National adaptations of the GDPR

Karen Mc Cullagh, Olivia Tambou, Sam Bourton

NATIONAL ADAPTATIONS OF THE GDPR

This book explores the impact of the General Data Protection Regulation (GDPR), in ten Member States (Austria, Denmark, France, Germany, Ireland, Italy, Netherlands, Spain, Sweden, and the United Kingdom including comments on Brexit situation) and its international influence in Switzerland and Japan. Eight months after the entry into force of the GDPR, this book analyses the tension between the visibility of the European Model and the readability of this model. This book provides insights and commentary on derogation and option differences between Member States. It outlines the issues most contested when national legislatures were drafting and implementing Bills to give effect to permitted derogations in the GDPR. Furthermore, this book questions to what extent the diversity of approach of national adaptations raises concerns regarding their conformity to the GDPR.

This book is the result of an international cooperation launched through an e-conference organised by blogdroiteuropeen in June 2018. It brings together papers from seventeen legal academics or practitioners (lawyers, Data protection officers, and Data Protection authority representatives). It is the second digital book of the Series Open Access Book edited by blogdroiteuropeen.

Dr Karen Mc Cullagh is a Lecturer in Law at the University of East Anglia.
Dr Olivia Tambou is an Assocate Professor at the University Paris-Dauphine, PSL Research University.
Sam Bourton is a PhD candidate and Lecturer in Law at the University of the West of England.

Collection Open Access Book
edited by Olivia Tambou

https://blogdroiteuropeen.com

ISBN 978-2-9199563-0-2

COLLECTION OPEN ACCESS BOOK
EDITED BY DR. OLIVIA TAMBOU

E-CONFERENCE

NATIONAL ADAPTATIONS OF THE GDPR

Edited by Dr. Karen McCullagh, Dr. Olivia Tambou and Sam Bourton

Blog Droit Européen

Bibliographic reference:

Mc Cullagh K., Tambou O., Bourton S. (Eds.), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg February 2019, 130 pages
Available at: https://wp.me/p6OBGR-3dP

Other books in this series:

Olivia Tambou, Sam Bourton (Eds.), *The Right to be Forgotten in Europe and Beyond/ Le droit à l'oubli en Europe et au-delà* (Series Open Access Book, Blogdroiteuropéen 2018)

Available at : https://wp.me/p6OBGR-2QK
Disponible sur Internet : https://wp.me/p6OBGR-2QK

ISBN 978-2-9199563-0-2

National Adaptations of the GDPR

Collection Open Access Book

Edited by Dr. Olivia Tambou

Edited by Dr. Olivia Tambou, Dr. Karen Mc Cullagh and Sam Bourton

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Agency)
AIQ	AggregateIQ Data Services Ltd
APEC	Asia-Pacific Economic Cooperation
APLOPD	Spanish LOPD Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
APPI	Act on the Protection of Personal Information
APPIHAO Held	Act on the Protection of Personal Information by Administrative Organs
APPI-IAA	Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.
ARCO Rights	Rights of access, rectification, cancellation or objection
Art.	Article
BCRs	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BfDI	Bundesbeauftrage für den Datenschutz und die Informationsfreiheit
BNDG	Bundesnachrichtendienstgesetz
BR	Bundesrat
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgrichts
BVerfSchG	Bundesverfassungsschutzgesetz
CC	Constitutional Council
CCTV	Closed-Circuit Television
CDC	Cartel Damage Claims
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale Informatique et Libertés (French Data Protection Authority)
CPR	Civil Registration System
DI	The Datainspektion

LIST OF ABBREVIATIONS

DNSB	Danish Neonatal Screening Biobank
DPA	Data Protection Authority
DPA	Data Protection Act
DPC	Irish Data Protection Commission
DPO	Data Protection Officer
Drs.	Drucksache
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DuD	Datenschutz und Datensicherheit
EC	European Commission
EC	European Community
ECJ	European Court of Justice
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
Eds	Editors
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
e.g.	For example
EPA	EU-Japan Economic Partnership Agreement
et. seq.	et sequentia.
EU	European Union
FADP	Federal Act on Data Protection
FAQ	Frequently Asked Questions
FDPIC	Federal Data Protection and Information Commissioner
FLFE	Swedish Fundamental Law on Freedom of Expression
Fn.	Footnote
FPA	Freedom of the Press Act
FTE	Full-time Employees
G 10	Artikel 10-Gesetz

LIST OF ABBREVIATIONS

GCHQ	Government Communications Headquarters
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GYou	Google You Owe Us
GVBl.	Gesetz- und Verordnungsblatt
HDSG	Hessisches Datenschutzgesetz
Ibid	In the same place/ in the same source
Ibidem	in the same place/ in the same source
ICO	Information Commissioner's Office
i.e. id est	In other words
ISS	Information Society Service
JCHR	Joint Committee on Human Rights
LED	Law Enforcement Directive
LIL	French Personal Data Protection Act also called Loi Informatique et Libertés
lit.	letter
LOPD	The Organic Law 15/1999, of 13 December, of Data Protection
LOPDGDD	The Spanish Organic Law 3/2018 for the Protection of Personal Data and for the granting of digital rights
LORTAD	The Organic Law 5/1992, of 29th October, of the Automated Treatment of Data
LT	Landtag
MADG	Gesetz über den Militärischen Abschirmdienst
NDPA	French New Data Protection Act
NOYB	(My Privacy is) None of Your Business
OECD	Organisation for Economic Cooperation and Development
OIPC	Office of the Information and Privacy Commissioner of British Columbia
OJ L	Official Journal Legislation
Ord.	Ordonnance
PIA	Privacy Impact Assessment

LIST OF ABBREVIATIONS

p., pp.	page, pages
para.	paragraph
PDA	Personal Data Act
PDeCAT	Mixed Parliamentary Group
PDO	Personal Data Ordinance
PPC	Personal Information Protection Commission
RLOPD	Regulation of Development, Royal Decree 1720/2007, of 21st December, which approved the Regulation implementing the LOPD
RSM	Regulation on Security Measures for automated files that contain personal data
RTBF	Right To Be Forgotten
SCCs	Standard Contractual Clauses
SME	Small and Medium-Sized Enterprises
SÜG	Sicherheitsüberprüfungsgesetz
TCA 2003	Telecommunications Act 2003
TDs	Members of the Irish lower house of parliament, Dáil Éireann
TFEU	Treaty on the Functioning of the European Union
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UK	United Kingdom
UKlaG	Unterlassungsklagengesetz Law on Actions for Injunctive Relief
ZD	Zeitschrift für Datenschutz

INTRODUCTION TO THE EDITORS

Dr. Olivia Tambou
Associate Professor at the Université Paris-Dauphine, PSL Research University, Cr2D. For correspondence: olivia.tambou@dauphine.fr

Dr. Olivia Tambou is an Associate Professor at the Paris-Dauphine University specialized in European Law. She is also an External Scientific Fellow at the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law. She has been lecturing in French and foreign Universities for more than 20 years. Her current research interest is the effectiveness of the European data protection Law. She wrote several articles on the General Data Protection Regulation (GDPR) about certification, remedies, profiling and the de-listing right. She is a contributor to the comparative section of the European Data Protection Law (EDPL) Journal regarding data protection issues in France . She is also the editor of blogdroiteuropeen. Olivia Tambou has a LLM from Kiel Albrecht University (Germany) and a PhD in European Law from the Law faculty of Strasbourg University. She received a Marie Curie Scholarship from the European Commission for her post-doctoral research at the Universitat Autònoma of Barcelona. Her main scientific interest lies in legal pluralism (relationships between state legal orders in the EU, transfrontier cooperation, harmonisation, regulation).

Dr. Karen Mc Cullagh
Lecturer in Law, University of East Anglia.
For correspondence: k.mccullagh@uea.ac.uk

Dr. Karen Mc Cullagh is a Lecturer in Law at the University of East Anglia where she is also Course Director for the LLM in Media Law, Policy & Practice. Her research specialism is information rights: both the commercial and fundamental rights aspects of privacy and data protection and Freedom of Information, as an aspect of public law.

Sam Bourton
Lecturer in Law, University of the West of England. For correspondence: sam.bourton@uwe.ac.uk

Sam Bourton is a Lecturer in Law and PhD candidate at the University of the West of England. She lectures on several undergraduate and postgraduate modules including, Foundations for Law, Law of Financial Crime and Regulation, and International Financial Crime. Her research focuses on the law of financial crime, particularly tax evasion and money laundering, and she has written several articles on these topics.

INTRODUCTION TO THE CONTRIBUTORS

Mag. Janos Böszörmenyi

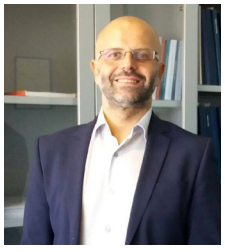
Janos Böszörmenyi has been an associate with Schoenherr Attorneys at Law since December 2017 and is part of the regulatory practice group. Janos' main areas of practice are data protection, telecom and gambling law. Janos graduated from University of Vienna (Mag. iur., 2010) and completed exchange semesters at the Université de Genève (2010) and the Hebrew University of Jerusalem (2015-2016 as part of his still ongoing PhD studies). Before joining Schoenherr, Vienna, he worked as an associate at a Viennese public law firm with a special focus on procurement and gambling law. Janos worked as a researcher for the "Centre for Computers and Law" at the University of Vienna and has published on issues relating to tracking of financial transactions, money laundering, terrorist financing and data protection.

Paul Breibarth

Director of Strategic Research and Regulator Outreach at Nymity Inc., and Senior Visiting Fellow at Maastricht University's European Centre on Privacy and Cybersecurity.

François Charlet

DPO and Lawyer specialising in IT Law.



Dr. Massimo Durante

Massimo Durante is Associate Professor in Philosophy of Law and Legal Informatics at the Department of Law, University of Turin. He holds a Ph.D. in Philosophy of Law, Department of Law, University of Turin, and a Ph.D. in Moral Philosophy, Faculty of Philosophy, Paris IV Sorbonne. Author of several books, he has widely published papers in Italian, English and French. Faculty Fellow of the Nexa Center for Internet and Society at the Politecnico of Turin, he is member of the Board of the Joint International Doctoral Degree in "Law, Science, and Technology". His main interests are law and technology, information ethics, internet governance, privacy and data protection law, AI & law.

Christian L. Geminn

Dr. jur. Christian L. Geminn is a Senior Researcher and Managing Director of the Project Group Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG) at Kassel University, Germany. The project group carries out interdisciplinary research projects on the legal issues arising from the use of information and communication technology and has been doing so since 1988. The research center was founded in 2005 and focuses on a socio-technical perspective on the design of information technology.

INTRODUCTION TO THE CONTRIBUTORS

Dr. Patricia Jonason

Dr. Patricia Jonason is an Associate Professor in Public Law at Södertörn University, Stockholm, Sweden. She teaches administrative and constitutional law as well as European law and Human Rights. Her current main research interests are on privacy and on the right of access to information as well as on the principles of good administration.

Dr. Günther Leissler LL.M.

Counsel at Schoenherr Attorneys at Law

Dr Karen Mc Cullagh

Dr Karen Mc Cullagh is a Lecturer in Law at the University of East Anglia where she is also Course Director for the LLM in Media Law, Policy & Practice. Her research specialism is information rights: both the commercial and fundamental rights aspects of privacy and data protection and Freedom of Information, as an aspect of public law.

Hiroshi Miyashita

Associate Professor, LL.D., Chuo University, Tokyo, JAPAN. Hiroshi Miyashita specializes constitutional law, comparative constitutional law, information law. He previously worked at the Office of Personal Information Protection for the international cooperation in the Cabinet Office of Japan. He has published five books on data privacy in Japanese, including commentary on the GDPR.

Dr. Maria Murphy

Dr. Maria Helen Murphy is a Lecturer in Law at Maynooth University. Her research interests include privacy law, surveillance, data protection, information technology law, and human rights. She recently published a new book, Surveillance and the Law: Language, Power and Privacy (2019).

Tenna Overby

Head of Section, POLITI, Danish National Police, Police Directorate, Data Protection Unit

INTRODUCTION TO THE CONTRIBUTORS

Dr. Alexia Pato

Dr. Alexia Pato holds a PhD in Law from the Universidad Autónoma de Madrid. Her thesis dealt with jurisdiction-related issues in cross-border collective redress cases. She currently works as a Senior Research Fellow in Private International Law at the University of Bonn.

Dr. Cristina Pauner

Cristina Pauner is Associate Professor in Constitutional Law at the Public Law Department of the Universitat Jaume I (Castellón de la Plana, Spain), since 2002. She has been visitor researcher in European centres and universities such as the Universitè Paris-Sorbonne, Università degli Studi Roma III, London School of Economics and University of Oxford. She has completed several specialization courses on human rights at the International Human Rights Institute (Strasbourg) as well as the specialization Diploma in Constitutional Law and Political Science at the Centre for Political Studies and Constitutional (Madrid).

She is currently developing her lines of research in several human rights groups and, especially, on personal data protection. She participates as a researcher in the project on «The impact of the new European Data Protection Regulation: National and Comparative Analysis» financed by the Ministry of Economy and Competitiveness. She has been part of the research team of the European project PHAEDRA II. Improving practical and helpful cooperation Between Data Protection Authorities II) financed by the European Commission (Directorate General of Justice) and has coordinated the European project «CRISP. Evaluation and Certification schemes for Security products «funded by the European Union (7th Framework Programme).

Her research interests include human rights, gender equality, privacy and press freedom; personal data protection; open access, intellectual property rights, rights of political participation; and freedom or rights of emigrants.

By Mag. Patrizia Reisinger

Associate at Schoenherr Attorneys at Law

Monica A. Senor

Former criminal lawyer specializing in privacy, data protection, ICT law and digital forensics, Monica A. Senor is a member of the staff of the Italian Supervisory Authority (Garante per la protezione dei dati personali) since December 2018. She is fellow of the Nexa Center for Internet & Society at the Politecnico di Torino (DAUIN), an independent research center focusing on interdisciplinary analysis of the force of the Internet and of its impact on society. She is the author or co-author of many publications, including online reviews (Medialaws.eu, ictsecuritymagazine.com, AgendaDigitale.eu), scientific journals and law textbooks (edited by the following publishing houses: Egea, Giappichelli, Springer, UTET Giuridica, and Aracne).

INTRODUCTION TO THE CONTRIBUTORS

Dr Olivia Tambou

Olivia Tambou is an Associate Professor at the Paris-Dauphine University where she specialises in European Law. She is also an External Scientific Fellow at the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law. She has written several articles on the General Data Protection Regulation (GDPR) about certification, remedies, profiling and the de-listing right. She is a contributor to the comparative section of the European Data Protection Law (EDPL) Journal on data protection issues in France. She is also the editor of blogdroiteuropeen.

Jorge Viguri

Jorge Viguri is a PhD researcher in Constitutional Law at the Universitat Jaume I of Castellón (UJI). He has a Master´s Degree in Legal Practice (2014-2016) and participated in two EU projects (CRISP and PHAEDRA II). He widened his studies at the International Institute of Human Rights in Strasbourg (2016), and the Poznań Human Rights Centre (2017) and the Swiss Institute of Comparative Law (2018). His scientific production focuses on privacy and data protection including certification schemes and new challenges on asylum seekers/refugees.

ACKNOWLEDGEMENTS

The editors would like to acknowledge the help of all the people involved in producing this book. Specifically, the editors would like to thank each one of the authors who contributed their time and expertise to their chapter contributions.

The editors also wish to acknowledge the valuable contributions of the reviewers whose feedback improved the quality, coherence, and content of chapters.

Finally, the editors wish to thank Olivia for conceiving of and commissioning this e-book, to Olivia and Karen for recruiting authors, editing and proof reading, and extend special thanks to Sam for her care and attention in formatting this e-book.

OPENING REMARKS

by Dr. Olivia Tambou

Associate Professor at the Université Paris-Dauphine, PSL Research University, Cr2D. For correspondence: olivia.tambou@dauphine.fr.

The General Data Protection Regulation (GDPR) is applicable since the 25 May of 2018. It is "not the end of the road, but a beginning of a new chapter", as the Commissioner Jourová said in her keynote speech at General Data Protection Regulation conference. The purpose of these opening remarks is twofold. On the one hand, it is to give an overview of the normative and substantive nature of the GDPR in order to explain why national adaptations are required. On the other hand, it is to give an initial overview of the general approach of these national adaptations in some States. Detailed analysis of adaptations in eleven Member States is provided in individual chapters. At the time of the writing, only five EU member States have not yet adapted their national law to the GDPR: Bulgaria, Czech Republic, Portugal, Slovenia, and Greece. By contrast, one third country, Japan, has adapted its national Law in order to secure a finding of adequacy from the EU Commission, thereby allowing personal data to flow freely between the EU and Japan. The first observation that can be made is that the GDPR ensures the global visibility of the European Model of Data protection, and international influence even if the readability of this model is still unclear.

I - THE VISIBILITY OF THE EUROPEAN MODEL OF DATA PROTECTION PROPOSED BY THE GDPR

The publicity and attention drawn to the GDPR coming into effect by the media and the numerous notifications distributed by search engines, social network sites, political parties, banks, associations, digital platforms, etc., illustrates the rising visibility of the GDPR. In these opening remarks it is necessary to recall that the GDPR is the result of five years of discussion at the European level. Adopted in April 2016, the GDPR replaced Directive 95/46/EC, which was the first European Union legal framework on data protection. The GDPR is a monster text of 99 articles. It cements personal data protection law as a fundamental right in the post-Lisbon Treaty legal context. The GDPR clearly applies to all processing of personal data of residents in EU member states including in situations in which the data controller or processor are not established in the EU. Nevertheless, the GDPR, like the former directive, has the double ambition of ensuring a "consistent and high level of protection of individuals and to remov[ing] the obstacles to flows of personal data." The GDPR provides for the visibility of the European Union model of data protection law based on three main features. Firstly, this European Union model provides rights so that individuals remain in control of their data. Therefore, personal data has to be collected fairly, lawfully, and for legitimate, specific and explicit purposes. The collection needs to be based on freely given, specific, informed and unambiguous consent, or on another lawful basis. The GDPR creates a deeper right to information, a right to portability, a right to erasure including a right to be forgotten, a legal framework for profiling and individual automated decisions beyond the former right to access, right to object and right to rectification. Secondly, the European Union model is based on the regulation of data protection by the controller and the processor under the supervision of national Data Protection Authorities (DPAs). The obligations of the data controller and processor have been strengthened through the principle of accountability. These actors need to comply, to verify that they comply, and to document their compliance. At the same time, the controller and the processor can benefit from the limitation of the prior formalities for their processing activities. Furthermore, the GDPR creates a new independent European body: the European Data Protection Board (EDPB) which is composed of representatives of the national data protection authorities and the European Data Protection Supervisor (EDPS). The national DPAs and EDPB should support stakeholder compliance through the issuance of guidelines, certification, and promotion of code of conducts etc. Thirdly, the European Union model in the GDPR provides stronger enforcement measures. The powers of national DPAs are harmonized and their ability to coordinate and cooperate on investigations is addressed through the consistency mechanism and the concept of a lead DPA. The EDPB can adopt binding decisions when several EU countries are concerned by the same case. The DPAs have the power to impose fines on businesses of

OPENING REMARKS, by *Dr. Olivia Tambou*

up to 20 million EUR or 4% of a company's worldwide turnover. Furthermore, the Member States have had to introduce effective remedies including judicial remedies in their national law in case of violation or damage caused by a violation of the GDPR. Just eight short months after the adoption of the GDPR the European Commission said that national data protection authorities have received more than 95 000 complaints from citizens – an indication that many have concerns about the protection of their personal data and are keen to enforce their rights.[1]

Immediately after the application of the GDPR, several complaints were commenced which demonstrate the visibility of the European Union model of data protection. These complaints have common features. Large American companies, in particular Google and Facebook, have been targeted for their "take it or leave it" privacy policies. The complainants argue that it constitutes forced consent in violation of article 6 of the GDPR. These complaints are based on the possibility of collective representation of data subjects in order to lodge a complaint with a DPA (Art. 77§1 in combination with Art. 80 GDPR). The European consumer rights organization Noyb, chaired by Max Schrems, and the French association La Quadrature du Net have requested the prohibition of the relevant processing operations and the imposition of effective, proportionate and dissuasive fines. On the 21 January 2019, the French Data protection authority: the Commission Nationale Informatique et Libertés, (CNIL) delivered the first €50 million post-GDPR fine against Google[2]. This decision will appealed before the French Conseil d'Etat because its gives rise to concerns "about the impact of this ruling on publishers, original content creators and tech companies in Europe and beyond", said a Google spokesperson[3]. This illustrates that currently there is still a lack of readability of the European Model issued by the GDPR.

