis of a contract with a health professional, for reasons of public interest in the area of public health, and others.[101] These exceptions would be beneficial especially for the health sector.[102]

However, companies may process these special categories of data, only if they could ensure appropriate and up-to-date measures to safeguard data subjects' interests.[103] The German legislator provides a number of standard measures which companies may adopt to fulfil this requirement. These include designation of a DPO, restriction of access, pseudonymisation, encryption, staff training, and others.[104]

1.3. Restrictions to data subjects' rights

Another highly discussed opening clause is the discretion afforded to Member States to derogate data subjects' rights. In fact, such derogations are not new to German legislation, as the previous data protection act provided for various exceptions.[105] For instance, there were numerous

[100] Baker McKenzie, 'GDPR National Legislation Survey 2018' (*Baker McKenzie*, January 2018) 16 <www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en> accessed 11 June 2019.
[101] GFDPA, art 22(1).
[102] Schüßler and Karniyevich (n 93).
[103] GFDPA, art 22(2).
[104] Ibid.
[105] Daniel Felz, 'An English-Language Primer on Germany's GDPR Implementation Statute: Part 4 of 5' (*Alston & Bird LLP*, 10 October 2017) <www.alstonprivacy.com/english-language-primer-germanys-gdpr-implementation-statute-part-4-5/?cn-reloaded=1> accessed 11 June 2019.

cases where controllers were exempted from the obligation to provide privacy notices or access to personal data.[106] Even though the new GFDPA also provides for a number of exceptions to data subjects' rights, they have a narrower scope in comparison with the previous law.[107]

Confidentiality duty

A significant exemption, preserved from the previous data protection act, derogates data subjects' rights when necessary to protect confidential information.[108] For example, controllers might be exempted from their duty to provide privacy notices in cases where personal data have not been obtained directly from the data subjects.[109] The obligation to provide access to information might also be derogated.[110] Both of these data subjects' rights would be restricted if they might lead to disclosure of confidential information, especially where a third party's overriding legitimate interest might be prejudiced.

German law lays down explicitly certain statutory confidentiality obligations, such as trade secrets and bank secrecy.[111] Thus maintaining their confidentiality would probably serve as a basis not to provide privacy notices or to refuse access to data subjects.[112]

The right of the individual to be informed for a data breach could also be restricted due to confidentiality duty.[113] Under the GDPR,[114] in a data breach that could lead to a high risk to the rights of natural persons, the controller is obliged to notify the data subjects immediately. However, similar to the right of information and the right to access, if this notification would lead to disclosure of confidential information and there are overriding third party's legitimate interests,

[106] Ibid.
[107] Ibid.
[108] GFDPA, art 29(1).
[109] GDPR, art 14.
[110] GDPR, art 15.
[111] Felz (n 105).
[112] Ibid.
[113] GFDPA, art 29(1).
[114] GDPR, art 34(1).

the controller would not be obligated to notify.[115] Unlike the previous two rights, in this case the GFDPA introduces an additional test. The exemption would not be allowed if the data subjects' interests affected by the data breach outweigh the confidentiality interest of the controller and the third parties. The main criteria for assessing whether the interest of the data subject prevails is the threat of damage.

Right of access

Another exemption maintained from the previous German data protection is laid down in Article 34(1) of the GFDPA. Thereunder, companies are exempted from their obligation to provide access to data subjects due to certain particularities of the data. First, when the data are stored only due to retention obligations. Second, the data only serves the purpose of monitoring data protection or safeguarding data. To benefit from the exemptions companies must apply measures ensuring that processing of these data for other purposes is impossible.

Right of erasure

Another interesting exemption to the individuals' rights is laid down in Article 35 of the GFDPA which restricts the right of erasure[116] for non-automated data processing. Such restriction is applicable only if it meets two cumulative criteria: 1) the deletion of the data requires disproportionate effort or is even impossible due to specific way of storage, and 2) the data subject's interest in the deletion is minimal. However, if the personal data are not processed lawfully (e.g., without an appropriate legal ground), this exemption would not apply.[117]

[115] GFDPA, art 29(1).
[116] GDPR, art 17.
[117] GFDPA, art 35(1).

1.4. Digital age of consent

Germany did not make use of the opening clause which allows Member States to reduce the age of digital consent for children in the online world.[118] The national legislator has decided not to derogate the provisions of the Regulation, thus keeping the age threshold for providing a valid consent at 16 years.

1.5. Appointment of a DPO

Designating a data protection officer has been required under German law for a long time now. Logically, the national legislator makes use of the opening clause and introduces additional cases where controllers and processors are required to appoint a DPO.[119]

The first case concerns companies which employ at least 10 persons which regularly engage in automated processing of personal data.[120] This obligation is retained from the previous German data protection act.[121] As this rule has been very broadly interpreted under the previous act, practically any German company with 10 employees working on a computer, falls under the scope of this rule.[122]

The other cases of mandatory DPO assignment are not dependent on the number of employees processing personal data, but on the nature and/or purposes of the processing activities. Thus, designation of a DPO is obligatory also in any of the following two cases where the processing: 1) is subject to impact assessments under Article 35 of the GDPR, 2) is conducted

[118] GDPR, art 8.
[119] GFDPA, art 38.
[120] Ibid.
[121] Baker McKenzie (n 100) p 15.
[122] Tim Wybitul, 'New Requirements for Data Protection Officers in Germany' (2011) 16 Business & Technology Sourcing Review 19, 19 <www.mayerbrown.com/en/perspectives-events/publications/2011/06/new-requirements-for-data-protection-officers-in-g> accessed 11 June 2019.

commercially for the purpose of transfer, anonymised transfer, or for market or opinion research purposes.[123]

2. Austria

Austria is also one of the few pioneers in Europe as regards data protection law. The country has long-standing traditions going back to the 1970s, as the first domestic data protection law was enacted in 1978.[124] The next landmark piece of legislation was adopted in 2000 when Austria transposed the Directive.[125] The Austrian legislative framework is enhanced by strict authorities and case law.[126] Therefore, it is not surprising that Austria is among the Member States which managed to review their existing data protection regime and adopt the GDPR implementing legislation on time.[127]

The new Austrian data protection act[128] (hereinafter ADPA) was presented quite ahead of schedule, in June 2017, and was aligned to enter into force at the same time as the Regulation on 25 May 2018.[129] This somehow rushed approach was considered to have left certain important matters insufficiently clear and even confusing (e.g., applicability of data protection rules to legal

[123] GFDPA, art 38.
[124] Günther Leissler, Patrizia Reisinger and Janos Böszörmenyi, 'Austrian Adaptation of the GDPR' in Olivia Tambou, Karen Mc Cullagh and Sam Bourton (eds), *National Adaptations of the GDPR* (Collection Open Access, Blogdroiteuropéen 2019) 35 <https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf> accessed 11 June 2019.
[125] Ibid.
[126] Ibid.
[127] International Association of Privacy Professionals (n 82).
[128] Bundesgesetz zum Schutz Natürlicher Personen bei der Verarbeitung Personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999, available in German at <www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> accessed 11 June 2019.
[129] Austrian Parliament, 'Neu im Verfassungsausschuss: Regierung Legt Neues Datenschutzgesetz Vor' (Press Release 736, 16 June 2017) <www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0736/> accessed 11 June 2019; Austrian Parliament, 'Nationalrat Verabschiedet Umfangreiche Novelle zum Datenschutzgesetz: Opposition Kritisiert Tempo des Gesetzgebungsprozesses' (Press Release 829, 29 June 2017) <www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0829/> accessed 11 June 2019.

entities).[130] Hence, the Privacy Deregulation Act 2018[131] was adopted to amend the ADPA and to revise certain provisions which are significant from a practical perspective.[132]

Together with changes in data protection law, the Austrian legislator took the opportunity to align and review many other laws which interact with the GDPR.[133] An approach which should be supported, insofar as effective application of the GDPR and its national implementing legislation is only possible within a legal framework which reconciles eventual conflicts between competing rights and obligations. Furthermore, the ADPA makes use of GDPR's opening clauses and also consists of legal provisions which transpose Directive (EU) 2016/680 in Austrian law.

2.1. Processing of employees' personal data

The new ADPA does not lay down comprehensive rules regarding processing of personal data in an employment context. Initially, the ADPA stipulated that the Austrian Labour Constitution Act[134] would be considered a general rule within the meaning of the opening clause of Article 88 of the GDPR, but the Privacy Deregulation Act cancelled this provision.[135] On the other hand, certain specific provisions for processing in an employment context could be found in the Austrian Labour Constitution Act. According to it, for instance, data applications such as

[130] Günther Leissler and Veronika Wolfbauer, 'Austria: (De)Regulatory Affairs or the Delegates' Proposal for Altering the National Data Protection Act' (*Lexology*, 17 April 2018) <www.lexology.com/library/detail.aspx?g=bd1bd5ba-48b8-40e7-995d-8560fedf094d> accessed 11 June 2019.
[131] Bundesgesetz, mit dem das Bundes-Verfassungsgesetz und das Datenschutzgesetz Geändert Werden (Datenschutz-Deregulierungs-Gesetz 2018), BGBl I 24/2018, available in German at <www.parlament.gv.at/PAKT/VHG/XXVI/A/A_00189/fname_690299.pdf> accessed 11 June 2019.
[132] Andreas Schutz and Jurgen Polzl, 'Austria's Struggle With the GDPR' (*CEE Legal Matters*, 1 August 2018) <https://ceelegalmatters.com/austria/8977-austria-s-struggle-with-the-gdpr> accessed 11 June 2019.
[133] Austrian Parliament, 'Nationalrat: Umfassende Datenschutzanpassungen Samt ELGA-Datenschutz-Entschließung für Registerforschung: Opposition Setzt Verbandsklagerecht Nicht Durch, Keine Zwei-Drittel-Mehrheit für Alleinige Zuständigkeit des Bundes im Datenschutz' (Press Release 442, 20 April 2018) <www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0442/> accessed 11 June 2019.
[134] Bundesgesetz vom 14. Dezember 1973 Betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz – ArbVG), BGBl 22/1974, available in German at <www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008329> accessed 11 June 2019.
[135] Leissler and Wolfbauer (n 130).

employees' questionnaires requiring more than general information, specific monitoring systems, and automated HR management systems require the approval of the works council.[136]

Although not relevant only to processing employees' data, it is also interesting to mention the confidentiality obligation provided under Article 6 of ADPA. It obliges employees to treat as confidential the personal data which have been entrusted or made accessible to them due the employment, unless there is a legally permissible reason to disclose the data.[137] Employees are allowed to transfer personal data only if they have been explicitly instructed to do so by their employer.[138] In addition, employers are required to bind their employees by contract to transfer data only under instructions and to maintain the personal data confidential even after the termination of the employment.[139]

2.2. Special categories of personal data

Special categories of personal data are also not a subject of comprehensive regulation in the ADPA. One of the rare occasions where the national data protection act lays down further rules regarding special categories of data is in Article 7(3) of the ADPA. It provides that special categories of personal data could be processed for scientific, historical or statistical purposes only if there is 'important public interest' in the study, subject to further procedural requirements.