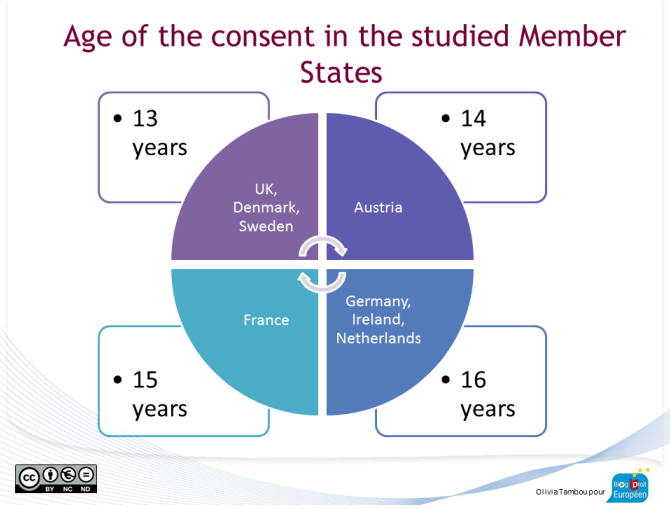
II- THE CURRENT LACK OF READABILITY OF THIS EUROPEAN MODEL

The current lack of readability of this European Model is due to several factors, which are interrelated and are mainly due to the 'General' nature of the GDPR.

A-The General Nature of the GDPR

The GDPR is considered to be a special Regulation compared to other EU Regulations. This is based on the existence of the so-called 'opening clauses,' which either permit or require Member States to adapt their national legislation in order to implement the rules of the GDPR. Nevertheless, this particularity should not be overestimated, because it can be found in other EU Regulations. Furthermore, the boundary between EU Regulations, which are generally regarded as complete texts, and EU Directives, which always need to be transposed into national Law, are more blurred in reality.

In reality, it is not the existence of opening clauses but rather the importance of the margin of discretion given to the Member States in the GDPR that could be disruptive. Half of the provisions of the GDPR contain opening clauses. Furthermore, some opening clauses give options to the Member States.



The most telling example is the age a child can consent to the processing of their personal data by information society services, which could vary from 16 to 13 years old, according to article 8 GDPR. A quick overview of the studied national adaptations shows that this provision has been subject of much debate in most of the Member States. In the end, each age option has been used. The Netherlands and Ireland have introduced a kind of experimental phase at the end of which the suitability of 16 years rather than 13 years will be assessed. France introduced a form of double consent from the parent and the child, which seems not to be expressly foreseen by the GPDR.

The application of fines to a public body is also a topic where Member States took different approaches. In France such fines have been only introduced for local entities but not for State bodies. In Spain, such fines have not been foreseen. In Netherlands and Ireland such fines exist. These examples illustrate that the GDPR cannot yet achieve its purpose of uniform application of the rules at the EU level.

1 See Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourovà and Gabriel ahead Data Protection Day, 25 January 2019

2 See our comment on that decision in the EDPL 1/2019 or in French in Dalloz Actualité

3 See Laurens Cerulus, Google to appeal €50 million GDPR fine, Politico.eu 23 January 2019 available at https://www.dalloz-actualite.fr/node/decryptage-autour-de-premiere-condamnation-de-google-par-cnil-post-rgpd

OPENING REMARKS, by *Dr. Olivia Tambou*

Furthermore, the GDPR allows the Member States to specify the application of data protection rules in specific sectors such as the public, employment and social security, and public health sectors, and for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, processing for journalistic purposes etc. Further, conditions and limitations can be introduced for genetic and biometric data. It is difficult to conceive how these kinds of opening clauses could simplify the legal environment for the actors involved.

This leads to the question, as noted by Julian Wagner and Alexander Benecke (EDPL 2016), whether the GDPR is a new kind of Regulation. The strongest argument in favour of this thesis is that the GDPR itself is labelled as a *General Regulation* [emphasis added]. Such wording is not part of the Art. 288 TFUE, which only mentioned the existence of Regulations. It is also not a current label in the praxis of the regulations.

The 'General' nature of the GDPR could be interpreted in two ways. According to the Longman dictionary, "general" means not detailed or relating to whole rather than specific situations. The General nature of the GDPR reflects this double dimension. It includes a vertical dimension of the specification of the set-up of the legal framework at national level. It also implies a horizontal dimension. This dimension is the result of the global approach between the GDPR and other European Union sectoral laws such as the specific directive on data protection in the area of police and justice or the future regulation on the handling of personal data by EU institutions and other EU bodies currently under discussion.

This General nature of GDPR is both an important factor in the visibility of the European Union model of data protection and a cause of its lack of readability. It brings the issue of coherence of the rules and the difficulties in assessing whether the derogations are not becoming the rules. This requires an analysis of the national uses of these opening clauses in order to identify if there are noticeable differences between Member States. It seems that some Member States have used these margins of discretion less moderately than others have. It will also be interesting to see whether these opening clauses have been used for the benefit of the private sector or the public sector. Therefore, this book gives some indication as to whether the general nature of the GDPR has an impact on the coherence of the European model of data protection.

B-The Complicated Nature of the National Adaptations of the GDPR

As the GDPR is a general regulation, the nature of the national adaptation raises two kinds of questions. The first is a question of terminology. The concept of transposition is usually dedicated to the direction. Both scholars and the European Commission itself have used the term national implementation[4]. Nevertheless, this could create some confusion with the implementing power of the European Commission. Therefore, the phrase national adaptation seems to be more neutral and allows the inclusion of a cultural approach to the national impact of the GDPR, such as the extended the scope of the application of some of its measures.

The second issue is related to drafting difficulties of these national adaptations. It has been stressed by the European Commission, that the "national legislator can therefore neither copy the text of the Regulation when it is not necessary in the light of the criteria provided by the case law, nor interpret it or add additional conditions to the rules directly applicable under the Regulation. If they did, operators throughout the Union would again be faced with fragmentation and would not know which rules they have to obey."(p. 9) This book gives some insights on whether there are some differences between Member States regarding those drafting obligations and what have been the most disputed issues during the legislative procedure.

Member States could be classified in different kind of groups:

- Those that have enacted a unique law for both the GDPR and the law Enforcement directive 2016/680 and those that have chosen to adopt two separates law. The unique act solution has been chosen by some States such as Austria, Germany, France, Ireland, and United Kingdom in contrast with Denmark, Italia, Spain, and Sweden.

- Those for which the GDPR implementation introduces a huge structural transformation of the former Data Protection Commissioner to a Data Protection Commission like Ireland, and others, which need only to strengthen the powers of the existing national protection authority.

- Spain seems to be apart because, as *Cristina Pauner* and *Jorge Viguri* show, Spain has taken the opportunity to introduce a Digital Charter.

Whatever the approach chosen, the book demonstrates that most of the national adaptations are still incomplete and raise concerns regarding their conformity with the GDPR. Several contributors wonder to what extent the national adaptation can go further than the wording of the GDPR. The contribution of *Dr.*

4 See for instance GDPR implementation, updated State of play in the Member States, 30/11, available at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=25109

OPENING REMARKS, by *Dr. Olivia Tambou*

Alexia Pato on national adaptations of article 80 GDPR (representation of data subjects) is a good example of these concerns. In those situations, the question of whether the data subject will always be able to directly invoke the GDPR will arise.

The GDPR implies some structural and cultural changes in the EU and beyond. Therefore, this book proposes to complete the analysis of the diversity of the national adaptations of the GDPR with some contributions about specific States situations. The contribution of *Karen Mc Cullagh* aims to provide an overview of the UK situation in the context of the Brexit. The contribution on Switzerland by *François Charlet* helps to remind us that the GDPR has also an impact on States in the European Economic Area, which need to adapt their data protection laws. Furthermore, the contribution by *Hiroshi Miyashita* illustrates the international influence of the GDPR and the first steps of convergence of data protection philosophies between Japan and the EU.

Part 1: Illustrations of the diversity of the national adaptations of the GDPR

The New Federal Data Protection Act – Implementation of the GDPR in Germany

By Dr. jur. Christian L. Geminn
Senior researcher at Kassel University and Managing Director of the Project Group Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG) at Kassel University, Germany. For correspondence: c.geminn@uni-kassel.de

I-INTRODUCTION

Germany was the first Member State to pass a law on the implementation of the GDPR (Regulation (EU) 2016/679; in German: Datenschutz-Grundverordnung, DS-GVO or DSGVO)[1] and on the adaption of national data protection law. The new "Bundesdatenschutzgesetz" (BDSG, Federal Data Protection Act) was officially published in July 2017 and came into force on 25 May 2018.

With 85 paragraphs, the new law is significantly longer than its predecessor which consisted of 48 paragraphs and a short annex. The reason for this is that the act does not only implement the GDPR, it also implements Directive (EU) 2016/680 (in German most commonly called Richtlinie für Justiz und Inneres, JI-Richtlinie).[2]

The new Federal Data Protection Act was introduced as Article 1 of the Act to adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU, DSAnpUG-EU, 30 June 2017).[3] Article 8 DSAnpUG-EU states that the previous Federal Data Protection Act[4] shall expire with the new, identically named, act coming into force.[5]

Articles 2 to 6 DSAnpUG-EU contain amendments to the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (Bundesverfassungsschutzgesetz, BVerfSchG),[6] the Military Counterintelligence Service Act (Gesetz über den Militärischen Abschirmdienst, MADG),[7] the Federal Intelligence Service Act (Bundesnachrichtendienstgesetz, BNDG),[8] the Act on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government (Sicherheitsüberprüfungsgesetz, SÜG)[9] and the Act to restrict the Privacy of Correspondence, Posts and Telecommunications (Artikel 10-Gesetz, G 10)[10].

Additionaly, a number of federal laws were adapted to the GDPR by the Act to Amend the Federal War Victims Relief Act and Other Provisions (Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften, 17 July 2017),[11] most notably provisions of the Social Security Code (Sozialgesetzbuch, SGB).

II-DATA PROTECTION LAW IN GERMANY

Germany has a long and rich tradition when it comes to data protection law. The Hessian Data Protection Act of 1970[12] is recognized as the oldest formal data protection act worldwide. A Federal Data Protection Act was introduced in 1977.[13] In 1983, the German Federal Constitutional Court in Karlsruhe (Bundesverfassungsgericht, BVerfG) gave its landmark decision on the then planned census (Volkszählungsurteil, Census Decision).[14] The decision established a new unwritten fundamental right in the Federal Republic: the right to informational self-determination.[15] Its importance for the development of German data protection law cannot be overstated.

1 Official Journal of the European Union L 119/1, 4 May 2016.
2 Official Journal of the European Union L 119/89, 4 May 2016.
3 Federal Law Gazette (BGBl.) 2017 I p. 2097. An English translation can be found here: https://www.bvdnet.de/wp-content/uploads/2017/08/BMI_%C3%9Cbersetzung_DSAnpUG-EU_mit_BDSG-neu.pdf.
4 Federal Law Gazette 2003 I p. 66.
5 Federal Law Gazette 2003 I p. 66.
6 Federal Law Gazette 1990 I p. 2954, 2970.
7 Federal Law Gazette 1990 I p. 2954, 2977.
8 Federal Law Gazette 1990 I p. 2954, 2979.
9 Federal Law Gazette 1994 I p. 867.
10 Federal Law Gazette 2001 I p. 1254, 2298; 2007 I p. 154.
11 Federal Law Gazette 2017 I p. 2541.
12 Law and Ordinance Gazette 1970 I p. 625.
13 Federal Law Gazette 1977 I p. 201.
14 BVerfGE (Decisions of the Federal Constitutional Court) 65, 1.
15 For further information on the decision see Hornung, G./Schnabel, C., Data protection in Germany I: The population census decision and the right to informational self-determination, Computer Law & Security Report, Vol. 25, Iss. 1, 2009, pp. 84-88.

IMPLEMENTATION OF THE GPDR IN GERMANY by, *Dr. jur. Christian L. Geminn*

Karlsruhe ruled that any interference with the right to informational self-determination must be based on a law that regulates the interference in an area specific and precise manner and that moreover regulates the lawful purpose as well as protective measures. This sparked the following development: The data protection law landscape in Germany has over time evolved and has become more and more complicated. All German states have their own data protection acts and there are provisions on data protection scattered all over sectoral German law, most notably perhaps in the Broadcast Media Act (Telemediengesetz, TMG)[16] and in the Telecommunications Act (Telekommunikationsgesetz, TKG)[17]. Adapting all of these provisions to the GDPR has proven to be a formidable task.

The federal structure of Germany means that beside the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftrage für den Datenschutz und die Informationsfreiheit, BfDI) each German state (Länder) has its own data protection commissioner.[18]

III-THE NEW FEDERAL DATA PROTECTION ACT

A-Structure

The new Federal Data Protection Act is divided into four parts. Part 1 contains common provisions relevant to both the GDPR and Directive (EU) 2016/680 as well as the processing of personal data beyond the scope of the two (Section 1 to Section 21). It is structured in 6 chapters: scope and definitions; legal basis for processing personal data; data protection officers of public bodies; Federal Commissioner for Data Protection and Freedom of Information; representation on the European Data Protection Board, single contact point, cooperation among the federal supervisory authorities and those of the states concerning European Union matters; legal remedies.

Part 2 is concerned with implementing provisions for processing for purposes in accordance with Article 2 GDPR. Like part 1, it is structured in 6 chapters: legal basis for processing personal data; rights of the data subject; obligations of controllers and processors; supervisory authorities for data processing by private bodies; penalties; legal remedies.

Part 3 serves the implementation of Directive (EU) 2016/680. The seventh chapter deals with: scope, definitions and general principles for processing personal data; legal basis for processing personal data; rights of the data subject; obligations of controllers and processors; transfer of data to third countries and to international organizations; cooperation among supervisory authorities; liabilities and penalties.

Part 4 consists of only a single section. Its Section 85 is concerned with the processing of personal data in the context of activities outside the scope of the GDPR and Directive (EU) 2016/680.

B-Scope of the Act

The Act applies to the processing of personal data of both private bodies and public bodies of the Federation (Bund).[19] Public authorities of the states (Länder) are only governed by the Act where data protection is not governed by state law. Other federal data protection law generally takes precedence over the Act.

Article 1(5) BDSG clarifies that the provisions of the Act shall not apply where the GDPR directly applies. For now, the burden to perform that evaluation is left to those applying the law. They will have to operate under the assumption that the new act does not violate the GDPR.

The overall scope of the GDPR is widened by Section 1(8) BDSG which states that the GDPR and Parts 1 and 2 BDSG generally apply accordingly to the processing of personal data by public bodies in the context of activities outside the scope of the GDPR and Directive (EU) 2017/680.

C-Opening clauses and regulatory mandates of the GDPR

The margin for the national lawmakers left by the GDPR is heavily disputed. The GDPR itself talks about "specifications or restrictions of its rules by Member State law".[20] German lawmakers have instead used the terms "Öffnungsklauseln" (opening clauses) and "Regelungsaufträge" (regulatory mandates) for classification.[21]

The regulatory mandates are ultimately meant to

16 Federal Law Gazette 2007 I p. 179.
17 Federal Law Gazette 2004 I p. 1190.
18 Plus the Bayerisches Landesamt für Datenschutzaufsicht (Data Protection Authority of Bavaria for the Private Sector). All meet and coordinate at the Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Conference of the independent data protection authorities of the Federation and the states).
19 Section 1 BDSG.
20 Recital 8 GDPR.
21 BT-Drs. (Bundestag printed matter) 18/11325, p. 1. For a more detailed analysis see Roßnagel, A./Bile, T./Friedewald, M./Geminn, C./Grigorjew, O./Karaboga, M./Nebel, M., *National Implementation of the GDPR: Challenges, Approaches,* Strategies Policy Paper, January 2018.

IMPLEMENTATION OF THE GPDR IN GERMANY by, *Dr. jur. Christian L. Geminn*

ensure the enforcement of the GDPR while opening clauses allow for a deviation from the GDPR. An obvious example for a regulatory mandate is Article 51(3) GDPR which requires Member States with more than one supervisory authority like Germany to define the supervisory authority which is meant to represent those authorities in the European Data Protection Board. The corresponding provision in the new Federal Data Protection Act is Section 17 which tasks the Federal Commissioner with that responsibility.

The total number of regulatory mandates and options is at about 70.[22] The GDPR is therefore said to resemble in parts a Directive. The purpose behind this is to enable Member States to maintain their complex, proven and practiced regulatory regimes in certain areas of life and administration as long as the European Single Market is not affected directly (e.g. tax law and social security, press law and labor law).

D-Areas of particular interest

1) Data processing for employment-related purposes

The provisions in Section 26 BDSG on data processing for employment-related purposes correspond with those of Section 32 of the old Federal Data Protection Act. In a single norm, the German legislator has placed a framework based on the opening clause of Article 88(1) GDPR.[23] It is expected that Section 26 BDSG will be reformed in the years to come to create a more specific framework.[24] It is also possible that a separate act on employment-related data processing will be created. Time restrictions and the high sensitivity of the subject only allowed for a transfer of the existing framework from the old BDSG to the new one. Attempts to reform employment-related data processing have failed several times in the past.

2) Video surveillance

The Act holds relatively detailed provisions on video surveillance of publicly accessible spaces in Section 4 BDSG. The provision is mostly identical with its predecessor in the old Federal Data Protection Act.[25] A major change of the old law was introduced in 2017 via the "Videoüberwachungsverbesserungsgesetz" (Act on the Improvement of Video Surveillance).[26] The change was meant to facilitate video surveillance for instance in the context of public transportation and at other places where large numbers of people gather like sports stadiums.

It is questionable if Section 4 BDSG is compatible with the GDPR. The GDPR regulates the lawfulness of processing in Article 6 GDPR. Specifications by the Member States are only permissible according to Article 6(2) GDPR if the processing in question is based on Article 6(1)(1)(c) or (e) GDPR.

It has to be noted that Section 4 BDSG is a deviation from the technological neutrality of the GDPR. The German legislator felt it was necessary to address the specific risks of video surveillance rather than rely on the abstract provisions of the GDPR.

3) Supervisory authorities

The provisions on the Federal Commissioner for Data Protection and Freedom of Information are found in Sections 8 to 16 BDSG. The Commissioner who is located in Bonn serves as supervisor for the public bodies of the Federation[27] with the exemption of federal courts acting in their judicial capacity[28] and represents Germany on the European Data Protection Board. Private bodies are supervised by the supervisory authorities of the states (Länder).[29]

The federal structure of Germany requires provisions on the cooperation between the many supervisory authorities of the Bund and the Länder. Such provisions can be found in Sections 18 and 19 BDSG. Clear responsibilities are of particular importance when it comes to handling complaints which play a pivotal role in the enforcement of the GDPR. According to Article 77(1) GDPR complaints can be lodged "with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement". Member States like Germany with multiple supervisory authorities are free to decide (or designate) which authority should be responsible. Section 19(2) BDSG states that in principle a complaint shall be forwarded by a supervisory authority which is not responsible according to Section

22 BT-Drs. (Bundestag printed matter) 18/11325, p. 73.
23 For further details see Kort, M., Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, ZD (2017) 319; Maier, N./Ossoinig, V., ‚Beschäftigtendatenschutz' in Roßnagel, A. (ed), *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze* (Nomos 2018) § 8 I.
24 BT-Drs. (Bundestag printed matter) 18/11325, p. 95; see also Coaltion Agreement 2018, pp. 1837 et seq., 6108.
25 Section 6b of the old Act.
26 Federal Law Gazette 2017 I p. 968. Full title: Gesetz zur Änderung des Bundesdatenschutzgesetzes - Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen.
27 Section 9(1) BDSG.
28 Section 9(2) BDSG; Article 77 GDPR.
29 Section 40(1) BDSG.

IMPLEMENTATION OF THE GPDR IN GERMANY by, *Dr. jur. Christian L. Geminn*

19(1) BDSG to the supervisory authority of a Land in which the controller or processor has an establishment.[30] If no such establishment exists, the addressee shall be the authority of the Land where the applicant resides.

A controversial[31] provision can be found in Section 29 BDSG. The investigatory powers of supervisory authorities according to Article 58(1)(e) and (f) GDPR shall not apply with regard to certain persons as far as exercising these powers would violate these persons' obligations to secrecy. A list of relevant persons can be found in Section 203(1), (2a) and (3) of the German Criminal Code and includes physicians, attorneys, psychologists, counsellors, social workers and other professions with special relationships of confidence with their clients.

4) Restrictions on the rights of the data subject

A significant part of the Act (Sections 32 to 37 BDSG) is devoted to restrictions on the rights of the data subject; ironically under the title "rights of the data subject".[32] The restrictions concern the information to be provided to the data subject (Sections 32 and 33 BDSG), the right of access (Section 34 BDSG), the right to erasure (Section 35 BDSG), the right to object (Section 36 BDSG) and automated individual decision-making (Section 37 BDSG). Additionally, Section 29 BDSG limits the rights of the data subject where secrecy obligations are involved.

The right to erasure[33] for instance shall not apply according to Section 35 BDSG if "in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal".

Another example is Article 37(1)(1) BDSG. The right "not to be subject to a decision based solely on automated processing[34] shall not apply if the decision is made in the context of providing services pursuant to an insurance contract and the request of the data subject was fulfilled". This is a limited transfer of Section 6a(2)(1) of the old BDSG.

Some of the restrictions were scaled back and limited to analogue processing after an earlier draft of the Act had come under fire because of the scope of the restrictions.[35]

5) Data protection officers

Section 38 BDSG contains a transfer of Section 4f of the preceding act into the new act. This means that the requirements for private bodies to designate a data protection officer go beyond those of the GDPR in Germany. Controllers and processors shall designate a data protection officer if they constantly employ as a rule at least ten persons dealing with the automated processing of personal data. Under certain conditions, a data protection officer has to be designated regardless of the number of persons employed in processing.[36]

Data protection officers of public bodies are regulated in Sections 5 to 7 BDSG.

6) Representation of data subjects

According to Article 80 GDPR, data subjects shall have the right to mandate a not-for-profit body, organization or association to lodge a complaint on their behalf and to exercise the rights referred to in Articles 77 to 79 GDPR. Member States are free to decide whether or not to give such bodies the right to act independently of a data subject's mandate.[37]

The corresponding provision is not located in the BDSG, but in Section 2(2)(1)(11) UKlaG (Unterlassungsklagengesetz, Injunction Act). This provision was created as early as February 2016 and is limited to data processing in the context of advertising, market and opinion research, credit bureaus, the creation of personality and usage profiles, address trading, other forms of data trading and similar commercial purposes. Section 2(2)(1)(11) UKlaG thus falls short of the possible scope of Article 80(2) GDPR.

7) Processing of special categories of personal data

Section 22(1)(1) BDSG allows for the processing of special

30 For details on the right to lodge a complaint see Geminn, C., ‚Rechtsschutz für Betroffene' in Jandt, S./ Steidle, R. (eds), *Datenschutz im Internet* (Nomos 2018).
31 See for instance Schuler, K./Weichert, T., ‚Beschränkung der Datenschutzkontrolle bei Berufsgeheimnisträgern nach § 29 Abs. 3 BDSG-neu ist grundrechtswidrig', 22.5.2017 <https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2017_dskontrolleinschr_bdsg-neu_03.pdf>.
32 Title of Part 2, Chapter 2 BDSG.
33 Article 17 GDPR.
34 Article 22 GDPR.
35 For more information on the draft see Geminn, C., Risikoadäquate Regelungen für das Internet der Dienste und Dinge? Die Neuerungen des Entwurfs für ein neues Bundesdatenschutzgesetz im Überblick, DuD (2017) 295-299 (296-299).
36 Section 38(1)(2) BDSG: "If the controller or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, they shall designate a data protection officer regardless of the number of persons employed in processing."
37 Article 80(2) GDPR.

IMPLEMENTATION OF THE GPDR IN GERMANY by, *Dr. jur. Christian L. Geminn*

categories of personal data by both public and private bodies. The permissible processing relates to social security, medicine, and public health. Section 22(2) BDSG states that "appropriate and specific measures shall be taken to safeguard the interests of the data subject" and lists a number of such measures.

8) Scoring

Section 31(1) BDSG on scoring is a continuation of Section 28b of the old BDSG; Section 31(2) BDSG on credit reports continues Section 28a of the old act. Section 31(1) BDSG only regulates scoring in the context of a contractual relationship with a natural person. Scoring is defined by the Act as "the use of a probability value for certain future action".

9) Penal provisions and fines

Section 42 BDSG contains penal provisions which amend the GDPR in accordance with Recital 152 GDPR. Transferring "personal data of a large number of people which are not publicly accessible" to a third party or otherwise making them accessible for commercial purposes is punishable with imprisonment of up to three years or a fine.[38] Processing without authorization of fraudulently acquiring personal data in return for payment or with the intention of enriching oneself or someone else or harming someone is punishable with imprisonment of up to two years or a fine.[39] Both offences are only prosecuted if the data subject, the controller, or a supervisory authority files a complaint.

Section 43 BDSG sets up administrative offences with fines of up to 50.000 € for violations of Section 30 BDSG on consumer loans. Section 43(3) BDSG states that authorities and other public bodies shall not be subject to any administrative fines.

Other noteworthy provisions are Section 42(4) and 43(4) BDSG which state that a notification pursuant to Article 33 GDPR or a communication pursuant to Article 34(1) GDPR may only be used in criminal proceedings as well as in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication if that person has given consent.

IV-CONCLUSION

The new Act transposes many provisions from its predecessor. This softens the requirements for controllers when it comes to adapting to the new data protection regime at least somewhat.[40]

Whether or not certain provisions in Germany's new law will hold out before the European Court of Justice will have to be seen. Some of the German supervisory authorities and data protection consultants have thus advised controllers not to utilize those national provisions that provide more leeway for processing of personal data.[41] For better or worse, Germany has deviated from the provisions of the GDPR by adjusting them. This runs contrarily to the goal of the GDPR to harmonize data protection law within the European Union and even beyond.

All in all, Germany has used the opening clauses contained in the GDPR in a rather one-sided manner.[42] The goal was to lift some of the burden that the GDPR has placed on the controller. This is particularly evident in the use of the opening clause of Article 23 GDPR to restrict the rights of the data subject.

The European Commission already threatened to start an infringement procedure against Germany in 2017.[43] The Commission seems irritated by the German approach and its representatives have sought to clarify that the GDPR merely allows for "specifications" thus limiting the margin for Member States.

V-OUTLOOK

Federal lawmakers are preparing an "omnibus law" to adjust 154 national (Federal) laws con-taining data protection provisions to the GDPR. Most of these adjustments will be of a formal nature to adapt the laws to the language used in the GDPR. There are however also new legal foundations for data processing and other significant changes[44] included. The governmental draft of the Second Act to adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (2. DSAnpUG-EU) was agreed on by the Federal gov-ernment on September 5th of 2018 and fills 563 pages.[45] Among the affected laws are for ex-ample the E-Government Act (Art. 15 of the 2. DSAnpUG-EU), and the Social

38 Section 42(1) BDSG.
39 Section 42(2) BDSG.

40 The legislator acknowledges this. See for instance BR-Drs. (Bundesrat printed matter) 110/17, p. 70.
41 E.g. the supervisory authority of the state Baden-Württemberg.
42 For further details see Roßnagel, A., Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, DuD (2017) 277-281.
43 https://heise.de/-3689759.
44 E.g. specifications for appropriate safeguards in the planned Section 18(3)(4) of the De-Mail Act (De-Mail-Gesetz).
45 BR-Drs. (Bundesrat printed matter) 430/18. Parallel to the 2. DSAnpUG-EU, there was also a draft introduced for an Act to Implement Directive (EU) 2016/680 in Criminal Proceedings and to adapt Data Protection Law to Regulation (EU) 2016/679; BT-Drs, (Bundestag printed matter) 19/4571.

IMPLEMENTATION OF THE GPDR IN GERMANY by, *Dr. jur. Christian L. Geminn*

Security Code (Art. 119 to 123); but there are also already minor changes planned for the new Federal Data Protection Act[46].[47] At the date of writing this chapter, the draft law is being discussed in committee at the Federal Diet (Bundestag) to address feedback from the Federal Council (Bundesrat).[48]

Some important aspects have not been touched in the Second DSAnpUG-EG: The first is data processing for employment-related purposes – despite the announcements mentioned above. The second and third are data protection in the Broadcast Media Act (Telemediengesetz, TMG) and in the Telecommunications Act (Telekommunikationsgesetz, TKG). It is to be expected that the two latter will not be reformed until the finalization of the planned ePrivacy Regulation. The existing confusion surrounding the question which provisions of TKG and TMG are suppressed by the GDPR and which remain applicable is thus going to continue.[49] On the state level, similar adjustments have been and continue to be made to state laws. The com-plexity of German data protection law is thus likely to remain – none of the existing national law will be dispensed with completely. For the administrations of the German states, local data protection acts exist, for instance the Hessian Data Protection and Freedom of Infor-mation Act (Hessisches Datenschutz- und Informationsgesetz, HDSIG).[50] These have also been reworked to become compatible with the GDPR.[51] However, not all states were able to complete the legislative process before 25 May 2018.

46 In Art. 12.
47 For an analysis see Roßnagel, A., Umsetzung der Unionsregelungen zum Datenschutz, DuD (2018) 741-745.
48For updates on the proceedings see dipbt.bundestag.de/extrakt/ba/WP19/2390/239070.html.
49 See Geminn, C./ Richter, P., 'Telekommunikation' and 'Telekommunikation' in Roßnagel, A. (ed), *Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts* (Nomos 2017) as well as Geminn, C./ Richter, P., 'Telekommunikation' and 'Telekommunikation' in Roßnagel, A. (ed), *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze* (Nomos 2018).
50 GVBl. 2018, p. 82 vom 09.05.2018.
51 Another example is the state of Saxony (Sachsen): Sächsisches Datenschutzdurchführungsgesetz (Saxonian Data Protection Implementation Act) of 26 April 2018 (GVBl. 2018, p. 198, 199) as part of the Gesetz zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Act to adapt state law to Regulation (EU) 2016/679 ...) of 26 April 2018 (GVBl. 2018, p. 198).

National Adaptations of the GDPR in Austria

By Dr. Günther Leissler LL.M.
Counsel at Schoenherr Attorneys at Law

By Mag. Patrizia Reisinger
Associate at Schoenherr Attorneys at Law

By Mag. Janos Böszörmenyi
Associate at Schoenherr Attorneys at Law. For correspondence: j.boeszoermenyi@schoenherr.eu

I-THE ORIGINS OF DATA PROTECTION IN AUSTRIA

In response to the technological evolution and as a result of growing concern related to the use of personal data by government agencies and large companies, a small number of European countries took the lead in enacting data protection legislation in the 1970s. Amongst them: Austria. The first Austrian data protection act (hereinafter 'Austrian Data Protection Act') was enacted in 1978 and came into force in 1980. Data protection was incorporated as a fundamental right for everyone[1] at constitutional level with third-party effect[2]. The 'Data Protection Commission' was established as competent authority and the concept of registration of data applications was introduced. Over time, the Austrian Data Protection Act was amended several times.[3]

The next milestone in the Austrian history of data protection was the transposition of the Directive 95/46/EC into Austrian law in 2000. The Directive was implemented by the Data Protection Act 2000 (hereinafter 'DPA 2000') and introduced several improvements. The DPA 2000 was amended several times and was applicable until May 24, 2018. The e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) was transposed in Part 12 of the Telecommunications Act 2003 (hereinafter 'TCA 2003'). The data protection provisions of the TCA 2003 remain in force and will probably be amended when the ePrivacy Regulation will take effect. Further important privacy-related provisions can be found in the Labour Constitution Act with regards to processing employees' data for human resources management and evaluation purposes. Moreover, the Austrian Criminal Code contains several criminal offences related to personal data.

II-NATIONAL CULTURE OF DATA PROTECTION IN AUSTRIA

The protection of personal data has been highly valued in Austria for a long time. Hence, the Austrian Data Protection Act of 1978 was one of the first of its kind in Europe. Further, the DPA 2000 imposed many restrictions on controllers concerning collecting, processing and transferring personal data and it granted a number of rights to data subjects. It set out the principles relating to processing of personal data (including lawfulness, fairness, and purpose limitation) and the lawfulness of processing (requiring a legitimate purpose and a legal basis). It also differentiated between the processing of 'ordinary' personal data and sensitive data. Data subjects had certain rights, such as the right of access, the right to rectification, the right to erasure and the right to object. Additionally, the TCA 2003 contains requirements, when it comes to electronic communications. Therefore, Austrian companies that were already compliant with the DPA 2000 and the TCA 2003 had a starting advantage.

The tight regulatory framework is accompanied by strict authorities and case law. For instance, Austrian case law requires to enumerate every personal data that a controller wants to collect by consent. Lastly, civil society is very active to uphold high standards on data protection. The best way to illustrate the civil society's activism is referring to the Data Retention Directive 2006/24/EC and the Safe Harbour Decision 2000/520/EC.

1 Including natural persons and legal entities
2 The 'third-party effect' of human rights obligates the State to provide individuals with sufficient protection in case their fundamental rights are violated by other individuals.
3 Cf. Jahnel D., ‚Datenschutzrecht' (Jan Sramek Verlag, 2010), 6.

National Adaptations of the GDPR in Austria

Both were invalidated inter alia on Austrian initiative.[4] The Austrian application that led to the invalidation of the Data Retention Directive was supported by 11,130 applicants. Maximilian Schrems who initiated the invalidation of the Safe Harbour Decision managed to commence a class action, supported by over 25,000 consumers against Facebook.[5] Even though the European Court of Justice turned down that class action,[6] it shows the high value of personal data to Austrians. Looking at recent events, on the very first day the GDPR came into effect, first complaints were filed by Maximilian Schrems' NGO NOYB – European Centre for Digital Rights[7] (hereinafter: 'NOYB'). NOYB filed complaints against Facebook in Austria, against Instagram in Belgium, against WhatsApp in Germany (Hamburg) and against Android (Google) in France.[8]

III-ADOPTION OF NATIONAL LAW TO SUPPLEMENT THE GDPR

To supplement and transpose the provisions of the GDPR and the Law Enforcement Directive (EU) 2016/680 the Austrian Parliament replaced the DPA 2000 by a legislative package on data protection which amended the current data protection framework in accordance with the GDPR and the Law Enforcement Directive.

The law-making process was politicised from the onset. The then governing coalition government agreed to avoid 'gold plating'; no additional obligations were supposed to be imposed on controllers. For instance, no cases – beyond the GDPR obligations – were defined, where private controllers would have to designate a data protection officer (hereinafter: 'DPO'). Moreover, the coalition agreement included not only to supplement the GDPR but at the same time to transpose Directive (EU) 2016/680. The reason to adopt one single act was inter alia to ensure a consistent level of protection.[9]

In June 2017, and thus before 2017 the autumn parliamentary elections took place, the Austrian Government presented the draft new Austrian Data Protection Act.[10] It contained several constitutional amendments, to name but one, the scope of the fundamental right would no longer include the protection of personal data of legal entities. The amendment of constitutional law provisions requires a two-thirds majority in the Austrian National Council.