2.3. Restrictions to data subjects' rights

The ADPA provides a few exceptions which apply in specific situations, and does not contain far-reaching derogations.

Secrecy obligation

[136] Leissler, Reisinger and Böszörmenyi (n 124) 38.
[137] ADPA, art 6(1).
[138] ADPA, art 6(2).
[139] Ibid.

The right of access of data subjects under Article 15 of the GDPR may be restricted if it could lead to disclosure of 1) an official secret[140] or 2) a business or a trade secret.[141] As regards official secrets, the right of access could be refused by a controller who fulfils statutory tasks if granting the information would jeopardise these tasks. Controllers could also refuse to grant access to personal information if doing this would disclose theirs or third party's business or trade secret.

Exception from the right to erasure and the right to rectification

Article 4(2) of the ADPA lays down a provisional exception to the data subjects' right to rectification[142] and erasure.[143] Where the corresponding obligation of the controller cannot be performed instantly due to economic or technical restrictions, the processing would instead be restricted pursuant to Article 18(2) of the GDPR, until it is possible to rectify or erase the data.

Freedom of expression

The ADPA implements the opening clause under Article 85 of the GDPR which allows Member States to introduce broad exemptions, including as regards essential data subjects' rights.[144] In that task, the Austrian legislator draws a distinction between 1) processing for journalistic purposes and 2) processing for scientific, artistic or literary purposes.[145]

On the one hand, ADPA provides broad exemptions for media undertakings, media services and their employees, by practically exempting their processing of personal data for journalistic purposes from the regulation of the GDPR, including Chapter III (Rights of the data subject).[146] On the other hand, to the extent necessary to reconcile freedom of expression and data protection, the ADPA provides a narrower scope of derogations of the GDPR for scientific, artistic or literary

[140] ADPA, art 4(5).
[141] ADPA, art 4(6).
[142] GDPR, art 16.
[143] GDPR, art 17.
[144] ADPA, art 9.
[145] See ADPA, art 9(1)-(2).
[146] Leissler, Reisinger and Böszörmenyi (n 124) 39; ADPA, art 9(1).

purposes.[147] Nonetheless, it also allows for exemption of all data subjects' rights under Chapter III of the GDPR.[148]

2.4. Digital age of consent

Unlike Germany, Austria has made use of the opening clause which allows for lowering the age threshold for digital consent. According to Article 4(4) of the ADPA children could provide a valid consent for the processing of their personal data if they are at least 14 years of age. The approach to lower the age should be supported, insofar as the GDPR threshold is unnecessarily high. It ultimately restricts the rights of persons who are sufficiently aware of their decisions and respective consequences in the online world.

2.5. Appointment of a DPO

The Austrian legislator has not introduced additional cases where the designation of a DPO is mandatory, hence, only the cases provided in the GDPR apply.[149] Even though the ADPA has not made use of the opening clause under Article 37(4) of the GDPR, it has supplemented the Regulation's requirements with a number of more stringent rules regarding the rights and obligations of data protection officers.[150]

The DPOs and their privacy team are under strict secrecy obligations which apply even after the end of their activity.[151] For instance, they should not disclose the identity of individuals who have approached them, as well as details which could help to identify these persons.[152] The DPO

[147] ADPA, art 9(2).
[148] Ibid.
[149] Bird & Bird, 'GDPR Tracker: Austria' (*Bird & Bird*) <www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/austria> accessed 11 June 2019.
[150] ADPA, art 5.
[151] ADPA, art 5(1).
[152] Ibid.

and their privacy team are entitled to a specific right to remain silent and the obtained data, files and documents under this right cannot be confiscated.[153]

3. Bulgaria

Bulgarian data protection legislation does not have the same long standing traditions as Germany and Austria. The first Bulgarian Personal Data Protection Act[154] (hereinafter BPDPA) was introduced in 2001[155] and entered into force in 2002. Even though at that time Bulgaria was not a Member State yet, the act was drafted in conformity with the Directive.[156] Since its adoption, the BPDPA has been amended numerous times and it is still into force.

In order to align national law with the GDPR requirements, the Bulgarian legislator chose to introduce amendments to the existing act rather than adopting an entirely new one. It should be noted, however, that this was not carried out in a timely manner. The first bill of the amended act was proposed on 18 July 2018 which was after the GDPR had already become directly applicable.[157] This caused uncertainty and inconveniences for local companies, in particular in terms of transaction costs. They had to first align their business activities with the GDPR, and afterwards had to wait for the amendments in the BPDPA, and only then to carry out new alignment with the national act.

Since there was a lot of public interest and even criticism against the first version of the bill, it took relatively long time for the involved stakeholders to agree on the final provisions. Hence,

---

[153] DLA piper, 'Data Protection Laws of the World: Data Protection Officers: Austria' (*DLA Piper*, 10 January 2019) <www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=AT> accessed 11 June 2019.
[154] Zakon za zashtita na lichnite danni (Personal Data Protection Act), SG 1 from 4 January 2002 as last amended with SG 17 from 26 February 2019, available in Bulgarian at <www.lex.bg/laws/ldoc/2135426048> accessed 11 June 2019.
[155] Bulgarian Parliament, Draft Bill Bulgarian Personal Data Protection Act, 25 <www.parliament.bg/bills/39/154-01-23.pdf> accessed 11 June 2019; DLA Piper, 'Data Protection Laws of the World: Law: Bulgaria' (*DLA Piper*, 10 January 2019) <www.dlapiperdataprotection.com/index.html?t=law&c=BG> accessed 11 June 2019.
[156] Ibid 22.
[157] Bulgarian Parliament, Draft Bill Act for Amending and Supplementing the Bulgarian Personal Data Protection Act, 575 <www.parliament.bg/bills/44/802-01-27.pdf> accessed 11 June 2019.

the final draft was adopted on 20 February 2019. Also at that time, the Bulgarian data protection supervisory authority published its black list under Article 35(4) of the GDPR indicating for which activities it considers that a data protection impact assessment must be carried out.[158]

The adopted amendments of the BPDPA aim to repeal old legislation which would contradict the GDPR, to transpose Directive (EU) 2016/680, to supplement the GDPR provisions, and make use of the opening clauses.

3.1. Processing of employees' personal data

The amended BPDPA does not implement extensive rules in the employment context, but rather focuses on certain fragmented matters.

Copying of personal identification documents

One of the amendments concerns a data protection matter which become sensitive for Bulgarian citizens in the recent years - processing of personal identification documents (e.g., identity cards, driving licences or residence documents). To address this particular subject, the BPDPA prohibits controllers and processors to make copies of personal identification documents, unless there is a special law authorising it.[159] Even though this is a general provision and not employment-specific, its main aim is to stop the widespread practice of employers which have been making and retaining unnecessary copies of identification documents of their employees, just in case.

Retention period for personal data of job applicants

[158] Bulgarian Commission for Personal Data Protection, 'CPDP adopted a list of the types of processing operations for which data protection impact assessment is required ' (Press Release, 13 February 2019) <www.cpdp.bg/?p=news_view&aid=1370> accessed 11 June 2019.
[159] BPDPA, art 25g.

Employers are required to predetermine a retention period for personal data of job applicants.[160] The period cannot be longer than 6 months, unless the applicant has provided his or her explicit consent for a longer retention of the data. After the expiry of the relevant period, the employer has to delete or destroy the documents containing personal data, unless there is a special law requiring otherwise. There is a partial derogations from this rule. Certain documents which are particularly important and usually harder to obtain have to be returned to the employee.[161] Those documents include originals or notarised copies of documents which certify the physical or mental capacity of the job applicants, their qualification and work experience.

Providing statutory retention period for processing documents of job applicants should also be asserted positively. Similar to the identification documents, the aim of the legislator is to stop the practice of employers to keep documents containing personal data for an unnecessary long period.

Additional rules and procedures

Employers are obliged to adopt internal rules for certain activities which involve data processing.[162] These include: 1) reporting breaches, 2) using internal company resources (e.g., equipment, information, etc.), and 3) monitoring systems for access control, working time and labour discipline. These internal rules have to regulate at least the scope, obligations and implementation steps, taking into account the particularities of the business activity. If applied and enforced properly, this obligation could have a positive effect. For instance, transparent and consistent rules combined with employee awareness will facilitate compliance with data protection law. However, if employers would follow a formalistic approach, by adopting general rules which

[160] BPDPA, art 25k(1).
[161] BPDPA, art 25k(2).
[162] BPDPA, art 25i.

do not consider the specifics of the business, and do not conduct appropriate staff training, these rules would become just another piece of thesis.

3.2. Special categories of personal data

The BPDPA does not make use of the opening clauses on special categories of personal data. Given the domestic particularities, especially in the employment context, it might be reasonably expected that the national legislator would implement additional rules in the future.

3.3. Restrictions to data subjects' rights

The Bulgarian legislator has provided only a few derogations to data subjects' rights applicable in specific processing situations.

Freedom of expression

The BPDPA implements the opening clause allowing reconciliation of the right of data protection and the right of freedom of expression. Pursuant to Article 25z(3) of the BPDPA, controllers and processors are provided the discretion to exclude almost all data subjects' rights under Chapter III of the GDPR (Articles 12 to 21) for journalistic, academic, artistic or literary purposes. Other GDPR provisions regulating data subjects' rights in a broader sense are also excluded, including the controller's obligation to notify data subjects in case of a data breach and processing of special categories of personal data.