Shortly before the vote in Parliament, the Austrian Government anticipated that it would not obtain the required majority and agreed on a different approach, aiming at adoption of the legal framework by the end of the former legislative period.[11] Instead of the new draft, the Government proposed an amendment to the current data protection framework without the revision of any constitutional provisions. The Austrian Parliament subsequently adopted – by a simple majority – the new national Data Protection Act (hereinafter 'DPA 2018') accordingly.[12]

In autumn 2017 parliamentary elections were held and a new government was sworn in. The Freedom Party joined the People's Party to form a coalition government, while the Social Democrats (who had been in the coalition government) had to go into opposition. The new Government aimed to repair the flaws of the DPA 2018. It seemed that the required two-third majority to amend the constitutional provisions in the DPA 2000 would be obtained. Members of the National Council from the government parties and from the Social Democrats put forward on 22 March 2018, a three-party motion that was supposed to become the Data Protection Deregulation Act (hereinafter: "Deregulation Act").[13] The National Council adopted its report on the bill on 11 April 2018. However, on 20 April 2018 the opposition parties, including the Social Democrats, introduced an amendment.[14]

4 CJEU Digital Rights Ireland and *Seitlinger* and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C: 2013:845; CJEU *Maximilian Schrems* v Data Protection Commissioner, Case C-362/14 ECLI:EU:C:2015:650.
5 See http://www.europe-v-facebook.org/sk/PA_OGH_en.pdf
6 CJEU Maximilian Schrems v Facebook Ireland Limited, Case C-498/16, ECLI:EU:C:2018:37.
7 NOYB stands for '(My Privacy is) none of your Business'
8 Kurier.at, Datenschutz: Schrems' Beschwerde gegen Google, Facebook & Co (25.05.2018) accessed May 30, 2018 https://kurier.at/wirtschaft/schrems-noyb-brachte-beschwerden-gegen-google-facebook-co-ein/400040704; Scally D., 'Max Schrems files first cases under GDPR against Facebook and Google' (2018) The Irish Times <https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177> accessed May 30, 2018.
9 Cf. Kunnert G, ‚Was bleibt vom DSG (2000)?' jusIT (2017) 239 (240).
10 Press release of the Austrian Parliament (hereinafter 'Press Release') Nb. 736 of June 16, 2017, on the DPA 2018, https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0736/, accessed May 22, 2018.
11 Press Release Nb. 803 of June 26, 2017, on the draft of a new Austrian Data Protection Act, https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0803/, accessed May 22, 2018.
12 Press Release Nb. 829 of June 29, 2017, on the new DPA 2018, https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0829/, accessed May 22, 2018.
13 Datenschutz-Deregulierungs-Gesetz 2018, Initiativantrag 189/A, March 22, 2018, https://www.parlament.gv.at/PAKT/VHG/XXVI/A/A_00189/imfname_686854.pdf, accessed May 25, 2018.
14 Abänderungsantrag, AA-8, April 20, 2018, https://www.parlament.gv.at/PAKT/VHG/XXVI/AA/AA_00008/imfname_691032.pdf, accessed May 25. 2018.

National Adaptations of the GDPR in Austria

The main objective of this amendment was to implement Article 80 (2) of the GDPR. Organizations in the field of data protection were to be empowered to lodge complaints with the supervisory authority independently of a data subject's mandate. The government parties however blocked that amendment, because they considered it as 'gold plating'. The government's program for this legislative period expressly stated that it would avoid gold plating regarding the transposition or implementation of EU law.[15] As a consequence – and according to media reports also due to political issues – the Social Democrats withdrew their support for the Deregulation Act.[16] Due to prior talks the governing coalition was expecting that outcome and submitted an amendment on the same day as well (hereinafter: "Amendment").[17]

Finally, the Austrian Parliament adopted the Deregulation Act as amended by the governing parties on April 20 together with three other bills as a legislative package[18]:

- Data Protection Act, Amendment (amending DPA 2018)
- Administrative Acts Data Protection Amendment Act (collective amendment of 120 different administrative acts to comply with the GDPR)
- Data Protection Amendment Act – Science and Research

In May 2018, a second 'Administrative Acts Data Protection Amendment Act' (amending approximately another 100 acts) was adopted by the Austrian Parliament[19]. The second 'Administrative Acts Data Protection Amendment Act' was published in June 2018, but many of its provisions came into effect retroactively on 25 May 2018.[20]

IV-MAIN PROVISIONS AT NATIONAL LEVEL IN AUSTRIA

This section will outline the most important provisions of the DPA 2018 implementing and supplementing the GDPR.

Fundamental right for legal entities: Despite the fact that the GDPR only covers the protection of natural persons, the fundamental right set out in Section 1 of DPA 2000 was not rephrased within DPA 2018 which has triggered discussions about whether the DPA 2018 offers protection to the personal data of legal entities. The legislator tried to remedy this defect in the DPA 2018 through the Deregulation Act. Yet, it became evident that the Deregulation Act would not get the two-third majority necessary to amend that constitutional provision. Therefore, the legislator rephrased Section 4 (1) of DPA 2018 and explicitly narrowed the applicability of the DPA 2018 to natural persons.[21] A third attempt to clarify that legal persons are not covered any longer by the DSG 2018 failed in December 2018 / January 2019.[22] The required two-third majority could once more not be reached. Due to the lack of applicability and thus enforceability, the DPA 2018 does not offer data protection to legal persons any longer. Nevertheless, Directive 2016/943 (EU)[23] which was transposed into national law by the end of January 2019,[24] shall offer sufficient protection for the data of legal entities.[25]

Registration of data applications: The Data Protection Authority operated a data processing register under the DPA 2000.[26] Controllers had to notify the Data Protection Authority of data applications they wished to run. Only certain data applications were exempt from the obligation to notify, inter alia those declared 'Standard Applications' which were published as an ordinance by the Federal Chancellor.[27] In order to enable controllers to review their registry inputs, the registry has been archived and will be accessible until 31 December 2019. It is prohibited to insert new entries

15 Zusammen für Österreich, Regierungsprogramm 2017-2022, 23, https://www.oevp.at/download/Regierungsprogramm.pdf, accessed May 25, 2018.
16 Press Release Nb. 442 of April 20, 2018, on the legislative package, https://www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0442/, accessed May 22, 2018.
17 Abänderungsantrag, AA-10, April 20, 2018, https://www.parlament.gv.at/PAKT/VHG/XXVI/AA/AA_00010/imfname_691038.pdf accessed May 25, 2018.
18 Press Release Nb. 442 of April 20, 2018, on the legislative package, https://www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0442/, accessed May 22, 2018.
19 <https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00108/index.shtml#tab-ParlamentarischesVerfahren> accessed May 30, 2018
20 BGBl I 2018/37

21 Leissler G / Wolfbauer V, 'Proposals to alter national Data Protection Act' (24.04.2018) International Law Office.
22 BGBl I 2019/14
23 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
24 BGBl I 2018/109
25 Anderl A., Hoerlsberger F., Mueller B., ‚Kein einfachgesetzlicher Schutz für Daten juristischer Personen', Oesterreichische Juristenzeitung (2018), 14 (16).
26 Section 16 of DPA 2000
27 Section 17 of DPA 2000

National Adaptations of the GDPR in Austria

into the registry or to change existing entries therein.[28] The Standard Applications remain a useful guideline for drafting records of processing activities.

Processing of data relating to criminal convictions and offences: Article 10 of the GDPR provides that data relating to criminal convictions and offences may only be processed under the control of official authority, unless otherwise permitted by Member State law. Section 4 (3) of DPA 2018 details the requirements for processing criminal data, e.g. statutory authorization or legitimate interests pursued by the controller.

Child's consent in relation to information society services: Based on the opening clause in Article 8 of the GDPR, Section 4 (4) of DPA 2018 contains the age requirement for legal consent given by a child. The age of consent for children has been set at 14 years.

Official secrets: Section 4 (5) of DPA 2018 provides a limitation of the right of access as set out in Article 15 of the GDPR. The right of access may not be granted if the controller fulfils sovereign tasks and providing the requested information would endanger those tasks. Section 4 (5) of DPA 2018 is based on the opening clause in Article 23 of the GDPR which provides a basis for restrictions to the rights of data subjects with respect to public safety or public security reasons.[29]

Business secrets: The right of access by the data subjects as set out in Article 15 of the GDPR is limited if the obligation to provide such information would jeopardize the controller's business or trade secrets or the performance of the controller's statutory duties.[30] The provisions on official secrets and business secrets were inserted by the Amendment.

Special provisions for data protection officers: Section 5 of DPA 2018 contains special provision for the DPO. If the DPO obtains knowledge of data processed by a person who has the statutory right to refuse to give evidence, the DPO may refuse to give evidence to the extent to which the said person exercises that right. To the extent the DPO may exercise the right to refuse to give evidence, the files and documents of the DPO are subject to a prohibition of seizure and confiscation. Sections 5 (3), (4) and (5) of DPA 2018 apply to the DPOs of public authorities or bodies. Such public-sector DPOs are not bound by any instructions when exercising their duties. However, the highest governing bodies or officers have the right to obtain information on the tasks performed by the DPO. Each federal ministry shall employ at least one DPO. The DPOs of the federal ministries shall regularly exchange information to ensure uniform data protection standards.

Data Secrecy: Pursuant to Section 6 of DPA 2018 employees must keep confidential all personal data that have been entrusted or have become accessible to them solely due to their employment ('Data Secrecy'), unless there is a legitimate reason for the transmission of the data. This obligation shall continue beyond the end of the employment contract. Employees may transmit such personal data only upon explicit order of the employer. Employers shall contractually bind their employees to comply with these standards.[31] In case of violation of data, the controller or processor may be punished with a penalty of up to EUR 50,000.[32] Violations committed with the intention to make a profit or to cause harm shall be punished by a court with imprisonment of up to one year or with a fine of up to 720 penalty units.[33]

Processing personal data in the context of employment: Processing employee data might require the conclusion of a works agreement between the controller and its works council. As laid down in the Austrian Labour Constitution Act approval by the works council is required for, inter alia, the following data applications:

- Staff questionnaires that contain information beyond general employee information
- Technical monitoring systems that may, at least in theory, impinge on the human dignity of the employees
- Automated human resources management systems (for instance payroll accounting systems, time recording systems etc.)

Processing personal data for scientific and historical research, statistics and archiving purposes of substantial public interest: As set out in Section 7 of DPA 2018, the controller may process any personal data which is publicly accessible, which the controller has lawfully collected for other research or similar purposes or which has been pseudonymized for the controller, unless the controller intends to obtain results that relate to the specific data subject. In the latter case, the controller needs to obtain consent from the data subject

28 Section 69 (2) of DPA 2018
29 Leissler G / Wolfbauer V, 'Proposals to alter national Data Protection Act' (24.04.2018) International Law Office.
30 Section 4 (6) of DPA2018
31 Section 6 of DPA 2018
32 Section 62 (1)(2) of DPA 2018
33 Section 63 of DPA 2018

National Adaptations of the GDPR in Austria

or the permission of the Data Protection Authority. The Data Protection Authority will only grant permission in certain circumstances. Moreover, with the 'Data Protection Amendmant Act - Since and Research' [34] special data protection legislation was put in place for scientific research purposes by amending the Research Organisation Act (Forschungsorganisationsgesetz).

Freedom of speech and freedom of information: Based on the opening clause in Article 85 (1) of the GDPR, Section 9 of DPA 2018 reconciles the right to the protection of personal data with the right to freedom of expression and information. The processing of personal data through media undertakings, media services and their employees for journalistic purposes is in fact exempt from the scope of the GDPR and the DPA 2018. Processing of personal data for purposes of academic, artistic or literary expression falls out of the scope of most provisions of the GDPR to the extent necessary to reconcile their right to freedom of expression and information with data protection. The original version of the DPA 2018 had outlined the role of media undertakings, media services and their employees, but treated them like everyone else exercising their right to freedom of expression and information. The special treatment was inserted by the Amendment. Interestingly, even data secrecy does not apply to employees of media undertakings and media services – it did apply in the original version of the DPA 2018.

Processing and transmission of data in the event of disaster: In the event of disaster, public sector and aid organizations may transfer personal data of a person who is directly affected by the disaster to their close relatives under strict conditions as set out in Section 10 of DPA 2018.

Issuance of reprimands: As set out in Section 11 of DPA 2018, instead of imposing an administrative fine right away, the Data Protection Authority shall issue reprimands to a controller or processor where processing operations have infringed provisions of the GDPR for the first time. Sanctions imposed pursuant to Article 83 of the GDPR shall be proportionate. This provision was introduced by the Amendment.

The fact that the Data Protection Authority shall issue reprimands in the first place caused heated debates on whether the provision of the DPA 2018 still was in accordance with the GDPR. Critical voices called the provision a toothless tiger and according to public sources, the European Commission has some concerns about this provision.[35] However, the provision reflects the content of Article 58 (2) of the GDPR which states that each supervisory authority shall have corrective powers and amongst them the power to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR. Neither the second part of Section 11 of DPA 2018 stating that the imposed sanctions shall be proportionate deviates from the wording of Article 83 (1) of the GDPR which states 'each supervisory authority shall ensure that the imposition of administrative fines [...] shall in each individual case be effective, proportionate and dissuasive'. The Explanatory Notes outline, that fines shall be imposed in accordance with Article 58 of the GDPR and under consideration of the criteria in Article 83 of the GDPR.[36]

Under Austrian administrative penal law, the principle of proportionality also applies when determining the punishment for an administrative offence, considering both aggravating and mitigating circumstances with equal diligence and care. The issuance of a reprimand to a first offender may potentially be justified under that principle just like the issuance of an increased penalty to a repeat offender.[37]

Processing of images: Sections 12 and 13 of DPA 2018 are dedicated to the processing of images for private purposes (e.g. monitoring and security) using technical devices. Recording images includes acoustic information processed together with the images. The so-called household exemption provision as set out in Article 2 of the GDPR and detailed in Section 12 (3)(3) of DPA 2018 provides that the processing of images is exempt from the application of the provisions if it serves a private documentary interest and does not aim at recording uninvolved persons to identify them or to record, in a targeted manner, items (e.g. license plates) that are appropriate for indirectly identifying such persons.

The processing of images is not permitted e.g. to monitor employees. It is neither permitted to automatically match personal data obtained from

34 BGBl I 2018/31

35 Schmid F., ‚EU-Kommission nimmt Oesterreichs Regelnzum Datenschutz ins Visier' (2018) Der Standard <https://derstandard.at/2000080583421/EU-Kommission-nimmt-oesterreichische-Datenschutzregeln-ins-Visier?ref=nl&userid=415519&nlid=4> accessed May 30, 2018.

36 Abänderungsantrag, AA-10, April 20, 2018 https://www.parlament.gv.at/PAKT/VHG/XXVI/AA/AA_00010/imfname_691038.pdf, accessed May 29. 2018.

37 Anderl A., Nino Tlapak, ‚Die Novelle der Novelle des Datenschutzgesetzes' (2018), Computerwelt, <https://computerwelt.at/news/kommentar/die-novelle-der-novelle-des-datenschutzgesetzes/> accessed May 30, 2018

National Adaptations of the GDPR in Austria

image recordings with other personal data without the express consent of the data subject. To give an example, face identifications from mobile devices are illegal without the express consent thereto.[38]

The provisions on processing of images are presumably most relevant to the use of video and audio surveillance systems (hereinafter 'CCTV'). The use of CCTV is not explicitly mentioned in the GDPR, but falls within the scope of the GDPR if it captures images of data subjects. CCTV might capture sensitive personal data, even if processing such data is not the intention of the controller. However, in case law to date the Austrian Data Protection Authority has not qualified the use of CCTV as processing of sensitive data, unless it is the controller´s intention to capture such data.

CCTV data processing is permitted if it is supported by the overriding legitimate interests of the data controller and if it is proportionate to use it or if the data subject has consented to the processing of their personal data. If CCTV data processing is permitted, the controller must take appropriate measures corresponding to the risk posed by the interference and must ensure that unauthorized persons cannot access or subsequently change the image recording. Except in the case of real-time surveillance, the controller shall keep logs of every processing operation. The controller shall erase personal data recorded if they are no longer necessary in relation to the purposes for which they were collected and if there is no other statutory obligation to maintain the data. Maintaining data for more than 72 hours must be proportionate, separate logs must be kept of the data and reasons must be stated.

The controller of an image recording must appropriately mark the recording. The mark shall clearly specify the controller, unless the controller is already known to the data subjects based on the circumstances of the case. However, it is recommended to fully mark the CCTV.

Austrian Data Protection Authority: The former Data Protection Commission was replaced in 2014 by the 'Data Protection Authority' which now holds the position as national supervisory authority.[39] Under the scope of the DPA 2000, the Data Protection Authority had already been an independent authority responsible for ensuring protection of the rights of data subjects. The authority handled complaints lodged by data subjects[40] and had a right to demand clarification and information from controllers as well as to carry out audits and inspections if there was a justified suspicion of a violation.[41] Now, it is entrusted with supervision under the GDPR. As set out in Section 18 to 23 of DPA 2018, the Data Protection Authority is now established as a national supervisory authority pursuant to Articles 51 to 54 of the GDPR and has been granted competences, powers and tasks in accordance with Article 55 et seq. of the GDPR. Additionally, it will serve as the only national accreditation body pursuant to Article 43 (1) of the GDPR. The DPA 2018 also specifies procedural provisions for proceedings in front of the Data Protection Authority.

Representation of data subjects and right to compensation: In accordance with Article 80 (1) of the GDPR and as set out in Section 28 of DPA 2018, data subjects shall have the right to mandate a non-profit organization that has statutory objectives of public interest and is active in the field of data protection to lodge complaints on their behalf and to exercise the rights referred to in the Sections 24 to 27 of DPA 2018. So far, no specific organization has been granted the right to represent data subjects, but any organization that fulfils the requirements may take action on behalf of the data subject. Two such organizations are the Consumers Association of Austria (https://vki.at/) and NOYB – European Centre for Digital Rights (https://noyb.eu/).

Pursuant to Section 29 of DPA 2018 data subjects who have suffered material or non-material damage as a result of an infringement of the GDPR or their fundamental right to data protection have the right to receive compensation from the controller or processor for the damage suffered. Under the current provisions of DPA 2018, the above mentioned non-profit organizations may not be mandated to exercise such right to receive compensation on the data subjects' behalf. Consumer protection and data protection groups and activists have been very critical of this lack of opportunity, especially as the first draft to the DPA 2018 provided the possibility to mandate such organizations to lodge a complaint to exercise the right to receive compensation on behalf of the data subjects. The paradox outcome of this late amendment of the DPA 2018 is that class action in its Austrian form remains feasible against Austrian controllers[42], while class action against controllers abroad is prevented.[43]

38 Leissler G / Wolfbauer V, 'Proposals to alter national Data Protection Act' (24.04.2018) International Law Office.
39 http://archiv.dsb.gv.at/site/6179/default.aspx, accessed May 22, 2018
40 Section 31 of DPA 2000
41 Section 30 of DPA 2000
42 Cf. Klauser, A, ‚Alpine, VW und noch immer keine echte österreichische Sammelklage', Zeitschrift für Verbraucherrecht (2015) 182.
43 Cf. EU-Datenschutz: Regierungsparteien schwächen

National Adaptations of the GDPR in Austria

Imposing administrative fines: Pursuant to Section 30 of DPA 2018 and relating to the processing of data by legal entities, administrative fines may be imposed on legal entities only if infringements were committed through misconduct or lack of supervision/control by one or several of the legal entity's representatives holding a leading position within the legal entity.

The procedure to impose administrative fines is regulated by the Administrative Penal Act. This Act however deviates to some extent from the GDPR. The Administrative Penal Act does not foresee a fine for legal entities. Instead pursuant to Section 9 of that Act, the 'responsible natural persons' are held accountable for non-compliance of a legal entity. To comply with the "ne bis in idem" principle, Section 30 (3) of DPA 2018 stipulates that such a responsible natural person may only be fined if the legal entity is not fined.

According to Section 30 (5) of DPA 2018 public authorities and bodies established in Austria may not be fined. The Amendment introduced an explanation to the term "public bodies", which at first glance, reads like a definition. However, the Explanatory Notes clarify that it is only a concretization. For the actual legal definition, the Explanatory Notes refer to Section 4 (1) of the Information Re-Use Act, which transposes the PSI Directive 2003/98/EC.[44]

National administrative fines: In addition to the sanctions of Article 83 of the GDPR, Section 62 of DPA 2018 contains a number of administrative fines of up to EUR 50,000 to be imposed for certain administrative offences (such as intentional data transmission violating the provisions of Data Secrecy). These fines may be imposed unless a sanction has already been imposed for the same infringement under Article 83 of the GDPR or the infringement may be punished with a higher penalty under any other administrative penal provisions.

Existing consents according to DPA 2000: As set out in the transitional provisions of DPA 2018 in Section 69 (9), consent given pursuant to the DPA 2000 shall continue to be valid if it meets the requirements of the GDPR. Furthermore, certain authorizations (e.g. regarding cross-border transmission of personal data) granted by the DPA under the provisions of the DPA 2000 shall remain unaffected.

Data protection impact assessment: In accordance with Section 35 (5) of the GDPR the Data Protection Authority established and adopted a list on the kind of processing operations for which no data protection impact assessment is required ('White List'), which entered into force on 25 May 2018.[45] Later on in November 2018, the Data Protection Authority also made public a list of the kind of processing activities which must be subject to a data protection impact assessment ('Black List').[46]

Rechtsdurchsetzung gegen globale Konzerne, https://noyb.eu/wp-content/uploads/2018/04/PA_DSGVO.pdf, accessed May 29, 2018.
44 Abänderungsantrag, AA-10, April 20, 2018 https://www.parlament.gv.at/PAKT/VHG/XXVI/AA/AA_00010/imfname_691038.pdf, accessed May 29. 2018.

45 Federal Law Gazette, Part II, No 108/2018, issued on May 25, 2018

46 BGBl II 2018/278

THE SWEDISH MEASURES ACCOMPANYING THE GDPR

By Dr. Patricia Jonason
Associate Professor, Södertörn University. For correspondence: patricia.jonason@sh.se

I-INTRODUCTION

On the 18th of April 2018 the Swedish Parliament, the Riksdag, passed the *Act with supplementing provisions to the EU Data Protection Regulation*[1], or in short, the *Data Protection Act*[2] (DPA). With the new Act and the General Data Protection Regulation (GDPR)[3], both entering into force on 25 May 2018, Sweden enters its third generation of data protection legislation. The DPA replaces the *Personal Data Act* (PDA) and the *Personal Data Ordinance* (PDO) introduced in 1998 to transpose the Data Protection Directive 95/46/EC which in turn replaced the *Data Act* from 1973, the first national data protection legislation of its kind in the world.

The work of drafting the new Swedish Data Protection Act aimed at complementing the GDPR began officially on the 25 February 2016 – that is about two months before the adoption of the GDPR by the EU Parliament and the Council – with the Government's decision on terms of reference.[4] According to these guidelines, the task of the committee of inquiry appointed, named the *Data Protection Inquiry*[5], was principally circumscribed to propose a repeal of the current data protection legislation as well as to propose *"legal provisions which, on a general level, complement the GDPR"*.[6] In order to successfully deliver a timely, satisfying, accessible and coherent legal framework, the legislator had to focus on the more urgent issue, i.e. the drafting and enactment of a general Act, thus setting aside the sectoral regulations.[7]

The Committee of inquiry submitted a report, entitled *The New Data Protection Act - supplementing provisions to EU Data Protection Regulation*[8] to the Government on 12 May 2017. This report of about 500 pages contained a general introduction to the GDPR and a detailed overview of the components of the GDPR that had lead to the enactment of supplementary national provisions.[9] It also contains a proposal for the draft of a new data protection act. The proposal was then referred to the Council of legislation for consideration and submitted for comments to different organisations (public authorities, universities etc.). Backed by the committee's report, the Council of legislation's assessment and submitted comments, the Government then proposed, a revised draft of a new Data Protection Act.[10] The bill was then examined by a Parliamentary committee[11] before a vote by the Riksdag. The new Act was passed on the 18th of April, just one month before the GDPR's entry into force.

The task of tackling the transposition of the Directive (EU) 2016/680 into the Swedish legal system was entrusted to a distinct inquiry committee.[12] The special investigators and the secretaries of the two committees of inquiry met several times, including in the begining of their missions, in order to plan their investigative work. The Data Protection inquiry however confessed that the *"limited available time for our investigative*

1 *Lag med kompletterande bestämmelser till EU:s dataskyddsförordningen* (2018:218).
2 *Dataskyddslagen.*
3 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.
4 Kommitteedirektiv 2016:15. The terms of reference are based on the version of the GDPR to be found in document 2012/0011COD, 5455/16 from 28 January 2016.
5 Dataskyddsutredningen. The Committee was composed of a special investigator and about 10 experts.
6 Dir. 2016:15, p. 6. The question of the future supervisory authority has been left outside the scope of the remit of the Data Protection Committee as another committee of inquiry (Utredningen om tillsynen över den personliga integritet) has been assigned the task.
7 Prop. 2017/18:105, p. 23. This does not exclude, says anyways the legislator, that other important changes might be required and discussed in other contexts.
8 Ny dataskyddslag, Kompletterande bestämmelser till EU:s dataskyddsförordningen.
9 SOU 2017:39.
10 Prop. 2017/18:105, Ny dataskyddslag.
11 Report of Committee on Constitutional affairs which took position on the Government proposal. (2017/18:KU23), February 15, 2018.
12 JU 2016:06.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

work has not allowed us the opportunity to sufficiently process the proposal and other documents from the committee of inquiry on the data protection directive from 2016". It concludes that *"there might therefore be unintentional differences between the two committees' stances on various issues"*. [13]

The enthusiasm preceding the entering into force of the new data protection affected not only the legislature but also the Swedish Data Protection Authority (the Datainspektion, DI) and data controllers. The DI worked tremendous hard and introduced a variety of measures to help data controllers prepare for the new law. The supervisory authority has *inter alia* published comprehensive guidelines and other information on its website and has offered several training sessions. For Swedish data controllers the fear and panic associated with the 25 May 2018 could be compared to the predictions of the Y2K scare at the turn of the last Century.

The remainder of this paper, will focus on Sweden's supplementary provisions to the GDPR, i.e on the Data Protection Act (2018:218). First, the scheme of the new Swedish Act will be examined (II), secondly the impact of the GDPR and of the accompanying adaptation measures on the Swedish legal system will be analysed (III).

II-THE SCHEME OF THE SWEDISH DATA PROTECTION ACT

As mentioned above, the terms of reference gave the special investigator and the experts of the Data Protection inquiry the task of proposing the repeal of the Personal Data Act (1998:204) and of the Personal Data Ordinance (1998:1191) as well as the enactment of a new national Act. There doesn't seem to have been any discussion on whether to keep and adapt the existing Personal Data Act as was the case in France with the Loi Informatique et Libertés. On the contrary, the preparatory works sharply assessed that the GDPR *"will constitute the general regulatory framework on the processing of personal data within the EU"* which *"means that the Personal Data Act and related regulations have to be repealed"*.[14] The preparatory works explain further that *"the Swedish general regulatory framework on data protection can not continue to exist as it would lead to prohibited duplication of regulation"*.[15] The choice of the name of the new Swedish Act - the A*ct containing supplementary provisions to EU General Data Protection Regulation* - may be regarded as marking a break with the previous national legal framework. It is motivated by the intention to *"emphasise the fact that the statutes are not comprehensive and that they are simply a supplement to the GDPR"*.[16]

This begs the following questions: What is the content of the new Act (A)? What is its scope of application (B)? How does the new act tie with the GDPR (C)?

A-The content of the Data Protection Act (2018:218)

The Data protection Act is comprised of 40 provisions arranged in seven chapters.

Chapter 1, with the heading *Preliminary provisions*, contains provisions of different kinds: it informs of the supplementary nature of the Data Protection Act and determines the substantive scope of application of the GDPR and of the Data Protection Act – it extends beyond the scope of application of the GDPR. It also sets out the territorial scope of application of the Data Protection Act. Additionally, the first chapter contains a provision on the relationship between the GDPR and the Data Protection Act on one hand and the freedom of the press and freedom of expression on the other hand. It also contains a provision on professional secrecy for data protection officers.

Chapter 2, with the heading *Legal basis*, contains provisions related to the processing of personal data when there is a legal obligation, when a task is carried out in the public interest or a task is carried out in the exercise of official authority. The second chapter also contains a provision concerning private archives as well as a provision about childrens' consent, fixing the age of consent at 13 years.

Chapter 3 is related to the *processing of certain categories of personal data* and encompasses provisions on when sensitive personal data according to GDPR art. 9.1 may be processed (in the field of employment, social security and social protection; when an important public interest exists; in the field of health services, medical care and social care; in the fields of archives and statistics). The chapter also contains provisions on personal data relating to criminal offences and on identification numbers.

Chapter 4 contains provisions on *Limitations of use* related to archives and statistics.

Chapter 5 lays down *Limitations of certain rights and*

13 SOU 2017:39, p.61.
14 Id., p. 77.
15 Id., p. 78.
16 Id., p.29.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

obligations, which are the freedom of opinion and the right of access to information.

Chapter 6, with the heading *The supervisory authority's handling and decisions* contains a provision dedicated to the supervisory authority's competence. This explicitly gives the Swedish authority the competence to monitor the Data Protection Act and other Swedish regulations that supplement the GDPR, according to articles 58.1, 58.2 and 58.3 of the GDPR. This does not mean, however, that the monitoring authority has the right to levy fees for other violations as the ones referred to in article 83 of the GDPR. The remaining six provisions of Chapter 6 deal with penalties.

The last chapter, *Chapter 7* on *Damages and appeal*, contains, besides a provision on damages, four provisions dedicated to the question of appeal. One provision deals with appeals lodged against decisions taken by public authorities in their capacity of data controllers. Such decisions may be submitted to the administrative courts. However neither the decisions of the Government nor the decisions of the Supreme Court, the Supreme Administrative Court or the Parliamentary Ombudsman are subject to appeal. The chapter furthermore contains a provision about the appeal lodged against the decisions of the supervisory authority. The competent court is, here as well, the administrative court. Chapter 7 ends with two provisions, one that states which kinds of other decisions may be appealed against, another that lays down the prohibition to lodge an appeal against all remaining decisions taken on the basis of the GDPR or on the basis of the Data Protection Act.

B-The scope of the new Act

As was the case for the transposition of the Data Protection Directive, the Swedish legislator chose to extend the scope of application of the general rules of the data protection legislation beyond what is required by the European legal instrument.[17] Indeed, the GDPR and the Data Protection Act are, in Sweden, intended to *"even apply for activities outside the scope of application of the European law as well as when it concerns Sweden's participation in the Common Foreign and Security Policy "*.[18]

The reasons for this choice are manifold. Some of the arguments for applying the general rules to all kinds of processing are related to the need to have a high level of *privacy protection* within the whole public sector – which is the sector concerned by the exemptions provided in the GDPR.[19] Arguments of a more technical and practical nature were also considered by the legislator for justifying the extension of the scope of the general rules beyond what is required by the GDPR. The legislator referred to the difficulty of *"precisely determin*[ing] *the frontiers of the scope of application of EU law"*. It also emphasizes that this approach would allow public authorities that carry out activities both within and outside the scope of EU law to apply the same rules to all kinds of activities.[20] An additional argument related to Sweden's international obligations: the legislator referred to the obligation, stemming from the Convention No. 108 of the Council of Europe, to set up a general legal framework on data protection.[21]

The legislator's choice to extend the GDPR's rules into the national data protection landscape is enshrined in the Data Protection Act under Chapter 1, Section 2 under the heading *"Extended application of the provisions of the EU General Data Protection Regulation."* Section 2 states *"The provisions of EU's Data Protection Regulation in its original form, and of the current Act are even applicable to the processing of personal data in the course of an activity which falls outside the scope of EU law and in the course of an activity covered by Title V, Chapter 2 of the Treaty on European Union"*.

There are however some exceptions. According to Section 3, the abovementioned doesn't apply to activities covered by:

1. Act (2007:258) Concerning The Processing Of Personal Data In The Armed Forces' Defence Intelligence And Military Security Service

2. Act (2007:259) Act on Processing of Personal Records within the Scope of the Defence Intelligence and Development Activities of the National Defence Radio Establishment

3. Chapter 6 of the Police Data Act (2010:361). The chapter in question contains provisions related to the processing of personal data in the course of the activities of the security police.[22]

17 Prop. 2017/18:105, p. 28.
18 Ibid.

19 See Prop. 2017/18:105, p.28
20 Prop. 2017/18:105, pp.. 29-30.
21 Id., p. 29.
22 The DPA also laid down a specific provision stating that articles 33 and 34 of the GDPR do not apply when it concerns personal data breach that have to be notified according to the Protective Security Act (1996:627) or to rules enacted on its basis. The legislator emphasizes, in the preparatory works, which in Sweden constitute

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

C. The relationship to the GDPR

The new Swedish Data Protection Act uses two methods for referencing provisions in the GDPR: references of a dynamic nature and references of static nature.[23]

The term *dynamic references* means that the references made to the GDPR concerns the version applicable at any given moment. The mechanism ensures direct application of potential changes that may occur in the lifetime of the GDPR. It does not discount however the fact that changes in the GDPR may lead to changes in the Data Protection Act.[24] This dynamic method of reference is used in provisions of informative character such as the provisions concerning the legal basis required for sensitive personal data and the provisions related to damages. The method is similarly used for an informative purpose when the DPA advises that the terms and expressions employed in the Act have the same meaning than in the GDPR.[25] Dynamic references are also used for GDPR provisions that had to be introduced *"in Swedish law in order for Sweden to comply with its European obligations"*.[26] These are inter alia the provisions on which public authorities are competent or have obligations to adopt measures and the provision about data protection officer's professional secrecy obligation. A final category of dynamic references covers exemptions from the provisions of the GDPR regarding the rights of the data subjects and the obligations of the data controllers.

Two s*tatic references* are included in the new Swedish Data Protection Act. The term 'static' means that the references made in the PDA to the GDPR concern the GDPR in its original form. The first static reference concerns the provision regarding the processing of personal data outside the scope of the GDPR, while the second concerns provisions on penalties.[27]

III-THE IMPACT OF THE NEW EUROPEAN DATA PROTECTION LEGISLATION ON SWEDISH LAW

Below, three questions are posed and answered to allow us to assess the impact of the GDPR on the Swedish data protection legislation. First, what is the relationship between freedoms of opinion and the data protection legislation? While this question was not the subject of controversy in the context of the transposition of the Data Protection Directive, it has been the forefront of debate regarding the new data protection Act (A). Secondly, the question of formalism: while the new philosophy of the GDPR, which places less importance on formalities, suits the Swedish legislator better than the highly formalistic and prescriptive approach in the Data Protection Directive, the replacement of the Directive by the GDPR nevertheless constitutes a step backwards for Sweden in terms of formalism (B). Thirdly, the question of the increase of the rights of the data subjects in their relationship to the Supervisory authority (C).

A-The relationship between the GDPR and freedom of opinion

Before going deeper into the wording of the law, it is worth mentioning that freedom of opinion, i.e. freedom of the press, freedom of expression and the right of access to official documents, are highly valued freedoms, with constitutional protection, in Sweden. [28]. These freedoms are also highly valued in society, not least among politicians and journalists. One may recall that it was the Swedish Government who, fearing that the transposition of the Data Protection Directive would impair the generous right of access to information as laid down in Swedish law, pushed for the introduction of recital 72 in the Preamble of the Directive allowing «[…] *the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive*». Swedish journalists have, on several occasions, shown a strong commitment to protecting the abovementioned freedoms against limitations, including limitations justified by the need to protect privacy. For example, the Association of Swedish journalists initated a campaign called "Don't touch my principle of publicity" at the time of the transposition of the Data Protection Directive. The journalists feared a negative impact of the European Act on the right of access to official documents.

an important legal source, that *"Sweden has not transferred the decision-making competence to the EU within the areas the GDPR's rules will apply according to the* [current] *bill"*. Therefore, *"If the GDPR is reformed, the Swedish legislator should* […] *decide if the changes also will impact the areas that are* [according to the European law] *exempted from the scope of application of the GDPR"*. This is why the Data Protection Act refers to the GDPR's *"original form"*. Prop. 2017/18:105, p. 32.

23 Prop. 2017/18:105, p. 24.

24 Id., p. 25.

25 Chap. 1, Section 1.

26 Prop. 2017/18:105, p. 25.

27 The committee of inquiry had proposed to apply the system of dynamic references regarding the penalties but the Government decided to apply the static approach to these sanctions. See Prop. 2017/18:105, p. 24.

28 The freedom of the press is regulated in the Freedom of the Press Act and the freedom of expression in the Fundamental Law on Freedom of Expression. The right of access to official documents is regulated in the Freedom of the Press Act (Chapter 2).

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

When the Data Protection Directive was in force, the Swedish Personal Data Act contained two provisions dedicated respectively to the relationship of the data protection legal framework to freedom of the press and freedom of expression on the one hand (Section 7) and the principle of public access to official documents on the other hand (Section 8). The first section was a transposition of article 9 of the Directive, the second took into account the margin of appreciation offered to member States by recital 72.

The GDPR contains two articles respectively dedicated to processing and public access to official documents (art. 86) and to processing and freedom of expression and information (art. 85). However, the new Data Protection Act contains only one provision, with the heading *"Relationship to freedom of the press and freedom of expression"*.

Chapter 1, Section 7 states *"Neither the GDPR nor this Act shall apply so far that they will infringe upon the Freedom of the Press Act or the Freedom of expression Act.*

Articles 5-30 and 35 to 50 of the GDPR as well as Chapters 2 to 5 of this Act shall not apply on the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression."

Although the heading only refers to the freedom of the press and freedom of expression, the provision also encompasses the right of access to official documents. I will analyse this right before examining the freedom of the press and freedom of expression.

1) The relationship between the right of access to official documents and the data protection legislation

The right of access to official documents in Sweden is, regulated in detail, by the Second Chapter of the Freedom of the Press Act (FPA). The Personal Data Act (1998:204), mirroring the margin of appreciation offered by Recital 72 in the Directive, had facilitated this in Section 8[29] which stated: *"The provisions of this Act are not applied to the extent that they would limit an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide personal data"*.

The Committee in charge of the first draft of the new Data Protection Act, considered that *"the scope for allowing the principle of public access to official documents to take priority over the personal data regulations is clear in the General Data Protection Regulation"*[30], and accordingdly decided that there was no need to have an equivalent provision to section 8 of the Personal Data Act in the new Data Protection Act. Consequently, the only provision addressing the relationship between data protection legislation and freedom of opinion proposed by the committee concerned the relationship to the freedom of the press and the freedom of expression.