Article 25z(5) of the BPDPA introduces a narrower scope of exceptions when the purpose of the processing is to create a photographic or audiovisual work by filming a person in the course of their public activity or in public space. Nonetheless, this provision also excludes the application of the same data subjects' rights (as indicated above), including the controllers' obligation to notify the data subject for a data breach.

As a side remark, it is interesting to note that the implementation of this opening clause in the Bulgarian legislation was a particularly controversial topic, especially as regards processing for journalistic purposes. The culmination point was the veto of the Bulgarian president on the final amendments in the national data protection act.[163]

The Bulgarian legislator introduced a balancing test in order to assess whether the processing of the personal data for these purposes is at all lawful.[164] It includes 10 criteria on the basis of which to evaluate whether the processing strikes a balance between the right to personal data protection and the right to freedom of expression.[165] Only if the test is satisfied, i.e. a balance is achieved, the personal data could lawfully be made available to the public.

These criteria include, inter alia, assessment of: the categories of personal data, the impact which a disclosure could have on the privacy and the reputation of the data subject, the importance of disclosure to clarify a matter of public interest, the circumstances in which the data became known to the controller, etc. Actually, these criteria are not even exhaustive, as the last one requires to take into account also other circumstances which are relevant for the specific case.

Due to the broad wording of the numerous criteria, this provision was highly criticised, including by the Bulgarian Association of Journalists,[166] for allowing too much discretion. It raised concerns that its interpretation and application could become arbitrary. Worst case scenario - abuse of this broad discretion could lead to suppression of the freedom speech and ultimately to media censorship.[167]

---

[163] Bulgarian President, 'The President Vetoed a Provision of the Act for Amending and Supplementing the Bulgarian Personal Data Protection Act' (Press Release, 4 February 2019) <www.president.bg/news4798/prezidentat-nalozhi-veto-varhu-razporedba-ot-zakona-za-izmenenie-i-dopalnenie-na-zakona-za-zashtita-na-lichnite-danni.html > accessed 11 June 2019.
[164] BPDPA, art 25z(2).
[165] Ibid.
[166] Management Board of the Association of the Bulgarian Journalists, 'Attack Against the Freedom of Speech' (Press Release, 25 January 2019) <www.sbj-bg.eu/index.php?t=41677> accessed 11 June 2019.
[167] Ibid.

In addition, the motives of the President's veto raised another concern. The implementation of these 10 criteria leads to unnecessary overregulation.[168] Therefore, they do not fulfil their purpose of reconciliation between the two fundamental rights. Instead, the criteria rather give preference to the right of personal data protection.[169] As correctly noted in the motives of the veto, the GDPR requires reconciliation of the rights, and not giving preference to one or the other.

However, the president's veto has been overridden by the Parliament and the discussed provision has already entered into force.[170] Hence, now it remains to be seen whether the concerns expressed by the journalists and the president would turn out to be justified or not. Nevertheless, courts and supervisory authorities would also play an important role to monitor the proper application of this provision.

Statistical purposes

Further, Article 25m of the BPDPA provides for restrictions of the data subjects' rights when the processing of the personal data is carried out for statistical purposes. In this case, the individual's right to access, to rectification, to restriction and to object under the GDPR could be excluded.

Humanitarian purposes and disasters

The processing of personal data for humanitarian purposes by public authorities or humanitarian organisations, as well as processing in the case of disasters is also subject to specific exceptions.[171] Similar to above, all data subjects' rights provided for in Articles 12 to 21 and Article 34 of the GDPR are excluded.

---

[168] Bulgarian President (n 163).
[169] Ibid.
[170] Bulgarian Commission for Personal Data Protection, 'The Act for Amending and Supplementing the Bulgarian Personal Data Protection Act was promulgated' (Press Release, 26 February 2019) <www.cpdp.bg/?p=news_view&aid=1373> accessed 11 June 2019.
[171] BPDPA, art 25o.

3.4. Digital age of consent

The Bulgarian legislator implemented the opening clause allowing for lower digital age of consent. Article 25v of the BPDPA sets the age at 14 years which is the same as under the Austrian data protection act.

3.5. Appointment of a DPO

The initial draft bill which was published for public consultations contained a provision which made use of the opening clause on data protection officers.[172] According to Article 25b(1) of this first draft, controllers and processors had to appoint a DPO when processing personal data of more than 10 000 individuals. However, this provision was dropped from the final text of the act. It was highly criticised due to its ambiguity. The text did not provide any further guidance whether the threshold of 10 000 individuals concerns data collected for a certain period, data which are processed on a regular basis, etc. The lack of additional criteria caused confusion and legal uncertainty as to how this provision is supposed to be interpreted. The finally adopted version of the BPDPA does not introduce additional cases for mandatory assignment of a DPO. In that regard, only the general requirements of the GDPR apply.

Therefore, the only particularity which has to be considered regarding DPOs concerns the procedure for appointing a DPO. According to Article 25b of BPDPA, controllers and processors are obliged to notify the national data protection supervisory authority, if they have designated a DPO and to provide contact information. The form, content and procedure for submitting the notification are also expressly defined.

[172] Dessislava Fessenko, 'Bulgaria Plans to Introduce a Range of Derogations From the EU General Data Protection Regulation' (*Lexology*, 18 May 2018) <www.lexology.com/library/detail.aspx?g=8a42dc5b-756c-49f1-9aef-9b1ceea600ed> accessed 11 June 2019.

4. Ireland

Ireland is another one the countries with relatively long traditions in data protection law, adopting its first national data protection act in 1988.[173] The next milestone in the data protection development was the transposition of the Directive in Irish law in 2003.[174]

In order to align its legislation with the GDPR, the national legislator introduced a new Irish Data Protection Act in 2018[175] (hereinafter IDPA). The bill was initiated on 30 January 2018 and was signed into law on 24 May 2018.[176] Ireland did not adopt a minimalistic approach when introducing the GDPR implementation legislation. On the contrary, the new IDPA is a comprehensive and lengthy act consisting of 232 Articles. The previous data protections acts from 1988 and 2003 still apply for a limited number of specific matters.[177]

According to the published Explanatory Memorandum, the IDPA has four key purposes. It supplements the GDPR requirements where this is allowed, transposes Directive 2016/680, constitutes the Data Protection Commission as a data supervisory authority and implements changes to other national laws which refer to the previous data protection acts from 1988 and 2003.[178] Of interest for this thesis are mainly the provisions of Part 3 of the IDPA which give further effect to the GDPR.

---

[173] IT Governance Europe, 'Data Protection Act (DPA) Ireland 2018' (*IT Governance Europe*) <www.itgovernance.eu/en-ie/data-protection-ie> accessed 11 June 2019.
[174] Ibid.
[175] Data Protection Act 2018, No 7 of 2018, available in English at <http://www.justice.ie/en/JELR/Data_Protection_Act_2018.pdf/Files/Data_Protection_Act_2018.pdf> accessed 11 June 2019.
[176] Irish Parliament (Oireachtas), 'Data Protection Act 2018: History of this Act' (Irish Parliament, 24 May 2018) <www.oireachtas.ie/en/bills/bill/2018/10/> accessed 11 June 2019.
[177] Irish Data Protection Commission, 'Data Protection Legislation: Key Data Protection Legislative Frameworks Applicable From 25 May 2018' (*Data Protection Commission*) <www.dataprotection.ie/en/legal/data-protection-legislation> accessed 11 June 2019.
[178] Explanatory Memorandum to the Data Protection Act 2018, 2 <http://www.justice.ie/en/JELR/Data_Protection_Act_2018_Explanatory_Memorandum.pdf/Files/Data_Protection_Act_2018_Explanatory_Memorandum.pdf> accessed 11 June 2019 (hereinafter Explanatory Memorandum).

4.1. Processing of employees' personal data

The IDPA does not contain comprehensive rules on processing of personal data in an employment context. The only provision which is of practical importance is Article 46 of the IDPA. It allows processing special categories of personal data where required under employment or social welfare domestic legislation. The controller must implement appropriate safeguard measures to guarantee the data subjects' fundamental rights when carrying out processing of sensitive data.

4.2. Special categories of personal data

The Irish legislator has embraced a fairly comprehensive approach when laying down rules on processing of sensitive personal data, dedicating a whole chapter to it – Chapter 2, Part 3 of the IDPA – which is called 'Processing of special categories of personal data and processing of personal data relating to criminal convictions and offences'.

Article 45 of the IDPA starts by outlining a general rule that processing special categories of personal data is lawful only if: 1) it is authorised by the therein indicated IDPA provisions, or 2) Article 9 of the GDPR. The rest of the provisions in the Chapter contain different specific rules on the lawfulness of the processing depending on its purpose.

Namely, Articles 46 to 54 of the IDPA lay down rules on processing of special categories of data for the following purposes: 1) employment or social welfare law, 2) legal advice and legal proceedings, 3) electoral activities and functions of the Referendum Commission (the wording is limited to data revealing political opinions),[179] 4) administration of justice and performance of functions, 5) insurance and pension (the wording is limited to health data),[180] 6) substantial public

[179] IDPA, art 48.
[180] IDPA, art 50.

interest (it includes also data under Article 10 of the GDPR),[181] 7) health and medical purposes under Article 9(2)(h) of the GDPR, 8) public interest in the area of public health, 9) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Most of the above mentioned provisions require implementation of appropriate measures to guarantee the fundamental rights and freedoms of individuals when sensitive data are being processed. The Irish legislator provided companies with guidance for implementing such safeguards by indicating a number of exemplary measures in Article 36 of the IDPA. They are not mandatory but could serve as a reliable guidance for compliance purposes. For instance, companies are encouraged to require explicit consent, limitation on access to personal data within a workplace, deadlines for deletion of personal data, staff training, appoint a data protection officer even if it is not mandatory, etc.

Further, it is interesting to take a closer look at Article 50 of the IDPA. It provides a derogation for processing of data concerning health without the individual's express consent for insurance and pension purposes. The purposes are further specified as follows: 1) a policy of insurance or life assurance, 2) a policy of health insurance or health-related insurance, 3) an occupational pension, a retirement annuity contract or any other pension arrangement, and 4) the mortgaging of property. Last, the processing of the health data should not only be necessary, but also proportionate for these purposes. Supposedly, Article 50 of IDPA would be welcomed by insurance and financial companies which would not have to deal with the peculiarities of the stringent consent requirements under the GDPR as a basis for processing of special categories of data.[182]

[181] IDPA, art 51.
[182] John Cahir, 'Ireland passes Data Protection Act 2018' (*A&L Goodbody*, 25 May 2018) 4 <www.algoodbody.com/images/uploads/services/EU-Data-Protection/Irish_Government_Published_DP_Act_2018.pdf> accessed 11 June 2019.