Therefore, the provision, under the heading *"Relationship to the freedom of the press and the freedom of expression"*, had the phrase *"Neither the GDPR nor this Act shall apply so far that they will infringe the provisions on freedom of the press and freedom of expression laid down in the Freedom of the Press Act or in the Fundamental Law on Freedom of Expression"* in the version proposed by the Committee. However, the Government assessed that there was a crucial need for making the relationship between the data protection legislation (GDPR and the Swedish Act) and the Swedish constitution clear,[31] not least because of the high penalties that may apply under the GDPR. The changes made by the Government - and endorsed by the Parliament - in the provision proposed by the committee consist of omitting the reference to the *provisions* on the freedom of the press and the freedom of expression and instead refer to the *constitutional acts* themselves. As the right of access to official documents is regulated by the Freedom of the Press Act, this right automatically falls within the scope of the new provision. Nevertheless the Government did not make any adjustment to the heading of the provision, which is still entitled *"The relationship to the freedom of the press and the freedom of expression"*. Since this choice of words does not include the right of access to information, the adopted provision is confusing.[32]

29 Under the heading *"Relationship to the principle of public access to official documents"*.

30 SOU 2017:39, p.31.The Swedish legislator is of the meaning that the GDPR does not impact this regime, i.e that it is possible to maintain a system where precedence is given to the right of access to official documents. The terms of reference notice for instance: *"it is even clearer as it is in the Data Protection Directive that the European Data Protection legislation does not impinge the field of the Freedom of the Press Act* [...].", Dir. 2016:15, p. 22.

31 Prop. 2017/18:105, p. 43.

32 It had been more correct to have a heading not only mentioning the relationship to the freedom of the press and the freedom of expression but also the relationship to the right of access to official documents. Or even better, as it better corresponds to the very wordings of the provision, to entitle the heading *"Relationship to the Freedom of the Press Act and to the Fundamental Law on Freedom of Expression"*. The preparatory works, here the proposition, giving the explanations, if needed, that this covers the three freedoms of opinions. One may regret that neither the Council of legislation nor the Datainspektion had per definition the possibility to express themselves on this question as it was not tackled in the first report they had to address comments on.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

2) The relationship between the freedom of expression and the data protection rules

Read from the perspective of the relationship to the freedom of the press and the freedom of expression, Section 7, Chapter 1 of the DPA is composed of two parts corresponding to two legal regimes, as was also the case under the Personal Data Act.

The first paragraph, which applies to processings falling within the scope of the constitutional protection of the freedom of press and freedom of expression, lays down in a general manner the principle of precedence of the constitutional legal framework of the freedom of the Press and the freedom of expression over data protection legislation. The second paragraph that regulates freedom of expression outside the scope of the constitutional protection sets out a special regime for the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

In this second paragraph, that was not subject to controversy during the legislative procedure, the legislator followed the model adopted when transposing the Data Protection Directive, i.e. it made maximum use of exemptions offered in the GDPR,[33] only applying the provisions related to security and inspection.[34]

The first paragraph on the question of the relationship between the data protection legislation on one hand and the freedom of the press and the freedom of expression as constitutionally guaranted on the other hand had been the subject of a less straightforward legislative process. Firstly, the committee of inquiry decided of its own volution to take on this task even though the terms of reference had not asked it to propose provisions on this issue. The committee proposed a provision similar to its counterpart in the PDA, i.e. laying down the rule of the precedence of the provisions concerning the freedom of the press and the freedom of expression contained in the FPA or the Fundamental Law on Freedom of Expression (FLFE).[35]

The reasons invoked by the committee for regulating this issue were, firstly, that it was *"important that the provisions of the GDPR and of the Data Protection Act do not raise uncertainty about the possibilities to process personal data within the scope of the constitutional regulation* [of freedom of expression and of the press] *as this may impact vital and very sensitive parts of the opinion-making activities such as freedom of communication and protection of sources"*.[36] Furthermore the committee advanced that since the European law is now directly applicable regulation, for which violations may lead to significant penalties, it increases the need for a clear relationship between the laws. Beyond arguing for the *need* to introduce such a provision of informative character, the committee also defended the possibility of maintaining a provision laying down *the rule of the precedence* of the constitutional legal framework before the data protection legislation.[37] The Committee referred for that purpose to the fact that the previous provision of the Personal data Act[38] with a similar content had not been the subject of legal challenges nor had it been questioned by the European Commission during its 20 years of application.

The Swedish Data Protection Authority (DI), when asked to give comments on the first draft of the new Data Protection Act criticized serveral of the proposed provisions. Firstly, it pointed out the incorrect legal interpretation of the relationship between EU law and national law by the committee. The DI argued that the situation is different under the GDPR than it was under the Data Protection Directive. To consider that the Swedish constitutional texts have precedence over the GDPR is therefore *"not a correct description of the legal situation"*.[39]

Secondly, the DI critised the committee for its interpretation of the margin of appreciation provided by the GDPR and denied that Article 85 of the GDPR allows the member States to set out general exemptions such as the one proposed by the Swedish legislator. The DI argued that as there are two crucial human rights that have to be balanced against each other, an appreciation of proportionality has to be made in the individual cases, according to the case law of the CJEU and of the ECtHR.[40] The DI made use of the ECtHR case *Satukunnan Markkinapörssi OY and Satamedia OY v. Finland* to support its argument. In this case concerning mass collection of personal taxation

33 See Blanc-Gonnet Jonason, P., *Protection de la vie privée et transparence à l'épreuve de l'informatique, droit francais, droit suédois et directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995*, Université Paris XII, 2001, pp. 64-65.
34 *"We are of the opinion that the exemption from the provisions of the Data Protection Act and the GDPR have to be made so long as the GDPR allows, with the exemption of the provisions related to the security of personal data and to inspection"*, See SOU 2017:39, p. 102.
35 PDA, Section 7.
36 SOU 2017:39, p. 100.
37 This was not questioned by the Government in the terms of reference though.
38 I.e. Section 7. See SOU 2017:39, p. 101.
39 Remittering av betänkandet SOU 2017:39 Ny dataskyddslag.
40 Id.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

data (publicly accessible information in Finland) and its publication, the Strasbourg Court established that Finland's administrative Supreme Court, which had prohibited the publication, had correctly balanced the protection of privacy against freedom of expression considerations so that no infringement of article 10 ECHR had occurred.[41] Finally the DI argued that the Swedish system of so called *certificate of publication* which extends the constitutional protection of the FLFE to the databases of the entities in possession of such a certificate, whether or not there exists a journalistic purpose, may lead to infringement of privacy.[42]

However, the Datainspektion that wanted the provision to be withdrawn has not been heard by the Government[43] which, as described before, kept the provision and added changes in order to cover the right of access to official documents.

B-An increase of formalism

The Swedish legal system had initially based the protection of personal data on formalities, i.e. procedures prescribed in the Personal Data Protection Act, supervised and enforced by the Data Protection Authority, that to be complied with by data controllers.[44] When evidence was adduced that the data protection supervisor and data controllers were experiencing difficulties enforcing and complying with the formal requirements of the law, [45] the Swedish legislature decided to reduce the formalism on the two abovementioned aspects.

The alleviation of the formalism firstly consisted of suppressing, through provisions in the Act of 1998, the procedures having to be complied with by the data controllers in relation to the data protection authority (.e.g. registration, notification of processing activities, etc.). The Swedish legislator made great use of the possibilities offered by the directive to exempt processing from these kinds of procedures.[46] The data protection reform generated by the GDPR was imbued with a similar philosophy to Sweden's and, in a way, may be said to enshrine the Swedish position, positively impacting on the Swedish data protection regime.

However, the fight against formalism has not been restricted to reducing the procedures that have to be complied with prior to the processing but has also secondly consisted, in Sweden, in suppressing, under certain conditions, the data controllers' obligations to comply with several data protection rules. This special regime, introduced in the Personal Data Act in 2007 and known under the name of *the abuse-centered model,* has not however been renewed on the occasion of the implementation of the GDPR. This may lead to an increase of the formalism in the new Act in comparison to the PDA from 1998.

1) The GDPR leads to fewer preliminary procedures

The Swedish legislature, which made great use of the possibility of exempting processing activities from notification obligations under the Directive (art. 18), uses, after the GDPR reform, the authorization procedure with caution.

The first Swedish Data Protection Act from the 1970's laid down a general obligation for the data controllers to notify the Data Protection Authority of processing activities. Processing activies considered to be especially harmfull for privacy were submitted to an additional authorization procedure by the supervisory authority. About 20 years later, the Swedish legislature that had planned to reduce the formalities surrounding the processing took the opportunity of the transposition of the Directive to reform its law in that direction.[47]

41 The DI interprets this case as when the Parties to the Convention lay down a large openness to personal data, this choice has to be balanced with privacy protection measures which means that public authorities and the courts should be able to make a proportionality appreciation in accordance to the case law of the European court of human rights in the particular cases they handle. This Finnish case, which tackles the freedom of expression in combination to the right of access to information, is of particular interest for Sweden which, as Finland, has a generous right of access to official documents.

42 The procedure for aquiring this certificate is easy and not specifically onerous (about 200 Euros). For more information on this Swedish mechanism see Österdahl, I., Between 250 years of free information and 20 years of EU and Internet, Etikk i praksis, 2016, Vol.10(1), pp.27–44.

43 The Government did not take into consideration the Datainspektion's criticisms. On the contrary it establishes that article 85 of the GDPR gives a larger space for exemptions to the member States than the Data Protection Directive did, not least because the new provision does not requires that the processing shall be carrioud "solely" for journalistic purposes, or the purpose of artistic or literary expression. Moreover the Government put to the forth that recital 153 of the GDPR states that the concept of freedom of expression has to be interpreted broadly. See Prop. 2017/18:105, pp. 41-42.

44 See Blanc-Gonnet Jonason, P., Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle: les exemples français et suédois, Actualité juridique - édition droit administratif, Nº 38, 2008, pp. 2105-2108.

45 According to a survey made 1993 only 10 % of the processing existing in Sweden had been notified to the DI.

46 The Swedish legislator took the opportunity given by the transpostion of the directive 95/46/EC for alleviating the formalism but the idea to carry out such a reform is more ancient in Sweden.

47 The Swedish legislator did actually found the European Act too formalistic and bureaucratic and made the larger use as possible of the possibilities offered by the Directive to lighten the preliminary

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

The Personal Data Act 1998 laid down, as required by the Directive, the principle of the notification for data processing but sets out a large number of exemptions.[48] The non-inclusion of the requirement of notification in the GDPR may be said to suit the Swedish legislator well.

The wish to use as few formalities as possible is also tangible when it comes to the processing that had to be submitted to a procedure of pre-processing checking/ approval. Art 20.1 of the Directive stated that member states had to *"determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof"*, and the Swedish legislator had transposed this provision in the PDA by further delegating to the Government to decide the kinds of processing to be submitted to this procedure. The Personal Data Ordinance had in the past contained such provisions (these were repealed in 2013).[49] So also did some sectoral regulation.[50] The Swedish legislator explicitly expresses its satisfaction that the GDPR, contrary to the Directive, does not require regulation of the question of pre-processing checks.[51] It further assessed that there was no need to delegate in a general manner to the Government, in the DPA, the competence to set out obligations to carry out prior checks. However, there may be reasons to lay down such obligations in sectoral legislation.[52]

2) The GDPR confirms the regulatory model

The Swedish legislator not only wished to reduce the preliminary formalities imposed on the data controllers but also wanted to take the opportunity to introduce a lighter compliance regime. The idea was to replace the regulatory model in place – a law that lays down every step in the processing of personal data – with a so-called abuse-centered model which focuses on uses of personal data considered to be abusive. At first the legislator considered such a model incompatible with the Directive.[53] However, it changed its mind in the middle of the 2000's[54] and carried out a reform to that effect. This consisted of the introduction in 2007 of a provision in the PDA (Section 5a) exempting the processing of personal data that may be deemed processing in *unstructured material* from the majority of the provisions of the PDA. This included *inter alia* the rules on the conditions of legitimation of the processing of personal data, the rules concerning the obligation of information, the rules on rectification, the rules prohibiting the processing of sensitive data and the rules on the transfer to third countries. Thanks to this new provision, continuous texts, for example, published on the Internet or not, or in e-mail were exempt from the processing rules in the PDA, subject to a backstop rule that the processing of personal data in unstructured material should not occur *"if it entails an infringement of the privacy of the person concerned"* (Section 5a in fine, PDA).

This Swedish model is not applicable in the context of the GDPR, which means an increase in the number of rules data controllers who process of personal data have to comply with compared to the position under the abuse-centred rules.[55] The omission of the abuse-centered model will also impact on rule making. Indeed, as stated in the preparatory works when the question of exemptions to the prohibition on processing sensitive personal data is discussed *"the need for exemptions will probably increase"* due to the fact that *"the so called abuse rule in Section 5a of the PDA will not be able to constitute a basis for processing when the GDPR will enter into force"*. [56]

C-The improvement of the data subjects' rights in regard to the Data Protection Authority

Because of the reinforcement of certain existing rights (e.g. the right to information) and of the introduction of new rights (e.g. the right of portability) vis-à-vis the data controllers, the protection of data subjects' rights is generally improved with GDPR compared to the Directive. The strenghening of the protection is also a result of the data subjects' rights as they relate to the Data Protection authorities. Indeed it is a consequence of the introduction of: (1) an explicit right to logde a complaint before the supervisory authority and of the obligations imposed on this authority to examine complaints, and (2) the reinforcement of the

formalities.
48 These exemptions applied when a data protection officer was appointed or according to the exemptions decided by the Government or the supervisory authority.
49 Concerning the processing of genetic data.
50 E.g. concerning processing of personal data regarding the fiscal administration cooperation in criminal investigations.
51 SOU 2017:39, p. 246.
52 Ibid.
53 Sweden hoped that the European institutions would come themselves to the conclusion that the legal framework had to be lightened.
54 The reasons were inter alia the flexible character of the case law of the CJEU and the incentive of the Commission to the member States to make use of the margin of manoeuvre offered by the Directive for processing personal data.
55 The Datainspektion has taken measures on its website in order to make the data controllers aware of the changes in the legislation.
56 SOU 2017:39, p. 181.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

protection is also a result of the introduction of legal remedies against Data Protection Authorities.

1) The right of the data subject to lodge a complaint and the obligation of the supervisory authority to examine the complaint

The Personal data Act did not contain any provision about a data subject's right to lodge complaints to the Data protection authority nor did it contain any legal obligation for the Datainspektion to examine complaints. Nevertheless, the DI claimed on its website that it examined all the complaints, determined whether there was a need for an investigation and informed the complainant of the outcome. The indication provided by the Datainspektion – was not, however, a decision in the legal sense of the term- it did not contain any legally binging obligations to change practice, nor was it subject to appeal or judicial appeal.

The entry into force of the new GDPR constitutes an improvement of data subjects' rights according to the letter of the law as it gives data subjects a legal right to lodge a complaint before the data protection authority (according to article 77.1 GDPR that is directly applicable[57]). Furthemore, the Data protection authority now has an explicit obligation to examine complaints (article 57f GDPR).

This raises the question whether the situation will improve for data subjects. In practice it seems that a decision made by the DI to investigate or not, following a complaint made by a data subject, will not be considered to be a proper "decision". The DI explains on its website that data subjects may leave tips or lodge a complaint to the DI.[58] The supervisory authority explains further that it will decides whether to conduct an investigation and that the data subject will *"get an answer telling him or her if there will be an investigation or not, and why"*.[59] If the "answers" of the DI are not considered to be *"legally binding decisions"*, they will not be subject to an *"effective judicial remedy"* (Article 78 GDPR, see next section). And what about the reason for the decision? Will the rules of the Administrative Procedure Act[60] apply when the DI decide to not investigate?

2) The rights of the data subjects to judicial remedies against the supervisory authority

According to article 78.1 of the GDPR, data subjects *"shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them"* and according to article 78.2 of the GDPR, data subjects *"shall have the right to an effective judicial remedy"* where the supervisory authority *"does not handle a complaint or does not inform the data subject within three months on the progress or outcomes of the complaint lodged"*.

The first paragraph of article 78 has led to the enactment of a provision in the Data Protection Act stating that the decisions of the supervisory authority may be submitted for review by the administrative courts.

The second paragraph is not subject to supplementary provisions in the Data Protection Act, although the terms of reference as well as the committee of inquiry in charge of the first draft of the DPA had proposed to introduce an action for failure to act in the new Swedish law. Indeed, the committee of inquiry had proposed to introduce a mechanism by which the DI would be required, if it had not, within three months, considered the complaints lodged before it, and after a written request has been made by the data subject, to indicate whether or not it intended to exercise supervision, or in a "*specific decision*", reject the request for indication. If the DI had rejected the request for such an indication the data subjet could then lodged an appeal against this decision before an administrative court (claim of delay). If the court granted the appeal, it might have required the monitoring authority to, within a determined time period, give an answer to the data subject regarding the investigation. The decision of the court was not possible to appeal against.

In this way the committee has proposed a mechanism similar to the general action on failure to act that will be introduced in the Administrative Procedure Act that will enter into force in July 2018. In the revised draft, the Government having taken inter alia account of the comments from certain organisations that found

57 The Swedish legislator takes into consideration that the right for the data subject to make complaints as laid down by art 77 of the GDPR is directly applicable and that there is no need to write this right in the new act. Additionally the obligation of the data protection authorities to handle a complaint is laid down by art 57.1 f of the GDPR. SOU 2017:39, p. 306 and Prop. 2017/18:105 p. 152.

58 Under the theme *"The supervisory authorithy's role"* and not under the theme *"The rights of the data subjects"*.

59 The website also informs the potential complainant that all information they send, to the Datainspektion, including the complaints, are considered to be official documents, i.e. covered by the right of access to official documents laid down in the Freedom of the Press Act. The Data protection authority recommends therefore to the complainants to give no more information than necessary and to avoid to provide the DI with sensitive information.

60 In the new version of the Act, which will enter into force in July 2018, the obligation of the public authorities to provide a clear motivation is reinforced.

THE SWEDISH MEASURES ACCOMPANYING THE GDPR by, *Dr. Patricia Jonason*

the system to be unnecessary complicated, time consuming and expensive,[61] decided not to introduce the provision proposed by the committee. No provision at all was actually proposed, the Goverment having considered that the current rules were sufficient for complying with the GDPR. The Government put forth the existence of the directly applicable provision of the GDPR obligating the Data Protection Authority to handle complaints, as well as the provisions of the Swedish Administrative Procedure Act on prompteness and on the obligation to inform. Additionnally the Government referred to the fact that there were no reported cases of unhandled or delayed handling of complaints by the DI[62] and that, if in the exceptional case that a data subject would not get any response from the DI, he/she may logde a complaint with the Ombudsman. The Govermnent also referred to the possibility of a data subject receiving damages according under the Tort Liability Act (1972:207). Lastly, the Government referred to the procedure on failure to act set out in the new Administrative Procedure Act. This procedure, the government says, may be applicable where slow handling occurs in a case initiated by a complaint but *"only against the final decision"*. The Government concluded that *"effective remedies* (effektiviva rättsmedel) *already exist for the data subjects within the Swedish legal order"*. [63] In reality it may be questioned if the Swedish legal order complies with the GDPR, as it looks like there is no *"right to a judicial remedy"*, meaning a right to lodge an appeal to a court, as required by the GDPR in a case where the Datainspektion *"does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint"*. In defence of the Swedish legislator one may mention the limited period of time – about 9 months – the Government had at its disposal to review the first draft of the DPA presented by the committee of inquiry. Another aspect that might have lead to the Government's misunderstanding of the GDPR's requirements might be the partially misleading translation of article 78, in that a *"right to an effective judicial remedy"* has been translated as *"a right to effective remedy"*.