Another noteworthy provision is Article 48 of the IDPA. It governs the processing of personal data revealing political opinions. This is allowed in two instances. First, during electoral activity for gathering information on individuals' political views by a political party or a single politician. Second, by the Irish Referendum Commission when it executes its tasks.

Lastly, it is interesting to note that Ireland adopts an approach which differentiates from the other Member States reviewed until now. It confers powers on the executive branch to enact further rules regarding sensitive data.[183] Subject to specific procedures, ministers could make further regulations allowing the processing of special categories of personal data, insofar as this is justified by a substantial public interest. This interest should be exactly identified in the regulation itself, together with the safeguard measures undertaken to protect the fundamental rights of the individuals whose data are processed.[184]

4.3. Restrictions to data subjects' rights

Most of the rules containing restrictions of data subjects' rights and controllers' obligations are laid down in Chapter 3 of Part 3 of the IDPA. Outside this chapter, the IDPA contains only a few fragmented rules stipulating restrictions.

Article 58 and 59 of the IDPA are another illustration of the specific attention which the Irish legislator has paid to the processing of personal data for electoral activities. By acknowledging the overriding significance of the elections for the democracy in the State, the provisions restrict certain data protection rights of individuals.[185] Namely, the rights of data subjects to object to 'direct marketing' via direct mailing (post) and the right to object under Article 21 of the GDPR. These restrictions are applicable when personal data are processed within electoral activities by

[183] IDPA, art 51.
[184] IDPA, art 51(4).
[185] Explanatory Memorandum (n 178) 11.

political parties or single politicians, or by the Referendum Commission when it executes its tasks. According to the Explanatory Memorandum, current limitations on voting activities conducted via electronic means without the explicit consent of data subjects under ePrivacy regulations would not be prejudiced.[186]

Article 60 of the IDPA allows for wide-ranging derogations from all data subjects' rights,[187] the right to notification in case of a data breach,[188] and principles of data processing[189]. Such derogation could be allowed for important objectives of general public interest, such as cabinet confidentiality, parliamentary privilege, national security, defence, prosecution of criminal offences, exercising legal claims, etc.[190] Further, Article 60(3)(b) of the IDPA allows exemptions when the personal data is an opinion about a particular individual, and are provided confidentially to another person who has a legitimate interest to know this information. This particular derogation could be very useful for confidential disclosures of information or whistleblowing.[191]

The IDPA also provides for extensive restrictions of the data subjects' rights for the purposes of reconciliation with the fundamental right to freedom of expression and information.[192] All data subjects' rights and all other provisions under Chapter II to VII of the GDPR (with the only exception for Article 5(1)(f)) could be excluded from application if they are incompatible with the right to freedom of expression and information. However, the wording of the provision is broad and does not contain enough guidance in order to avoid inconsistent and even conflicting interpretation.[193] It is therefore helpful that the provision expressly provides the possibility for the

[186] Ibid.
[187] GDPR, arts 12-22.
[188] GDPR, art 34.
[189] GDPR, art 5.
[190] IDPA, art 60(3)(a).
[191] Explanatory Memorandum (n 178) 11.
[192] IDPA, art 43.
[193] Hugh McCarthy, 'Part I: The GDPR, Freedom of Expression and a Right to Remember?' (2018) 11(3) Data Protection Ireland 5, 5.

Irish data protection supervisory authority to refer questions of law to the High Court, when in doubt regarding the application of the freedom of expression exemption.[194]

4.4. Digital age of consent

The Irish legislator has adopted a stricter approach as regards the processing of children data in an online context. First, it does not take advantage of the opening clause allowing Member States to lower the digital age of consent. Thus, only persons who are at least 16 years old could provide valid consent for processing of personal data under Article 8 of the GDPR.[195]

A peculiar decision of the Irish legislator is to stipulate that, for the purposes of the IDPA, any reference to a 'child' in the GDPR would be considered reference to persons under 18 years of age which corresponds to the definition in the UN Convention on the Rights of the Child.[196]

Further, Article 30 of the IDPA determines as an offence the processing of children's personal data for direct marketing, profiling, or micro-targeting.[197] Thus, processing of personal data of individuals under 18 years of age for these purposes could be sanctioned with an administrative fine by the national data protection supervisory authority. The rationale behind this prohibition is to address the childhood obesity issue in Ireland, by restricting direct marketing of junk food and drinks, in particular.[198]

However, Article 30 of the IDPA has raised concerns that it might not comply with the Regulation, because it exceeds the discretion provided to the Member States and imposes restrictions on processing of personal data which is otherwise allowed by the GDPR.[199] Therefore,

---

[194] Ibid.
[195] IDPA, art 31(1).
[196] IDPA, art 29; Explanatory Memorandum (n 178) 6.
[197] IDPA, art 30.
[198] Irish Parliament (Oireachtas), Data Protection (Amendment) Bill 2018 Dáil Éireann Debate 29 November 2018 <www.oireachtas.ie/en/debates/debate/dail/2018-11-29/18/> accessed 11 June 2019 (hereinafter Dáil Éireann Debate 29 November 2018).
[199] Explanatory Memorandum (n 178) 7.

the application of the provision was not commenced.[200] Instead, on 29 November 2018 a Data Protection (Amendment) Bill 2018 was initiated.[201] The main purpose of the amendment is to address the potential incompatibility of Article 30 of DPA with the GDPR. The bill proposes a change in the wording whereby such processing of personal data would not be considered 'an offence' but simply 'unlawful'.[202] However, the provision has not been changed yet and its performance is not yet commenced.

Regarding processing of children personal data, it is also worth mentioning Article 32 and Article 33 of the IDPA. Both provisions aim to provide enhanced protection for children's personal data. The first requires the Irish data protection authority to encourage companies to draw up codes of conduct on processing of children's personal data. The second establishes an 'enhanced right to be forgotten' applicable for children data.[203]

4.5. Appointment of a DPO

Currently, the Irish Data Protection Act does not contain additional cases, other than the ones provided in the GDPR, where appointment of a DPO is mandatory. Still, the approach of Ireland is differentiating from the so far reviewed. Instead of explicitly providing additional specific cases in the national data protection act, the legislator has conferred power on the Irish Minister for Justice and Equality. The Minister, after consulting other ministers and the Irish data protection authority, may make further regulations which require designation of a DPO in addition to the cases provided in the GDPR.[204]

[200] Ibid.
[201] Dáil Éireann Debate 29 November 2018 (n 198).
[202] Ibid.
[203] Explanatory Memorandum (n 178) 7.
[204] IDPA, art 34(1).

5. Denmark

Similar to Germany, Austria and other countries such as Norway, France and Sweden, Denmark is also one of the pioneers in Europe's data protection legislation.[205] It has adopted its first piece of national data protection legislation back in 1979 which is the Public Authorities' Registries Act and the Private Registry Act.[206] The next piece of data protection legislation was the Act on Processing of Personal Data which was adopted in 2000.[207] It repealed the previous act and transposed the Directive into the Danish legislation.[208]

Finally, in order to align its legislation with the GDPR, Denmark adopted the Danish Data Protection Act (hereinafter DDPA).[209] The act was adopted by the Parliament on 17 May 2018 and came into force on the 25 May 2018, the same date as the Regulation.[210] With the entry into force of the new act, the previous Act on the Processing of Personal Data from 2000 was repealed.[211] The geographic scope of the DDPA does not include the Faroe Islands and Greenland, both of which are otherwise under the Crown of Denmark, but are not members of the European Union.[212]

The DDPA supplements the new EU requirements, by re-enacting some of the previous Danish data protection legislation, making use of opening clauses, and regulating specific matters

[205] Tenna Overby, 'The Danish Adaptation of the GDPR' in Olivia Tambou, Karen Mc Cullagh and Sam Bourton (eds), *National Adaptations of the GDPR* (Collection Open Access, Blogdroiteuropéen 2019) 61 <https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf> accessed 11 June 2019.
[206] Ibid.
[207] Ibid.
[208] Ibid.
[209] Databeskyttelsesloven (Data Protection Act), available in English at <www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf> accessed 11 June 2019.
[210] Overby (n 205) 61.
[211] DDPA, art 46(2).
[212] DDPA, art 48.

not regulated in the GDPR.[213] The use of opening clauses is mainly focused on providing the public sector with broader competences when processing personal data and to restrict data subjects' rights.[214]

5.1. Processing of employees' personal data

The DDPA generally authorises processing of personal data under Article 6 of the GDPR and sensitive data under Article 9 of the GDPR in an employment context in three cases.[215] The first is quite common and it allows for such processing if this is required by law or a collective agreement.

Second, the legislator stipulates that even a legitimate interest which arises from a law or a collective agreement is an appropriate ground to process both personal and sensitive data. This approach is differentiating from the reviewed until now. It provides a more flexible and broader possibility for processing of personal data in an HR context. However, it is rather peculiar that the rule is also applicable for public authorities, insofar as this is not allowed by the GDPR.[216]

Last, the DDPA expressly states that employees' data could be processed on the basis of consent. Although this is not a unique provision, insofar as, for instance, the German legislator also considers consent to potentially be a valid legal ground for processing personal data in an employment context (commented in Section III.1.1 above) - here, there is a noteworthy difference. Whereas the German data protection act lays down additional conditions which have to be met for a valid consent in an employment context,[217] it seems that the Danish data protection act acknowledges consent as an appropriate legal ground, subject to no additional criteria (besides the

[213] See Karsten Holt, 'Analysis: The Danish Data Protection Act and Its GDPR Derogations' (*IAPP*, 18 December 2018) <https://iapp.org/news/a/analysis-the-danish-data-protection-act-and-its-gdpr-derogations/> accessed 11 June 2019.
[214] Overby (n 205) 62.
[215] DDPA, art 12.
[216] Holt (n 213).
[217] GFDPA, art 26(2).