IV-CONCLUSION

The Swedish legislator has accomplished the task of introducing supplementary provisions to the GDPR in a national law with tenacity - delivering a quite satisfactory supplementing act. The new Data Protection Act is, with some exceptions, intrinsingly clear, and its relationship to the GDPR is easy to understand. If one regret is permitted, it is that the short period of time the legislature had at its disposal negatively impacted the final text, not least when it concerns the relationship between data protection legislation and the right of access to official documents and on the question of effective judicial remedies.

61 Prop. 2017/18:105, p. 152.
62 Id., p. 153.
63 Ibid.

THE FRENCH ADAPTATION OF THE GDPR

by Dr. Olivia Tambou

Associate Professor at the Université Paris-Dauphine, PSL Research University, Cr2D. For correspondence: olivia.tambou@dauphine.fr

I-INTRODUCTION

On 20th June 2018 the new Personal Data Protection Act[1] (hereinafter NDPA), which adapts the French law to the General Data Protection Regulation (GDPR)[2] came into force.

The first legislation adopted in France regarding Personal Data Protection was the Act n°78-17 dating from 6 January 1978 also called LIL in French[3]. Despite the appearance of the Internet, the LIL was not modified for 25 years. The first modification[4] was adopted only on 6 August 2004[5] in order to transpose Directive 95/46 EC[6]. At this time, Member States were given three years for this implementation. In France, it took almost nine years because it required a far-reaching reform of the Act n°78-17, which was focused on the public sector. The NDPA is the second most important reform of the LIL. This chapter gives a brief presentation of the accelerated adoption of the NPDA in a first part. It presents an overview of the formal French approach to the adaptation of the GDPR in the second part. The third part gives a preliminary assessment of the approach, highlighting that the French Government has used its margin of manoeuvre moderately such that, the French approach respects the rationale of the GDPR reforms. The fourth part details some of the most disputed points during the adoption process.

II-THE ACCELERATED ADOPTION OF THE NPDA

The Bill was only proposed by the Government on 23 December 2017[7] after the consultation of the *Conseil d'État*[8] and the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, CNIL)[9]. This delay was due to the French presidential and legislative elections, which took place in June 2017. In contrast to the German situation, the French government in charge when the GDPR was adopted, decided to leave the adoption of the French national adaptations to the future elected political majority. Nevertheless, some former parliamentary works had facilitated the adoption of the NDPA. Firstly, data protection and the forthcoming GDPR was at the core of the adoption of the Digital Republic Law[10]. This law introduced in anticipation some news rights for the data subject[11], a collective redress in data protection and stronger enforcement power of the CNIL. Furthermore, the Assemblée Nationale (first chamber of the French Parliament) adopted in February 2017 a report on the impact of the data protection reform on the French Law[12].

1 LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles available at https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte

2 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), OJ L 119/1.

3 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; an English but not updated version is available at https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf accessed 1 March 2018.

4 The Act n°78-17 has been modified by 15 laws since its adoption.

5 Act n° 2004-801.

6 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, OJ L 281/0031.

7 Projet de loi n° 490 relatif à la protection des données personnelles, adopted on 13 December 2017.

8 Avis du Conseil d'État adopted on 7 December 2017 http://www.conseil-etat.fr/Decisions-Avis-Publications/Avis/Selection-des-avis-faisant-l-objet-d-une-communication-particuliere/Adaptation-au-droit-de-l-Union-europeenne-de-la-loi-n-78-17-du-6-janvier-1978-relative-a-l-informatique-aux-fichiers-et-aux-libertes accessed 1 March 2018. In France the Conseil d'Etat is both an administrative Court and an administrative body in charge of giving opinions to the Government including on laws in the legislative procedure.

9 Statement of CNIL, 30 November 2017 (avis de la CNIL Délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978) https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf accessed 1 March 2018.

10 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14

11 i.e. a right to be forgotten for the minors.

12 Rapport Assemblée nationale n°4544, sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française, A.Yvonne le Dain et P. Gosselin, 22 Février 2017, http://www.assemblee-nationale.fr/14/rap-info/i4544.asp

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

The NDPA was adopted in just five months through an accelerated procedure. This was possible because the parliamentary majority gave strong support to the government and the *Assemblée Nationale* overrode the opposition of the *Sénat*. Sixty senators had referred the Bill to the Constitutional Council (hereinafter CC), arguing that it did not conform to French constitutional law. However, the CC confirmed that the Bill was mainly constitutional which enable the Bill to enter into force on 20 June 2018.[13]

III-FRENCH FORMAL APPROACH OF THE NATIONAL ADAPTATION OF THE GDPR

France is part of the group of the Member States[14], which decided to adopt one bill both for the adaptation of the GDPR and the transposition of the Police Directive.[15] Therefore, Part I of the NDPA contains common provisions for the adaptation of the GDPR and the Police Directive. Part II focuses on the use of the margin of manoeuvre. Part III deals with the transposition of the Police Directive.

The implementation of the data protection package takes the form of a significant reshaping of the Data Protection Act of 1978. It was decided to retain but revise this text because it has great symbolic importance[16] in France. The reform proceeded in three different stages: the NDPA, an ordinance, and decrees.

The adoption of the NDPA amended the Data Protection Act of 1978. After the entry into force of the NDPA, the Government had a delegation of law-making authority for six months to rewrite with an ordinance the Data Protection Act of 1978. Simplification, consistency and extensions to overseas territories are the arguments for the use of this legislative technique. The ordinance was adopted on the 12 December 2018 and shall enter into force at the latest on the 1 June 2019 after its ratification by the French Parliament.[17] The ordinance updates twenty-four French Codes such as the code of defence, of education, of home security, and the penal code. The ordinance harmonises, the Codes by using the definition of personal data in art. 4 of the GDPR instead of the term personal information in the LIL. Thus, in the future LIL, the definition of personal information will be removed and replaced with the term personal data. In addition, the complete French adaptation of the data protection package included the revision of the Governmental decree of application of the LIL, which was adopted on 1 August 2018,[18] and the adoption of new decrees. [19] As mentioned before the complete package should enter into force by June 2019 at the latest.

Two observations can be made about the French approach. Firstly, stakeholders have only had clear access to the national adaptation of the GDPR in France since mid-December 2018. This created legal uncertainty at the beginning of the application of the GDPR. Secondly, the NDPA respects the formal obligations of drafting without repeating the text of the GDPR. The NPDA is a compact text of 37 articles[20], with 60 cross-references to the GDPR provisions up to 90 with the ordinance, including the part focused on the transposition of the Directive. Thus, the NDPA and the future LIL is mostly unreadable. The result of this imposed drafting method by the specific nature of the GDPR has been uniformly criticized. The French *Conseil d'État* proposed the introduction of hypertext links to the relevant GDPR provisions when the final

13 See decision n°2018-765 DC du 12 juin 2018, available at https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm. The CC only criticized the fact that the article 13 of the Bill provided that the processing of personal data relating to criminal convictions and offences shall be kept only under the control of official authority, without further explanations. This formulation was a copy-cut the article 10 GDPR as argued the French Government. See points 44-46 of the decision n°2018-765 DC du 12 juin 2018. Thus, final text of the NDPA deleted the criticized expression.

14 This is also the choice of other countries such as Bulgaria, Czech Republic, Greece, Ireland, UK, Slovenia and Slovakia. Other Member States will adopt two laws (one for the GDPR, one for the Police Directive) such as Cyprus, Spain, Denmark, Finland, Hungary, Italia, Lithuania, Luxembourg, Malta, Netherlands and Sweden. See Transposition of the Directive (EU) 2016/680 State of play in the Member States February 2018, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=12946

15 Directive EU 2016/680 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, OJ L 119/89.

16 The Data Protection Act of 1978 has a symbolic significance in French Law, because it deep roots French Data Protection Law in the Freedoms and Liberties of French Citizens. This echoes to the widespread definition of France as the country of the Human Rights and clearly explains why this pioneer and well-known Act is part of the French collective imaginary. This is why the 40th Anniversary of the Act was celebrated with the motto '40 years and always up to date', see https://www.cnil.fr/fr/janvier-2018-40-ans-et-toujours-dans-lair-du-temps accessed 1 March 2018.

17 Ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 d la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n°78-17 du 16 janvier relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel. JORF, du 13 décembre texte 5 available at https://www.legifrance.gouv.fr/eli/ordonnance/2018/12/12/JUSC1829503R/jo/texte

18 Décret n° 2018-687 du 1/08/2018

19 See for instance Décret n° 2018-932 du 29/10/2018 Conditions d'application de l'article L4123-9-1 du code de la défense relatif au traitement des données sur lesquelles figure la mention de la qualité de militaire des personnes concernées

20 In order to facilitate the future drafting work by the above-mentioned ordinance the Directive Police has been transposed in two articles. The article 30 includes in reality art. 70-1 to 70-27 of the futureLIL. Thus, in praxis the NDPA has 62 provisions.

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

text is published in the digital French Official Journal.[21] The senators argued in vain before the CC that this approach was a clear violation of the constitutional objective of accessibility and the comprehensibility of the law[22]. The senators listed several inconsistencies between the wording of the 1978 Act in its reformed version by the NDPA and the GDPR. They considered that it "*could confuse the legal subject regarding the scope of their rights and obligations*". Furthermore, as representative of the regional and local authorities, the senators pointed out the difficulties for French Overseas Countries and territories in which the GDPR should not apply[23]. In such territories, the previous version of the 1978 Act should apply until the ratification of the ordinance, on 1 June 2019 at the latest.

IV-RESPECT OF THE RATIONALE OF THE GDPR REFORM

The NDPA respects the rationale of the GDPR reform, by strengthening the CNIL, reducing prior formalities for processing of data and by using in moderation its margin of discretion.

A-Strengthening the CNIL

The first articles of the NDPA provide one of the most important reforms regarding the CNIL.

Firstly, the NDPA provides the CNIL with new powers in order to guide the stakeholders towards compliance with the GDPR. The NDPA formalizes the expansion of the CNIL's powers to develop soft law[24] such as guidelines, recommendations, and standards ('*référentiels*') for data protection impact assessments.[25] The CNIL may prescribe additional technical and organizational measures for the processing of specific sensitive data such as biometric, genetic, health data and processing of personal data relating to criminal convictions and offences.[26] The CNIL is also provided with a direct power for certification of persons, goods or data systems and processes that comply with the GDPR or the French Data Protection Law. In addition, the CNIL has can accredit certification bodies for the same purposes including with additional requirements in comparison to the national accreditation body, which is in France the *Comité Français d'Accréditation* (COFRAC).[27] During the parliamentary discussions, the Bill was amended in order to specify that the CNIL should have a specific personalised support mission for SMEs, and for the local and regional authorities. [28]

Secondly, the investigation powers of the CNIL are improved. CNIL agents will have a broader right to control and investigate in buildings used for the processing of personal data by the data controller or processor. It includes not only 'professionals' premises, but also common spaces such as corridors. Only professional secrecy between a lawyer and their client, the confidentiality of journalists' sources, and under certain conditions medical secrecy can be invoked against such controls.[29] Furthermore, the NDPA authorizes CNIL agents to use covert identities for their online investigations. In addition, the NPDA provides a framework for joint-investigations. The agents of other DPAs will be able to actively participate in joint operations with CNIL agents, and to take part in investigation hearings of data controllers or processors in France. The President of the CNIL will be in charge to clarify for each investigation the powers of the European agents. In any case, those agents should not have more investigation powers than the CNIL agents could have. The recognition of a potential active participation of agents of other European Member States aims to promote mutual trust with other DPAs, and as basis for mutual recognition. The NPDA also details the interaction between the CNIL and other DPAs when the CNIL will be lead DPA in the one-stop-shop mechanism. However, the implementation of this cooperation will need a decree of the *Conseil d'Etat* adopted after the opinion of the CNIL on procedural guarantees for controllers or processors. When the CNIL is the local authority in the mechanism of consistency, the Chair will be in charge of asking the pertinent structure to answer the lead authority. According to the internal distribution of the competences, the decision could be from the Chair[30] or a restricted Committee[31].

Thirdly, the sanction powers of the CNIL are increased. According to the GDPR, administrative fines can go up to €20 million or 4% of annual global turnover. The NDPA gives the CNIL the possibility to join a periodic

21 Opinion of the French *Conseil d'Etat* mentioned above in n 9.
22 Those principles are provided by articles 4, 5, 6 and 16 of the French constitution, but the CC is reluctant to decide a unconstitutionality on their basis. See decision n°2018-765 DC du 12 juin 2018, points 13-17.
23 See the position of the CNIL in order to clarify the applicable law to the different categories of French Overseas, Comment la Loi "Informatique et Libertés" s'applique t-elle à l'Outer Mer, 13 Juillet 2018 available at https://www.cnil.fr/fr/comment-la-loi-informatique-et-libertes-sapplique-t-elle-loutre-mer
24 In the last years the CNIL has already developed the elaboration with the stakeholders several sectorial 'pack de conformité' (Conformity Pack) such as the Conformity Pack on connected cars, on insurances, on social housing, on smart metering.
25 See art 1 of NDPA.
26 In relation to art 10 GDPR.
27 This will need a decree adopted in the *Conseil d'Etat* and after the opinion of the CNIL. The possibility of additional requirements established by a DPA of the accreditation of a certification body is provided by art 43(1) GDPR.
28 See the new art. 11 of the 1978 Act.
29 See art 5 of the NDPA.
30 This is the case for a warning or a formal notice.
31 This is the case for a reminder, an injunction to ensure conformity, the withdrawal of a certification or a BCR, of the suspension of a data transfer to a third country, the imposition of administrative fines.

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

penalty (with a maximum limit of €100,000 per day) to the administrative fines. However, it will not be possible to impose administrative fines for processing by the State[32]. Lastly, the ordinance introduces a new penalty for obstructing the actions of the CNIL. This includes different form of obstruction such as non-communication of documents requested, dissimulation of documentation, and communication of falsified information. These behaviours shall be punished by (up to) one year in prison and a fine of (up to) 15 000 €[33].

Fourthly, the CNIL obtains the right to refer to the judge in two situations. Firstly, in a *Schrems*-type[34] situation, when the CNIL receives a complaint from a data subject about the validity of an adequacy decision.[35] Secondly, the CNIL is permitted to present observations before a judge in litigation regarding the GDPR or the NDPA.

Fifthly, the tasks of the CNIL are enlarged. The *Assemblée Nationale* amended the French Bill in order to give to the CNIL the task of awareness-raising activities among consumer mediators and public ombudsmen.[36] This change takes into account that mediators are increasingly confronted with issues relating to personal data protection in conflicts between consumers and professionals or between administrations and users. Therefore, the CNIL should train and educate these mediators/ombudsmen about the rights of data subjects and the new rules provided by the GDPR or the NDPA. In addition, the CNIL obtains the right to be consulted not only by the Government on a bill, but also by the Parliament on a draft law related to personal data protection or the processing of personal data. The *Assemblée Nationale* extended this possibility by providing this right not only to Parliament Committees, but also to political groups[37]. Thus, the parliamentary opposition could require an opinion from the CNIL regarding a bill on personal data protection or on the processing of personal data[38]. Nevertheless, consultation of the CNIL is only compulsory on normative governmental activity such as the Bill, decree or provision of a Bill or decree on data protection or processing of personal data[39].

Finally, the French Bill improves the internal rules of procedure of the CNIL. In order to comply with the independence criteria, members of the CNIL will deliberate in the absence of agents of the CNIL and the Government Commissioner will not be present in deliberations either. The *Assemblée Nationale* added the obligation for the CNIL to publish the agenda of the plenary Commission in order to improve the transparency.

During the parliamentary debate, the expansion of the mission of the CNIL raised the question of its capacity to assume its new role, in particular regarding its human and financial resources[40]. However, the French Government underlined that the means of the CNIL have increased since 2010. The amount of the budget of the CNIL for 2018 is €17.6 million, an increase of €600,000 compared to 2017. The CNIL employed 200 staff in 2018 and should receive in 2019, 15 extra staff

B-Moderate Uses of Margin of Manoeuvre

The European data protection reform leads to a deep transformation of national data protection laws, which will be now mainly appropriate for specific situations. This causes fragmentation between national and European provisions, between a general and sectorial legal framework regarding certain types of data (sensitive data, health data, personal data relating to criminal convictions and offences) or certain activities in a sector (police, justice, marketing, employment, etc.) or certain categories of controllers (public authorities) and/or certain purposes of processing (journalistic purposes, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, etc.). These specific situations will not be analysed here[41]. This section will instead present some

32 This notion is defined strictly does not comprise the processing of the regional and local authorities contrary to what the senators had wanted.
33 See art. 13 of the ordinance 2018-1125.
34 Case C-362/14 *Schrems* (2015) ECLI:EU:C:2015:650.
35 See art 27 of NDPA.
36 See art 11 j) NDPA.
37 According to the French law, a political group is formed with a minimum of 15 Parliament Members.
38 The modalities of the new consultation had been discussed between the two assemblies. The senators would have liked a more effective right to consultation including simply provision related to Data protection Law such as an amendment presented during the discussion. The insufficient clarification of this right to consultation is also one of the arguments of the request before the CC. The senators argued that it would be up to the legislator to define when the request of consultation should be introduced and the deadline for the response of the CNIL, as it is the case for the consultation of the CNIL by the government. The CC did not accepted the argument of the Senators. See Decision n°2018-765 DC du 12 juin 2018 points 13-17.
39 The scope of this compulsory consultation of the CNIL has been broadly interpreted by the Conseil d'Etat see its decision n° 408185 20 June 2018 point 2. Available at https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034017907
40 A recent study pointed important national differences regarding the DPA Budget and staff in the world. According to this study the DPAs located in North America have the highest budget and most staff. However this study does not take really into account the specificities of the European Member States of the EU and give a partial overview of this matter. See Müge Fazlioglu, How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population available at https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/01/DPA-Budget-and-Staffing-White-paper.pdf accessed 1 March 2018.
41 The NDPA also introduce a special legal framework for health see Vlad Titerlea, Winds of Change Blow across Health Data in France, blogdroiteuropéen June 2018 available at https://wp.me/p6OB-GR-2ZA

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

specific illustrations of the French uses of the margin of discretion.

1) The Limitation of the Prior Formalities

Only processing on genetic and biometric data of the State acting in the exercise of its public powers will need a prior authorization[42]. This is the counterpart of the principle of accountability of the controller and processor introduced in the GDPR. The ordinance goes further by deleting the need for an authorisation for before the implementation of an automated measure of the audience on an advertising medium or the analysis of the typology or the behavioural of individuals while walking by billboards[43]. This could seem odds given that the CNIL recently denied such an authorisation in the *J Decaux* case[44].

2) Provision on the Law Applicable in Cross-Border Cases

France added a provision regarding the law applicable in cross-border cases in the exercise of the national derogation[45]. This provision aims to resolve potential horizontal conflicts between national laws regarding the implementation of opening clauses. The NDPA uses residence criteria in order to protect the fundamental rights of the data subject. The NDPA provides an exception for processing carried out for journalistic purposes. In this situation, the establishment criterion will apply. This provision could produce a conflict with Member states, which use an alternative criterion. This also creates a complex fragmentation of the territorial scope of the data protection rules.