GDPR's requirements) which could demonstrate that the consent indeed was freely given.[218] The Danish forthright manner is rather surprising, as it is contrary to the opinions of the Article 29 Working Party (replaced by the EDPB) which has numerously expressed its doubts regarding the freedom of and therefore the validity of an employee's consent.[219]

5.2. Special categories of personal data

In addition to the provisions on processing of special categories of data in an employment context discussed in Section III.5.1 above, the DDPA lays down a number of other noteworthy provisions.

On the one hand, the DDPA starts by expressly stating that most of the legal grounds for processing sensitive data under the GDPR are acknowledged under Danish law, without further specifying the Regulation's provisions where this is allowed.[220] The DDPA simply states that the GDPR conditions should be complied with. These legal grounds are: 1) consent, 2) protection of individuals' vital interests, 3) by NGOs, 4) data made public by the data subject, and 5) legal claims.[221]

On the other hand, the Danish legislator does not fully implement the legal grounds for processing: 1) in the field of employment and social security and social protection law, 2) substantial public interest, and 3) health and medical services.[222] The DDPA modifies the wording of the GDPR legal grounds in line with Danish law.[223]

---

[218] DDPA, art 12(3).
[219] Holt (n 213); Bird & Bird LLP, 'The Danish Data Protection Act Has Been Passed!' (*Lexology*, 8 June 2018) <www.lexology.com/library/detail.aspx?g=6098ea81-516f-4bf8-a566-5678551f546c> accessed 11 June 2019; Article 29 Data Protection Working Party, 'Guidelines on Consent Under Regulation 2016/679' (28 November 2017 revised on 10 April 2018) WP 259, 7 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030> accessed 11 June 2019.
[220] DDPA, art 7(1).
[221] GDPR, arts 9(2)(a),(c)-(f).
[222] GDPR, arts 9(2)(b),(g)-(h); Bird & Bird, 'GDPR Tracker: Denmark' (*Bird & Bird*) <www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/denmark> accessed 11 June 2019.
[223] Ibid.

Another noteworthy provision from a Danish perspective is Section 10 of the DDPA.[224] It governs the processing of personal data and sensitive data, including data related to criminal convictions and offences, for the purposes of statistical or scientific studies which are of significant importance. The provision re-enacts a text from the previous national data protection act.[225] It is of importance in Denmark, as scientific studies, in particular health research, are widespread and processing of sensitive data for such purposes has long been authorised without consent of the data subject.[226] Therefore, the opening clauses under Article 9(2)(j) and Article 89 of the GDPR have been amongst the priorities of Denmark during the GDPR negotiations.[227]

The Danish legislator has conferred powers on the ministers, after consulting the Minister of Justice, to enact more detailed rules on processing of special categories of data.[228]

5.3. Restrictions to data subjects' rights

Part 6, Chapter III of the DDPA is called 'Restrictions of the rights of data subjects'. Most of its provisions introduce derogations from the individuals' right to information (including when the information is obtained from another source), access and notification of data breach.[229]

For instance, all of these rights could be restricted if the data subject's interests are overridden by important private interests.[230] The rather broad wording of the provision seems to be open to potentially broad interpretations. Nevertheless, this exemption could be particularly useful during internal investigations, whistleblowing or for protection of business secrets.[231]

[224] Overby (n 205) 63.
[225] Ibid.
[226] Ibid.
[227] Ibid.
[228] DDPA, art 7(5).
[229] GDPR, arts 13(1)-(3), 14(1)-(4), 15, 34.
[230] DDPA, art 22(1).
[231] Bird & Bird LLP (n 222).

The DDPA introduces derogations from the same rights also for the public sector, too.[232] It provides a non-exhaustive list of public interests which could override the individuals' interests. These include, inter alia, national and public security, prevention and prosecution of crimes, protection of other data subjects, civil law claims and others.

Further, the Danish legislator excludes the application of the right to information and access under the GDPR in the context of the court's judicial activity.[233]

Given the already mentioned special attention to the issue in Denmark (commented in Section III.5.2), it comes as no surprise that a broader exception is provided for the purposes of scientific studies and statistics. Excluded from application are the right of access, rectification, restriction of processing, and the right to object to processing.[234] However, the provision does not derogate other essential rights such as the right of information and erasure.[235]

If disclosing information for a data breach may hinder an investigation of a criminal offence, the controller could be exempted from notifying the data subject under Article 34 of the GDPR.[236] However, such an exception could be authorised only by the police.

Article 23 of the DDPA contains another noteworthy exception. In certain cases, it allows public authorities to further process personal data for purposes other than the original purposes for which they were collected, without notifying the data subjects for this. Thus, individuals are precluded from their right of information under Article 13(3) and Article 14(4) of the GDPR. In practice, this means that in certain cases public authorities would not be obliged to disclose to data subjects when their personal data is being used for other purposes.

[232] DDPA, art 22(2).
[233] DDPA, art 22(4).
[234] GDPR, arts 15-16, 18, 21.
[235] GDPR, arts 13-14, 17.
[236] DDPA, art 22(6).

However, there is one important restriction to Article 23 of the DDPA – if the personal data are used for 'control purposes', the exception does not apply, and therefore public authorities would have to inform the data subjects for the further processing. According to a report to the draft of the DDPA submitted by the Legal Affairs Committee, such a processing by public bodies is very intrusive and therefore citizens are supposed to be informed for it.[237] Even though Article 23 of the DDPA has been subject to extensive negotiations and criticism for being too far-reaching and reducing the transparency to data subjects, the DDPA has been adopted only with minor amendments.[238]

The Danish legislator also has acknowledged that the freedom of expression needs to be guaranteed, especially against abusive exercise of data protection rights. And in doing so, the DDPA adopts a fairly categorical approach. First, Article 3(1) of the DDPA stipulates generally that neither the DDPA, nor the GDPR would be applicable if it would be contrary to: 1) Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms,[239] or 2) Article 11 of the EU Charter on Fundamental Rights.[240] Both of these provisions provide protection of the freedom of expression and information as a fundamental right.

Further, the act sets out additional derogations for specific processing situations. For instance, it again provides a full exception (i.e. neither the GDPR, nor the DDPA are applicable) in cases of processing of personal data covered by the Danish Act on Information Databases Operated by the Mass Media.[241]

---

[237] Danish Parliament, Legal Affairs Committee, Report from 9 May 2018 <www.retsinformation.dk/Forms/R0710.aspx?id=201193> accessed 11 June 2019.
[238] Ibid; Holt (n 213).
[239] Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocols No.11 and No.14 (opened for signature 4 November 1950, entered into force 3 September 1953) CETS No. 005.
[240] Charter of Fundamental Rights of the European Union [2010] OJ C83/389.
[241] DDPA, art 3(4).

A narrower exception is provided when the processing is carried out exclusively for journalistic, artistic or literary expression purposes. In such a case, the DDPA and Chapters II-VII and IX of the GDPR are not applicable (with the exception of Articles 28 to 32 of the GDPR). Other specific processing situations in the media context are also regulated.

5.4. Digital age of consent

The Danish legislator has made use of the opening clause under Article 8 of the GDPR, by setting the age for digital consent at 13 years.[242] This is the minimum allowed by the Regulation and the lowest age threshold from the legislations reviewed so far. Thus, minors who are at least 13 years of age would be able to provide their valid consent for information society services. When the child is younger, the holder of the parental responsibility has to give or approve the consent for processing the personal data.

It is interesting to note the contrasting approach of the Danish and the Irish legislator. As explained above in Section III.4.4, the rationale behind the decision of the Irish Parliament to maintain the age threshold of 16 years was to limit the exposure of children to certain online services (e.g., marketing of unhealthy food and drinks), thereby focusing on the possible negative influence of the Internet. However, the Danish legislator adopts another approach. The DDPA acknowledges that children could benefit from online content (e.g., educational, social, etc.) and takes into account that setting a lower threshold would either exclude children from possible positive effects or make them find ways to circumvent the requirement.[243]

[242] DDPA, art 6(2).
[243] Overby (n 205) 64.

5.5. Appointment of a DPO

The DDPA also does not make use of the opening clause allowing for implementation of supplementary cases where it is mandatory to designate a data protection officer. The general requirements of the Regulation are applicable.

Nonetheless, the national act contains a provision which further specifies the legal framework on data protection officers. Article 24 of the DDPA expressly prohibits DPOs to disclose or exploit, without justification, any personal data which have been obtained in relation to their duties. The provision addresses only the data protection officers under Article 37(b) and (c) of the GDPR, i.e. the ones in the private sector.

IV. Conflict of Laws

The GDPR is undisputedly an omnibus legislation which regulates a broad scope of data protection matters throughout all Member States in a unified way. Nonetheless, considering the review in Section III above, the concerns that the Regulation did not live up to its main aim to fully harmonise data protection law within the EU seem to be substantiated.

Unsurprisingly, Member States are taking advantage of the opportunity to enact laws within the discretion allowed by the opening clauses. However, making the situation even more complicated, national legislators even seem to be enacting rules which might be contradictory to the GDPR. For instance, the approach of the Danish legislator regarding employee's consent (commented in Section III.5.1 above) or the Irish legislator regarding processing of personal data of individuals under 18 years of age for the purposes of direct marketing, profiling, or micro-targeting (commented in Section III.4.4 above).

In such a context, the importance of determining the scope of application of the national data protection law of individual Member States and solving the problem of eventual overlap of

contradictory national provisions is ever growing. Originally, the lack of conflict of laws rules within the GDPR was not supposed to be an issue, had the GDPR fulfilled its initial aim. However, bearing in mind the areas with diverging national data protection legislation, both companies and individuals could be confronted with a serious challenge. Namely, the lack of certainty which law applies – whether it is the law where the data subjects are residing, the law to which the controller is subject, the law of the country where the processing of personal data takes place, or an altogether different law.

Without clear conflict of laws rules, even common day-to-day situations, such as parent companies which have to process data of their subsidiaries' employees across different Member States, or a single company providing services via the Internet to customers from different Member States, could become troublesome. Legal uncertainty as to which Member State's data protection law such companies would be subject to would be quite discomforting, to say the least.

Unlike the GDPR, Article 4 of the Directive (which was fully repealed by the Regulation)[244] expressly provided rules to determine the law of which Member State is applicable. Instead of laying down conflict of laws rules, Article 3 of the Regulation regulates only its territorial scope, i.e., when the processing of personal data by a controller or processor triggers the application of the GDPR. The recitals of the Regulation also do not include guidance for determining applicable national protection provisions.

Certainly, given the legislative nature of the Directive and the expected divergences in national regimes, relying on clear and pre-determined conflict of laws rules was essential for legal certainty. On the other hand, a regulation as a legislative tool applies directly 'as is' and does not per se involve issues of different overlapping national regimes, as there should be one single law.

[244] GDPR, art 94.

However, as already indicated, this is not the case for the GDPR. Considering the significant amount of provisions explicitly providing discretion to Member States to enact their own legislation, it could hardly be imagined that the removal of the guidance on applicable national law in the new data protection regime has been well thought out.

Given the lack of conflict of laws rules in the GDPR, this Section would review and suggest possible solutions to finding the applicable Member State's law.

1. National conflict of laws provisions and opening clauses

The Regulation does not lay down general conflict of laws rules, besides on a number of rare occasions where the wording of the GDPR seems to indicate towards certain Member State law. For example, Article 80(2) of the GDPR provides that the Member State law where the action is brought is applicable,[245] recital 153 of the GDPR provides that the Member State law of the controllers is applicable when derogations differ from one Member State to another, and others. Nonetheless, as useful as these indications might be for certain situations, the majority of opening clauses do not contain clear applicable law guidance, so a comprehensive solution is more than necessary.

Considering the lack of general conflict of laws guidance in the GDPR, on the face of it, it seems that nothing hinders EU Member States from enacting their own national conflict of laws rules in order to determine when their law would be applicable and to fill in the legislative gap.[246] Thus, where Member States have adopted provisions on the territorial applicability of national rules within the opening clauses, the applicable law should be determined pursuant to these

[245] Feiler, Forgó and Weigl (n 13) 520.
[246] Veronika Beimrohr, 'Tagungsbericht: DS-GVO Ante Portas – Zum Stand der Vorarbeiten im Zuge der Datenschutz-Grundverordnung' (2017) 8 jusIT digital exklusiv <https://lesen.lexisnexis.at/_/tagungsbericht-ds-gvo-ante-portas-zum-stand-der-vorarbeiten-im-z/artikel/jusit_digitalonly/2017/44/jusit_digitalOnly_2017_8.html> accessed 26 June 2019.

provisions.[247] A number of countries – for instance, Germany, Austria, and Denmark – have already implemented provisions which explicitly stipulate when their national data protection act applies.[248]

For instance, pursuant to the GFDPA, the act applies to private bodies in any of the following three cases: 1) when the personal data are processed in Germany, 2) the personal data are processed in the context of activities of a German establishment of a controller or processor, or 3) although there isn't an establishment of the controller or processor in a Member State or an EEA state, it falls within the scope of the GDPR.[249] While the first two cases seem clear, the third one is not entirely unproblematic. The third case is supposedly a reference to the targeting criterion under Article 3(2) of the GDPR.[250] However, as its wording is not further specified, the strict interpretation of this provision might lead to some rather odd conclusions. For instance, a US established company, without any kind of establishment in Germany or the EU, which offers goods and services to Italian citizens might be subject to the German data protection act, as it would fall under the scope of Article 3(2)(a) of the Regulation.[251] Of course, such conclusion would not be acceptable. In this case, it remains unclear why the national legislator did not explicitly modify the provision with a reference to Germany.[252] Thus, national legislators should be particularly cautious when drafting the scope of applicability of their domestic data protection acts in order to avoid potential ambiguous interpretation.

[247] Jürgen Kühling and Benedikt Buchner, *Datenschutz-Grundverordnung/BDSG: Kommentar* (2nd end, CH Beck 2018) DS-GVO Art. 3 para 108.
[248] GFDPA, art 1; ADPA, art 3; DDPA, art 4.
[249] GFDPA, art 1(4).
[250] Kühling and Buchner (n 247) BDSG § 1 para 29.
[251] See GDPR, art 3(a); Kühling and Buchner (n 247) BDSG § 1 para 30.
[252] Kühling and Buchner (n 247) BDSG § 1 para 30.

Other potential issues could arise where provisions of different Member States conflict each other or where there is no national provision on territorial applicability.[253] In turn, this might lead to a situation of parallel applicability of national laws (e.g., the controller has to observe both the German and Austrian data protection acts)[254] or to a situation where there aren't any provisions determining the applicable law.

In such cases, it might be helpful to derive additional indications from the wording of the opening clauses, which on a number of occasions seem to suggest which applicable law is.[255] These opening clauses could be divided into two main categories: 1) provisions based on the domicile/establishment principle and 2) provisions based on the territoriality principle.[256]

As regards the first, there are a few GDPR provisions which stipulate that the controller's or processor's law should apply for their particular regulatory area, thus the principle of country of domicile or establishment.[257] For instance, some useful guidance could be found in the text of Article 6(3) of the GDPR which stipulates that the basis for processing personal data pursuant to Article 6(1)(c) and (e) will be determined by 'Member State law to which the controller is subject'.[258] Also, according to recital 153 of the GDPR, when national legislators introduce derogations to reconcile the right to data protection with the right to freedom of expression and information and there is a difference in national law, 'the law of the Member State to which the controller is subject should apply'. Further, Article 14(5)(c) of the GDPR which introduces derogations from the right to information of data subjects also stipulates that the relevant Member

[253] Kühling and Buchner (n 247) DS-GVO Art. 3 para 108.
[254] Paul Voigt and Axel von dem Bussche, *EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch* (Springer-Verlag 2018) 36.
[255] Kühling and Buchner (n 247) DS-GVO Art. 3 para 108.
[256] Philip Laue, 'Öffnungsklauseln in der DS-GVO – Öffnung wohin?' (2016) 10 Zeitschrift für Datenschutz 463, 464.
[257] Ibid.
[258] Kühling and Buchner (n 247) DS-GVO Art. 3 para 108.

State law is 'law to which the controller is subject'.[259] In all of the illustrated cases, for determining applicable law it does not matter where the processing takes place or where the data subject is.[260] What determines the applicable law is where the headquarters of the company is located.[261] In turn, controllers and processors would not have to be faced with the legal uncertainty of applying other Member State's data protection laws which would usually be less known to them.[262]

The second category of opening clauses include an indication for applicable law based on where the processing or the data subject is located, thus the territoriality principle. Such clauses could be found, for instance, in Article 9(2)(b) and (g)-(j) of the GDPR which enables under certain circumstances the processing of special categories of personal data pursuant to a national law of a Member State.[263] Also, Article 49(1)(g) of the GDPR allows for transfers of personal data to a third country, if the transfer has been made from a register intended to provide public information according to Member State law. In these cases, for determining applicable law, it should not be relevant where the controller or processor is located, but rather where the processing takes place or where the data subject is.[264]

The above considerations logically lead to the question what would happen in case national provisions governing the scope of application, on the one hand, and the opening clauses' indications on applicable law, on the other, point out to different Member State laws. The answer to this question should be pretty straightforward, insofar as the GDPR, as a European Union legislative act, takes precedence over national legislation.

[259] Laue (n 256) 464.
[260] Ibid 465.
[261] Ibid.
[262] Ibid.
[263] Ibid.
[264] Ibid.

In summary, it should be noted that relying only on Member State's national conflict of laws provisions and a number of opening clauses containing applicable law is a plausible, but not a comprehensive solution. It might involve many potential issues, such as ambiguous or lacking national provisions on scope of applicability, overlapping national laws, many opening clauses which do not contain indication of applicable law, and others. For instance, in a cross-border processing situation, involving two Member States which have not enacted national rules to determine the scope of applicability of their domestic data protection acts, and where there are no indications on applicable law in the opening clause (e.g., child's consent under Article 8 of the GDPR), legal uncertainty would inevitably arise. Therefore, this thesis will expand on the conflict of laws issues with other possible solutions.

2. Rome I Regulation and Rome II Regulation

Next, it is worth elaborating whether the general conflict of laws rules in the Rome I Regulation[265] and Rome II Regulation[266] could provide further answers. The former regulates applicable law in contractual obligations in civil and commercial matters, and the latter regulates non-contractual obligations (including tortious claims).

As regards contractual obligations, even though the GDPR does not state explicitly what its connection with the Rome I Regulation is, on the face of it, it does not seem that its application could be completely excluded. For instance, in a situation where a company established in one Member State directs its activities towards consumers with habitual residence in another Member State, the law of the latter would be applicable pursuant to Article 6(1) of Rome I Regulation. In this case, the company would inevitably have to consider the age threshold for valid digital consent

[265] 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 L177/6 (hereinafter Rome I Regulation).
[266] 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 [2007] OJ L199/40 (hereinafter Rome II Regulation).

of the Member State to which it directs its activities and other potentially diverging areas of national law.[267]

Where Article 6(1) is not applicable, another important provision from the Rome I Regulation which has to be considered is Article 4, and especially Article 4(1)(b) which stipulates which law governs a contract for the provision of services.[268] Thereunder, it is the service provider's (thus the controller's) habitual residence which determines applicable law. What exactly services are is not defined. Nevertheless, the concept should be interpreted broadly, involving activities related to offering of services, irrespective of whether payment is required.[269]

Applying the regime of the Rome I Regulation to data protection law, however, is also challenging on certain occasions. An example of such a situation would be the case where a US-established service provider directed its activities only to children in the Republic of Ireland, but children in Germany also used the service.[270] Both the processing of the personal data of the Irish and the German children would be governed by the GDPR.[271] However, under Rome I Regulation different rules would be applicable. On the one hand, due to the directing of activities, the processing of the personal data of the Irish children would be under Article 6(1) of the Rome I Regulation, thus Irish law would apply. On the other hand, since there is no directing of activities, Article 4(1)(b) of the Rome I Regulation would be applicable for the children in Germany, i.e. the law of the US-established service provider should apply. However, as already established, in this case the GDPR's norms are applicable pursuant to Article 3(2)(a). Therefore, the non-EU Member State law could not be applied and the 16 years age threshold for digital consent under Article 8

[267] Laue (n 256) 466.
[268] Ibid.
[269] Ibid.
[270] Ibid.
[271] GDPR, art 3(2)(a).

of the GDPR would be applicable.[272] In summary, although providing further answers to the conflict of laws issues, adapting the Rome I Regulation to the new data protection framework seems like a challenging task.

As regards the Rome II Regulation, it is unlikely that its regulation on tortious claims could be applied at all. Sound arguments have been put forward in the law literature according to which due to the explicit exclusion of 'non-contractual obligations arising out violations of privacy and rights relating to personality, including defamation'[273] from its scope, it cannot be applied for personal data matters.[274] A possible solution in this regard could be to determine applicable law based on national law provisions where the action is decided.[275]

In light of the above, even if general EU conflict of laws rules under the Rome I Regulation would be applied to remedy the situation, it still seems that many issues would be left without a uniform EU-wide decision and thus uncertainty regarding applicable law.

3. Analogy to the rules for determining lead supervisory authority

Despite the lack of general conflict of laws guidance, the GDPR has established a comprehensive mechanism to determine which the lead supervisory authority is in case of cross-border processing[276] carried out by a controller or a processor.[277] These rules identify the supervisory authority of which Member State will be competent in case of cross-border processing, and do not expressly regulate the choice of law.[278]

---

[272] Laue (n 256) 466.
[273] Rome II Regulation, art 1(2)(g).
[274] Feiler, Forgó and Weigl (n 13) 577; Maja Brkan, 'Data Protection and Conflict-of-Laws: A Challenging Relationship' (2016) 2(3) European Data Protection Law Review 324, 330.
[275] Brkan (n 274) 337.
[276] See GDPR, art 4(23).
[277] GDPR, art 56.
[278] Katie Nolan, 'GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law' (2018) Berkeley Technology Law Journal <http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/#_edn10> accessed 11 June 2019.

Nevertheless, the authors of 'The EU General Data Protection Regulation (GDPR): A Commentary' have suggested that the rules on competence of the lead supervisory authority within the meaning of Article 56 of the GDPR could be applied by legal analogy in order to determine applicable national law.[279]

After pointing out that the lack of conflict of laws general guidance is a 'remarkable shortfall of the GDPR', the authors search for a plausible solution on the basis of EU law, within the internal logic of the Regulation, in order to remedy the identified gap.[280] First, it is considered that the absence of conflict of laws regulation is unintended only when there is a lead supervisory authority within the meaning of Article 56(1) of the GDPR, as these cases involve cross-border processing subject to the GDPR.[281] Whereas when there is no lead supervisory authority and no cross-border processing, it is a matter of national law to stipulate which Member State's law applies.[282] Second, it has been taken into account that from the wording of Article 65(1)(a) of the GDPR it could be concluded that the EDPB has to determine applicable national law as a preliminary question when issuing a binding decision under the said provision.[283]

Thus, according to the proposed solution, whenever there is cross-border processing regulated by the GDPR and a lead supervisory authority of a controller or a processor, the national law of the latter should be applied.[284] In these cases, however, it should be considered also whether the derogations under Article 56(2) of the GDPR apply, i.e. whether another Member State's law could be applicable.[285] This would be the case where a complaint or infringement: 1) concerns

[279] Feiler, Forgó and Weigl (n 13) 575-577.
[280] Ibid.
[281] Ibid 576-577.
[282] Ibid 577.
[283] Ibid 483, 577.
[284] Ibid 577.
[285] Ibid.

only the establishment in another Member State and 2) substantially affects data subjects only in another Member State (different from the lead competence).[286]

The authors have also suggested that, as an exception, regarding employment law, the applicable Member State law should be determined pursuant to the Rome I Regulation,[287] but their general idea is to remedy the identified gap with the legal analogy discussed above.

The suggested approach should be supported. It follows the internal logic of the new data protection framework and it proposes a comprehensive solution based on EU law as opposed to a patchwork of different national laws (which might have many negative implications, as discussed in Section IV.1 above). It remains to be seen whether the CJEU would follow the same direction.

V. Conclusion

The number of opening clauses in the GDPR is so significant that sometimes it is being referred to as a 'hybrid between a Regulation and a Directive'.[288] As the overview of the opening clauses in Section II of this thesis has shown, these flexibilities are indeed too many. This fact alone is enough to threaten the aims of the new data protection regime for establishing a uniform data protection framework in the EU and for eliminating the fragmentation and differences in the level of protection of data subjects.

Further, considering the comparative review of the five national GDPR implementation laws in Section III of this thesis, Member States are actively legislating within the opening clauses, thereby creating their own data protection peculiarities and nuances, even regarding some of the most common day-to-day business activities. To complicate matters even further, when specifying

[286] GDPR, art 56(2).
[287] See Feiler, Forgó and Weigl (n 13) 577.
[288] European Digital Rights, 'Proceed With Caution: High Risk Flexibilities in the General Data Protection Regulation' (*EDRi*, 11 July 2016) 2 <https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities_summary.pdf> accessed 11 June 2019.

the requirements of the GDPR, some Member States have implemented provisions whose compatibility with the Regulation is questionable. In turn, this results in the fragmentation of data protection law, legal uncertainty and obstacles to the free flow of personal data within the Union.

Another conclusion from the comparative review is that the differences in the approach of the Member States under the previous data protection regime could also be noticed under the new regime. National legislators with long established traditions, such as Germany, have adopted a comprehensive approach, taking advantage of many of the opening clauses and re-enacting some of their previous legislation. Whereas other Member States have chosen a more modest approach and have not provided for many deviations of the GDPR.

It should be noted that both of these approaches have their positive and negative sides. On the one hand, implementing more opening clauses is a valuable tool for national legislators. It provides, in particular, the necessary flexibility to align and reconcile potential conflicts between data protection law and other areas of law (e.g., employment, healthcare, freedom of expression, etc.) and to partially re-enact previous data protection legislation. A smoother transition to the new data protection regime and a well-adapted national legal framework without conflicts between different areas of law could be outlined as potentially positive implications of this approach. On the other hand, the more the Member States use the flexibilities provided by the GDPR, the more fragmented the EU data protection legal framework will be. Nevertheless, not taking advantage of the opening clauses might have negative effects on the domestic legal framework, in particular as regards the interplay of data protection with other areas of law.

While the persistence of inconsistencies across data protection regimes in the Union is a problem on its own, it seems further exacerbated by the decision of the EU legislator to remove the general conflict of laws guidance which existed under the Directive. The areas of diverging

national law and the lack of comprehensive conflict of laws rules create a troubling legal uncertainty for cross-border situations. Possible solutions to this issue have been suggested in the law literature, such as analogy to the rules for determining lead supervisory authority, relying on general EU conflict of laws rules (e.g., Rome I Regulation), relying on national conflict of laws rules, or derived from applicable law indications in certain opening clauses. However, it still remains to be seen whether the CJEU or the EDPB would support these or other solutions. It is therefore crucial that this legal uncertainty is urgently dealt with at the EU level.

In light of the above, it could be concluded that the GDPR did not fully attain its aims to establish a uniform data protection framework, which provides equivalent level of data protection and removes the obstacles to flows of personal data within the EU. While an improved consistency in the level of data protection has undoubtedly been achieved, it is also certain that the fragmentation of data protection across the EU has not been fully prevented and a new conflict of laws issue has arisen. It remains to be seen whether further guidance of the EDPB or CJEU case law would clarify the conflict of laws concerns and address problematic national provisions contrary to the GDPR.

BIBLIOGRAPHY

Works Consulted

Baker McKenzie, 'GDPR National Legislation Survey 2018' (*Baker McKenzie*, January 2018) <www.bakermckenzie.com/-/media/minisites/tmt/files/gdpr_national_legislation_survey.pdf?la=en> accessed 11 June 2019

Beimrohr V, 'Tagungsbericht: DS-GVO Ante Portas – Zum Stand der Vorarbeiten im Zuge der Datenschutz-Grundverordnung' (2017) 8 jusIT digital exklusiv <https://lesen.lexisnexis.at/_/tagungsbericht-ds-gvo-ante-portas-zum-stand-der-vorarbeiten-im-z/artikel/jusit_digitalonly/2017/44/jusit_digitalOnly_2017_8.html> accessed 26 June 2019

Bird & Bird, 'GDPR Tracker: Austria' (*Bird & Bird*) <www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/austria> accessed 11 June 2019

Bird & Bird, 'GDPR Tracker: Denmark' (*Bird & Bird*) <www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/denmark> accessed 11 June 2019

Bird & Bird LLP, 'The Danish Data Protection Act Has Been Passed!' (*Lexology*, 8 June 2018) <www.lexology.com/library/detail.aspx?g=6098ea81-516f-4bf8-a566-5678551f546c> accessed 11 June 2019

Brkan M, 'Data Protection and Conflict-of-Laws: A Challenging Relationship' (2016) 2(3) European Data Protection Law Review 324

Cahir J, 'Ireland passes Data Protection Act 2018' (*A&L Goodbody*, 25 May 2018) 4 <www.algoodbody.com/images/uploads/services/EU-Data-Protection/Irish_Government_Published_DP_Act_2018.pdf> accessed 11 June 2019

Chen J, 'How the Best-Laid Plans Go Awry: The (Unsolved) Issues of Applicable Law in the General Data Protection Regulation' (2016) 6(4) International Data Privacy Law 310

DLA Piper, 'Data Protection Laws of the World: Data Protection Officers: Austria' (*DLA Piper*, 10 January 2019) <www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=AT> accessed 11 June 2019

DLA Piper, 'Data Protection Laws of the World: Law: Bulgaria' (*DLA Piper*, 10 January 2019) <www.dlapiperdataprotection.com/index.html?t=law&c=BG> accessed 11 June 2019

DLA Piper, 'EU General Data Protection Regulation - Background' (*DLA Piper*) <www.dlapiper.com/en/austria/focus/eu-data-protection-regulation/background/> accessed 11 June 2019

European Digital Rights, 'Proceed With Caution: Flexibilities in the General Data Protection Regulation' (*EDRi*, 5 July 2016) <https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf> accessed 11 June 2019

European Digital Rights, 'Proceed With Caution: High Risk Flexibilities in the General Data Protection Regulation' (*EDRi*, 11 July 2016) <https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities_summary.pdf> accessed 11 June 2019

Feiler L, 'Öffnungsklauseln in der Datenschutz-Grundverordnung - Regelungsspielraum des österreichischen Gesetzgebers' (2016) 5 jusIT <https://lesen.lexisnexis.at/_/oeffnungsklauseln-in-der-datenschutz-grundverordnung-regelungssp/artikel/jusit/2016/5/jusIT_2016_05_093.html> accessed 15 June 2019

Feiler L, Forgó N and Weigl M, *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business 2018)

Felz D, 'An English-Language Primer on Germany's GDPR Implementation Statute: Part 4 of 5' (*Alston & Bird LLP*, 10 October 2017) <www.alstonprivacy.com/english-language-primer-germanys-gdpr-implementation-statute-part-4-5/?cn-reloaded=1> accessed 11 June 2019

Fessenko D, 'Bulgaria Plans to Introduce a Range of Derogations From the EU General Data Protection Regulation' (*Lexology*, 18 May 2018) <www.lexology.com/library/detail.aspx?g=8a42dc5b-756c-49f1-9aef-9b1ceea600ed> accessed 11 June 2019

Gabel D and Hickman T, 'Chapter 17: Issues Subject to National Law – Unlocking the EU General Data Protection Regulation' (*White & Case LLP*, 5 April 2019) <www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection> accessed 11 June 2019

Geminn C, 'The New Federal Data Protection Act – Implementation of the GDPR in Germany' (*Blogdroiteuropéen*, June 2018) <https://blogdroiteuropeen.files.wordpress.com/2018/06/christian-1.pdf> accessed 11 June 2019

Holt K, 'Analysis: The Danish Data Protection Act and Its GDPR Derogations' (*IAPP*, 18 December 2018) <https://iapp.org/news/a/analysis-the-danish-data-protection-act-and-its-gdpr-derogations/> accessed 11 June 2019

International Association of Privacy Professionals, 'EU Member State GDPR Implementation Laws and Drafts' (*IAPP*) <https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/> accessed 11 June 2019

IT Governance Europe, 'Data Protection Act (DPA) Ireland 2018' (*IT Governance Europe*) <www.itgovernance.eu/en-ie/data-protection-ie> accessed 11 June 2019

Kühling J and Buchner B, *Datenschutz-Grundverordnung/BDSG: Kommentar* (2nd end, CH Beck 2018)

Laue P, 'Öffnungsklauseln in der DS-GVO – Öffnung wohin?' (2016) 10 Zeitschrift für Datenschutz 463

Leissler G, Reisinger P and Böszörmenyi J, 'Austrian Adaptation of the GDPR' in Olivia Tambou, Karen Mc Cullagh and Sam Bourton (eds), *National Adaptations of the GDPR* (Collection Open Access, Blogdroiteuropéen 2019) 35 <https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf> accessed 11 June 2019

Leissler G and Wolfbauer V, 'Austria: (De)Regulatory Affairs or the Delegates' Proposal for Altering the National Data Protection Act' (*Lexology*, 17 April 2018) <www.lexology.com/library/detail.aspx?g=bd1bd5ba-48b8-40e7-995d-8560fedf094d> accessed 11 June 2019

Management Board of the Association of the Bulgarian Journalists, 'Attack Against the Freedom of Speech' (Press Release, 25 January 2019) <www.sbj-bg.eu/index.php?t=41677> accessed 11 June 2019

McCarthy H, 'Part I: The GDPR, Freedom of Expression and a Right to Remember?' (2018) 11(3) Data Protection Ireland 5

Nolan K, 'GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law' (2018) Berkeley Technology Law Journal <http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/#_edn10> accessed 11 June 2019

Overby T, 'The Danish Adaptation of the GDPR' in Olivia Tambou, Karen Mc Cullagh and Sam Bourton (eds), *National Adaptations of the GDPR* (Collection Open Access, Blogdroiteuropéen 2019) 61 <https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf> accessed 11 June 2019

Pavel V, 'European Commission Urged to Investigate Romanian GDPR Implementation' (*GDPR Today*, 3 July 2017) <www.gdprtoday.org/european-commission-urged-to-investigate-romanian-gdpr-implementation/> accessed 11 June 2019

Pormeister K, 'Genetic Research and Applicable Law: The Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-Border Genetic Research' (2018) 5(3) Journal of Law and the Biosciences 706

Rustad M and Kulevska S, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28(2) Harvard Journal of Law & Technology 349

Schutz A and Polzl J, 'Austria's Struggle With the GDPR' (*CEE Legal Matters*, 1 August 2018) <https://ceelegalmatters.com/austria/8977-austria-s-struggle-with-the-gdpr> accessed 11 June 2019

Schüßler L and Karniyevich N, 'Germany Is the First EU Member State to Enact New Data Protection Act to Align With the GDPR' (*Bird & Bird*, July 2017) <www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr> accessed 11 June 2019

Spies A, 'Germany Enacts GDPR Implementation Law' (*Lexology*, 6 June 2018) <www.lexology.com/library/detail.aspx?g=5f6cf3a2-56de-4484-beba-d6b20047e452> accessed 11 June 2019

Stoeckle T, 'GDPR – Much Ado About Nothing, or the End of the World As We Know It?' (*The Small Data Forum Podcast*, 11 June 2018) <www.smalldataforum.com/2018/06/11/gdpr-much-ado-about-nothing-or-the-end-of-the-world-as-we-know-it/> accessed 10 June 2019

Tambou O, 'Opening Remarks to the E-Conference on the National Adaptations of the GDPR' (*Blogdroiteuropéen*, 4 June 2018) <https://blogdroiteuropeen.com/2018/06/04/opening-remarks-to-the-e-conference-on-the-national-adaptations-of-the-gdpr-by-olivia-tambou/> accessed 11 June 2019

Voigt P and von dem Bussche A, EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch (Springer-Verlag 2018)

Voigt P and von dem Bussche A, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer International Publishing AG 2017)

Wybitul T, 'New Requirements for Data Protection Officers in Germany' (2011) 16 Business & Technology Sourcing Review 19 <www.mayerbrown.com/en/perspectives-events/publications/2011/06/new-requirements-for-data-protection-officers-in-g> accessed 11 June 2019

EU and Member States Institutions' Documents and Press Releases
European Union

Article 29 Data Protection Working Party, 'Guidelines on Consent Under Regulation 2016/679' (28 November 2017 revised on 10 April 2018) WP 259 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030> accessed 11 June 2019

Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/679' (29 November 2017 revised on 11 April 2018) WP 260 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025> accessed 11 June 2019

European Commission, ‘Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users’ Control of Their Data and to Cut Costs for Businesses' (Press Release, 25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> accessed 10 June 2019

European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)’ COM (2012) 011 final

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

European Commission, 'The General Data Protection Regulation (GDPR) is Now Applicable. Are You Ready for It?' (*European Commission,* 25 May 2018) <https://ec.europa.eu/easme/en/news/general-data-protection-regulation-gdpr-now-applicable-are-you-ready-it> accessed 10 June 2019

Austria

Austrian Parliament, 'Nationalrat: Umfassende Datenschutzanpassungen Samt ELGA-Datenschutz-Entschließung für Registerforschung: Opposition Setzt Verbandsklagerecht Nicht Durch, Keine Zwei-Drittel-Mehrheit für Alleinige Zuständigkeit des Bundes im Datenschutz' (Press Release 442, 20 April 2018) <www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0442/> accessed 11 June 2019

Austrian Parliament, ‘Nationalrat Verabschiedet Umfangreiche Novelle zum Datenschutzgesetz: Opposition Kritisiert Tempo des Gesetzgebungsprozesses' (Press Release 829, 29 June 2017) <www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0829/> accessed 11 June 2019

Austrian Parliament, 'Neu im Verfassungsausschuss: Regierung Legt Neues Datenschutzgesetz Vor' (Press Release 736, 16 June 2017) <www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0736/> accessed 11 June 2019

Bulgaria

Bulgarian Commission for Personal Data Protection, ‘CPDP adopted a list of the types of processing operations for which data protection impact assessment is required ' (Press Release, 13 February 2019) <www.cpdp.bg/?p=news_view&aid=1370> accessed 11 June 2019

Bulgarian Commission for Personal Data Protection, ‘The Act for Amending and Supplementing the Bulgarian Personal Data Protection Act was promulgated’ (Press Release, 26 February 2019) <www.cpdp.bg/?p=news_view&aid=1373> accessed 11 June 2019

Bulgarian Parliament, Draft Bill Act for Amending and Supplementing the Bulgarian Personal Data Protection Act <www.parliament.bg/bills/44/802-01-27.pdf> accessed 11 June 2019

Bulgarian Parliament, Draft Bill Bulgarian Personal Data Protection Act <www.parliament.bg/bills/39/154-01-23.pdf> accessed 11 June 2019

Bulgarian President, 'The President Vetoed a Provision of the Act for Amending and Supplementing the Bulgarian Personal Data Protection Act' (Press Release, 4 February 2019) <www.president.bg/news4798/prezidentat-nalozhi-veto-varhu-razporedba-ot-zakona-za-izmenenie-i-dopalnenie-na-zakona-za-zashtita-na-lichnite-danni.html > accessed 11 June 2019

Ireland

Explanatory Memorandum to the Data Protection Act 2018 <www.justice.ie/en/JELR/Data_Protection_Act_2018_Explanatory_Memorandum.pdf/Files/Data_Protection_Act_2018_Explanatory_Memorandum.pdf> accessed 11 June 2019

Irish Data Protection Commission, 'Data Protection Legislation: Key Data Protection Legislative Frameworks Applicable From 25 May 2018' (*Data Protection Commission*) <www.dataprotection.ie/en/legal/data-protection-legislation> accessed 11 June 2019

Irish Parliament (Oireachtas), 'Data Protection Act 2018: History of this Act' (Irish Parliament, 24 May 2018) <www.oireachtas.ie/en/bills/bill/2018/10/> accessed 11 June 2019

Irish Parliament (Oireachtas), Data Protection (Amendment) Bill 2018 Dáil Éireann Debate 29 November 2018 <www.oireachtas.ie/en/debates/debate/dail/2018-11-29/18/> accessed 11 June 2019 (hereinafter Dáil Éireann Debate 29 November 2018)

Denmark

Danish Parliament, Legal Affairs Committee, Report from 9 May 2018 <www.retsinformation.dk/Forms/R0710.aspx?id=201193> accessed 11 June 2019