3) A Derogation for the Communication of Personal Data Breach

The NDPA uses in moderation the possibilities of restrictions of data subject rights laid down in Article 23 GDPR. Article 24 NDPA provides a legal basis for not communicating a data breaches to a data subject when the processing is covered by a legal obligation, and when it is necessary in the public interest and if there is a risk to national security, national defence or public security. In addition, a decree should provide a list of processing to which this strict derogation could apply.

V-MOST DISPUTED TOPICS REGARDING THE ADOPTION OF THE NDPA

This section of the report presents a selection of five topics, which have been at the core of the discussion.

A-The Uses of the Opening Clauses in the context of the Algorithmic Decisions

The provision on automated individual decisions, which adapts Article 22 GDPR, has been at the core of the French debate. Each paragraph of art. 21 NPDA was debated intensely by the government and the assemblies. The only exception is the prohibition of automated decision-making of judicial decisions based on the use of personal data to evaluate certain aspects relating to a natural person and which produces legal effect on the data subject or similarly affects them. This prohibition was already laid down in art. 10 of the 1978 Act.

The wording of Art. 21 retains a prohibition[46] on decisions based solely on automated processing. Such decisions are prohibited as a principle without requiring a specific action of the data subject. Nevertheless, the rationale of this provision is to secure the development of the practical need of algorithmic decisions by adding measures to safeguard data subject's rights. Therefore, Art. 21 sets up a general legal framework for the processing of individual decisions solely based on automated processing in relation to Art. 22 (2) GDPR and its opening clauses. Furthermore, art. 21 provides a specific legal basis for a systematic use of administrative individual decisions solely based on automated processing.

1) General Legal Framework for the Implementation of the Individual Decisions Solely Based on Automated Processing

The NDPA introduces two kinds of guarantees in order to give data subjects a comprehensive overview of the implementation of individual decisions solely based on

42 Art. 11 NDPA.
43 See art.9 of the Ordinance. This authorisation was included in the article L.581-9 environmental code.
44 In this JC Decaux case this company tried to create a processing for the purpose of to test a methodology in order to estimate pedestrian flow in the Defense district in Paris. The advertisement company wanted to install and exploit WIFI boxes capable of tracking the addresses of a mobile phone which WIFI would be activated within a distance of 25 meters. The processing had a clear commercial purpose: to be able to adapt the ad board tariff to the number of pedestrians in the zone, but not a behavioural targeting one. The refusal was based on the lack of consent of data subjects. The CNIL observed that the data controller did not have a legitimate interest to oppose the lack of consent of the data subject. The main reason was the inadequate information of the data subject. (Only a small board which was not readable by all data subjects). Thus, the lawfulness of the collection was not respected. Furthermore, the CNIL referred to the non-respect of the proportionality between the risks of the processing and the guarantees created for the right of the data subject. See the CNIL deliberation n°2015-255 on 16 July 2015, confirmed by the CE in its decision n°393714 on the 8 February 2017 available at https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034017907.
45 Art. 10 NDPA.
46 The wording does not refer to the right not to be subject to a decision based solely on automated processing including profiling. Nevertheless this prohibition approach had been clearly endorsed by the G29 and now European Data Protection Board see WP251 Rev. 01, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Adopted on 3 October 2017 as Last Revised and Adopted on 6 February 2018, p. 19.

automated processing.

Generalization of the right to obtain a human intervention

The Bill did not refer to the right to have a form of human intervention on the part of the controller so that the data subject could express their point of view or contest the decision. The Government seemed to consider that this obligation concerned only the contractual or explicit consent derogations according to Article 22 (2) a) and c), but not the situation of the legal derogations of Article 22 (2) b). It is true that Article 22 (2) b) only refers to the need to lay down 'suitable measures to safeguard the data subject's right and freedoms and legitimate interests'. However, this interpretation was questionable. One could argue that the right to obtain a human intervention should be at least one of these suitable measures. Therefore, the final version of Art. 21 NDPA required the same guarantees for all individual decisions solely based on automated processing which produces legal effect on the data subject or similarly affects them.

Introduction of a Real Right to Explanation

There has been some debate whether Art. 22 GDPR includes a "right to explanation" of the decisions solely on automated processing, including profiling[47]. The right to explanation should go further than "the right to meaningful information about the logic involved", provided by Art. 13 and 14 GDPR. Those provisions contain only a right to an ex-ante abstract explanation of the functionality of the machine decision. A real right to explanation should grant ex-post information on how and why a specific individual automated decision has been made. The main argument for rejecting the creation of such right to explanation is based on the evolution of the wording of Art. 22 (3) in the draft of the GDPR. The explicit introduction of a right to explanation by the European Parliament[48] was deleted from the final version of the GDPR text. Thus, recital 71 contains the only reference to a right to explanation,[49] and although recitals are not legally binding,[50] they are important in European Law.[51]

Art. 21 NPDA clearly sets out an ex-post right to explanation. The rules regarding the processing and the main features of its implementation should be communicated by the controller to the data subject. This includes the possibility to have access to the source code of the algorithm in order to assess it. However, the communication needs a request from the data subject. This is why it is important that the data subject have correct prior information of the existence of the automated processing decision. Furthermore, the controller can refuse the communication when it interferes with secrecy covered by law.

Despite all these guarantees, the right to explanation raises the issue of how the data controller and processor will implement it and whether it will be effective for the data subject.

2) A Legal Basis for a Systematic Use of Administrative Individual Decisions Solely Based on Automated Processing

Art. 21 of the NDPA provides a legal basis for systematic use of individual administrative decisions based solely on automated processing. The purpose is to create a legal framework that facilitates the practical needs of administrative algorithmic decisions in order to improve their efficiency. The final version provides following guarantees.

Firstly, art. 21 NDPA lays down that individual administrative decisions based solely on automated processing are excluded in various situations. The use of automated decisions for the processing of sensitive data is excluded. This should not concern the administrative complaints ("recours gracieux")[52].

Secondly, it recalls transparency rules introduced by

47See eg Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "right to Explanation"' [2016] arXiv:1606.08813 [cs, stat] <http://arxiv.org/abs/1606.08813> accessed 24 August 2017; Wachter S, Mittelstad B, Floridi L (2017) Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law 7, n°2, p. 76.

48 See European Parliament Art. 20 5)adopted on the 12 March 2004 on its first reading : *Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including* ***an explanation of the decision reached after such an assessment.*** The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 *shall include the right to obtain human assessment and* ***an explanation of the decision reached after such assessment.*** [Bold added]

49 "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, **to obtain an explanation of the decision reached after such assessment [Bold added]** and to challenge the decision."

50 see, e.g., ECJ Case C-308/97, 25 November 1998, *Giuseppe Manfredi v. Regione Puglia*, para. 29–30, ECLI:EU:C:1998:566; ECJ Case C-162/97, 19 November 1998, *Criminal Proceedings against Nilsson, Hagelgren & Arrborn*, para. 54, ECLI:EU:C:1998:554.

51 K. Tadas and J.Vaisciukaite, *The Law of Recitals in the European Community Legislation*, ISLA Journal of International & Comparative Law, Vol. 15, 2008, Available at SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604, accessed 24 August 2017

52 In French administrative law « recours gracieux » are petitions against an administrative decision that the data subject can bring before the same administrative authority which takes the decision, and then appeal to the hierarchical authority.

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

the Digital Republic Law from 2016[53]. Administrative algorithmic decisions need to make explicit reference to the use of automated-processing decision making. The lack of this explicit reference is a cause for annulment of the administrative decision.

Thirdly, controllers have an obligation to control algorithm and their development. This obligation aims to allow the data controller to explain in detail and in an intelligible manner the implementation of the processing to the data subject. This obligation excluded as the CC said the machine learning algorithms of the scope of the legal basis. Such machine learning algorithms could make it impossible to the controller to explain their decisions[54]. This also implied that the administration should not use algorithms covered by property rights, which logic cannot be shared with the data subject[55].Thus, the will of the French legislator is to design a model of transparency of algorithmic decisions that complies with its political commitment to Open government[56]. One year later, the implementation of the guarantees introduced by the Digital Republic Law seems to be problematic. It requires a huge change in both the French administrative culture and resources.

The implementation of a platform for the registration at the University by the Minister Ministry of Higher Education has been at the core of the debate on administrative algorithmic decisions. The first platform called APB was invalidated by the CNIL[57] because it did not conform to the prohibition on administrative individual decisions based solely on automated processing. The algorithm made decisions on the degree that the students had to follow without human intervention. The new platform called *Parcoursup*, improves the original platform one by offering two potential opportunities for human intervention. It only collects the data and the course preferences of the future students. Nevertheless, the universities have to list the candidates they accept taking into account the prerequisites needed for performing the degree and logistical considerations[58]. In other words, the Ministry has tasked the University with a new mission of management of the "selection" of the candidates[59] who can register in their universities after the baccalaureate. *Parcoursup* was authorized by a ministerial ruling[60] after a positive opinion delivered by the CNIL during the parliamentary debate of the NDPA[61]. The government made public the new algorithm code later in May[62]. 900 000 aspiring students used *Parcoursup*. 7 million course preferences needed to be processed. In order to complete this task, Universities developed local algorithms. This raised the issue of whether these algorithms also needed to be made public. The new law regarding the orientation and success of the students adopted in March 2018 gave a margin of discretion to the universities. Art. L-612-3 of the code of Education provides that the rules of transparency of the algorithms are satisfied when "*the candidates are informed of the possibility to obtain the communication of the information regarding the criterion and the modalities of their applications and the pedagogical grounds of the final decision*". This provision has been seen by the senators as an exception to the transparency principle of the Digital Republic Law. The senators challenged its compatibility with the principles of accessibility and intelligibility of the law. It is also not very clear whether it conforms with the GDPR. The only guarantee introduced is that an ethics and scientific committee should inform the Parliament on the implementation of *Parcoursup* on an annual basis[63]. This committee can make proposals in order to improve the transparency of the system.

In conclusion, the pressure on University administrators to comply with the obligations of information and explanation of the administrative algorithmic decisions are strengthened by the application of the GDPR[64]. If the clarifications of the CC mentioned above are useful, it is still unclear whether art. 22 can authorise a Member State to implement such a huge derogation by introducing a legal basis for the systematic use of administrative algorithmic decisions.

B-The impact of the GDPR on specific situations

1) The need to consider the protection of the Child

Age of Consent for Children in Relation to Information Society Services: As in other countries, the age of

53 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
54 See decision n°2018-765 DC du 12 juin 2018, point 71.
55 See ibid point 70.
56 See https://www.etalab.gouv.fr/gouvernement-ouvert.
57 Décision n°2017-053 du 30 aout 2017, mettant en demeure le ministère de l'Enseignement supérieur de la Recherche et de l'Innovation.
58 In particular their capacities.
59 This became one reason for a strike movement in universities which blockage in exam periods. See for instance https://www.huffingtonpost.fr/2018/04/13/greve-des-universites-mais-que-reclament-les-etudiants_a_23410458/
60 Arrêté du 19 janvier 2018 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé Parcoursup.
61 Décision n°2018-119 du 22 mars 2018 portant avis sur le projet d'arrêté autorisant la mise en œuvre d'un traitement de données à caractère personnel dénommé Parcoursup.
62 See http://ingenuingenieur.blog.lemonde.fr/2018/05/29/parcoursup-2018-les-dessous-de-lalgorithme-racontes-par-ses-createurs/
63 See the first report of this committee Rapport au Parlement du Comité éthique et scientifique de Parcoursup, Documentation française, 21 janvier 2019, available at https://www.ladocumentationfrancaise.fr/rapports-publics/194000051-rapport-au-parlement-du-comite-ethique-et-scientifique-de-parcoursup
64 See also the criticism of the Mediateur des Droits regarding the lack of transparency in the selection process of Parcoursup in particular the décision n°2019-021.

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

consent for children in relation to information society services was strongly debated in France. The French Bill provided no specification on this matter. The French Government and the Senat wanted to apply the limit of 16 years old as laid down in Article 8(1) GDPR. The *Assemblée Nationale* proposed to reduce the threshold to 15 years of age, which is the age finally adopted.[65] The change was founded on the need to align the age limit with the age of sexual majority and the age of the capacity to consent to medical/health procedures. Nevertheless the final version of Art. Art. 20 NDPA also provides that when a minor is less than 15 years old, both the parent/guardian and the child should give consent. This double consent seems to go beyond the conditions of the Art. 8 GDPR, as the senators argued in their request before the CC. The CC did not follow this argument. It considered that article 8 GDPR distinguishes between the given-consent (by a child that has capacity to consent) and the authorised-consent by the holder of parental responsibility over a child that does not have capacity to consent. According to the CC this means consent can be given by the parents of a minor or that the parents can authorise a minor to consent[66]. This second situation enables double consent. It is likely that this will be the subject of an ECJ case at some point in the future. France appears to be the only Member State to introduce double consent, and it is arguably incompliant with Art 8 of the GDPR.

Some additional guarantees try to take into account the reality of the digital uses by minors. For example, controllers have an obligation to inform data subjects aged less than 15 years old in 'clear and easily accessible language' when they collect their data.[67] Also, Art. 22 of the NDPA introduces a new obligation for public schools to make available a public register of their processing.[68] Furthermore, Art. 1 of the NDPA provides that the CNIL should develop and promote a of code of conduct regarding the obligations of controllers processing children's data.

2) The Local and Regional Government Entities Concerns

The *Sénat* did not succeed in introducing in the NDPA some funding to address the economic impact of the implementation of the GDPR on regional and local government entities. Furthermore, the NDPA authorizes administrative sanctions against regional and local government entities, where such sanctions are excluded for processing of the State.

Nevertheless, the *Sénat* obtained small concessions. For instance, art 31 of the NDPA permits regional and local government entities to conclude between themselves an agreement to provide services regarding processing of personal data. The regional and local entities government are also allowed to create a unified department in order to assume in common the charges and the obligations related to personal data processing.

C-The "Qwant" Amendment

Art. 28 of the NDPA, aims to give more control to a data subject of the choice of application they can use on devices such as a smartphone, a laptop, a digital tablet, etc. It fights against the default of the pre-installation of applications without alternative services, which could be more privacy friendly. It clarifies that consent is not free, informed and specific when the final choice of the consumer is limited by imposing application settings without legitimate interest, technical or security considerations. This amendment is often described as a means for promoting the French search engine, Qwant, which presents itself as an alternative to Google with enhanced data protection functionality. Art 28 of the NDPA could have a strong impact on developers and operators by creating a market for different kinds of applications. This could, however, create practical difficulties, and create consumer dissatisfaction when they are required to bear the cost of the applications business model transformation.[69]

D-The Introduction of a Collective Action for Damage[70]

The *Assemblée Nationale* introduced the possibility of a collective action for damage[71], when the Government did not use the margin of discretion in Article 80 GDPR. The purpose of this collective action is to claim compensation for material and non-material damages. This change was expected. The '*action de groupe*' was first introduced into French Law in 2014[72] in respect of consumer litigation. It is only recently, in 2016, that

65 In the debate, the European Affairs Committee proposed to lower the age threshold to 13 years old, in order to converge with other Member States choices and curiously to avoid technical difficulties for the controller to assess the real age of the minor. See Avis n° 577, 20-21. For a recent report of the age of consent chosen across the EU Member States, see Ingrida Milkaite and Eva Lievens, 'Updated mapping of the age of consent in GDPR' (8 February 2018) https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2733703 accessed 1 March 2018.
66 See decision n°2018-765 DC du 12 juin 2018, point 63.
67 See art 14 bis nouveau of the proposal adopted by the Assemblée Nationale.
68 See art. L. 121-4-1 French Code of Education.
69 See for instance Benoit Felten, Données personnelles ne fragilisons pas l'écosystème mobile, Les Échos 11 May 2018, https://www.lesechos.fr/idees-debats/cercle/0301665742032-donnees-personnelles-ne-fragilisons-pas-lecosysteme-mobile-2175257.php
70 For more comparative details on this topic See: the contribution of Alexia Pato on p.94
71 See art 16 A nouveau of the proposal adopted by the Assemblée Nationale.
72 Loi n° 2014-344 du 17 mars 2014 relative à la consommation

THE FRENCH ADAPTATION OF THE GDPR, by *Dr. Olivia Tambou*

the scope of the collective actions was extended to various sectors including personal data protection.[73] However, the scope of this collective action was limited to the cessation of the violation. The Government and the Sénat proposed maintaining the status quo. The Assemblée Nationale was motivated to expand the scope of the collective action to include awards compensation for three reasons. Firstly, the collective action in data protection was the only one under French law to be limited to the cessation of the violation. Secondly, the enlargement should improve the effectiveness of the collective action in France. Thirdly, this change aims to give effect to the rights given by the GDPR to data subjects, as it had been argued that some Member States already had collective action for damages. The individual procedure of compensation for damages will apply.[74] It would be up to an individual, after the decision of the judge on the liability, to ask the data controller for damages. Art. 25 of the NDPA clarifies that this collective action can only apply to damages having occurred after May 25, 2018.

The legal action initiated by the Quadrature du Net on Monday 28 May 2018[75] are based on the possibility according to 77 GDPR to bring a (collective/action de groupe) complaint against a data controller before the CNIL[76]. It has led to a first post-GDPR €50 million fine against the company GOOGLE LLC,) for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization[77].

E-The processing of personal data relating to criminal convictions and offences

The NDPA provides two sets of rules regarding the processing of personal data relating to criminal convictions and offences, as permitted by Art 10 GDPR.

Firstly, art. 13 of the NDPA extends the legal basis of processing of personal data relating to criminal convictions and offences or related security measures based on art. 6 (1) GDPR beyond public authorities to private entities. Art. 13 of the NDPA opens up two such possibilities. Firstly, it could be processing by a legal person in cooperation with the Justice system. In such a situation, two guarantees have been introduced. These private legal persons should be listed under a future decree, which needs to be adopted in the Conseil d'Etat after publication of the opinion of the CNIL. This should limit and give more detail on the concerned legal persons. Furthermore, the processing should be strictly necessary for the missions of this legal person. Art. 13 of the NDPA provide an additional possibility for legal and natural person processing in order to initiate and follow a judicial action. This is limited to processing realised by victims or their representatives. A cumulative condition has been added, namely that the purpose of the processing should be the enforcement of a judicial decision. The data retention is strictly limited to these purposes. No transmission to third parties is allowed except if those same conditions are fulfilled.

The senators argued before the CC that this is an excessive enlargement to private entities of the criminal processing which is not conform to the French constitutional identity and that more safeguards needed to be included in the law itself. They considered, in particular, that such processing should be authorized by the CNIL as a prior formality. The CC rejected all these arguments. It considered that the legislator pursed a general interest and that the law gave sufficient safeguards and limits for these derogations[78].

Secondly, a special provision for the Legal tech has been introduced. It only recalls that the reuse of public judgements is allowed if the re-identification of the person is not possible.

VI-CONCLUSION

In conclusion, the NPDA is based on a balanced approach, which tries to compensate for the limitations of data subject rights by introducing safeguards. The strengthening of the CNIL respects the law enforcement focus of the European data protection reform. The opening clauses are mostly used for the benefit of the public authorities as the authorization for a systematic use of administrative individual decisions solely based on automated processing illustrates. The added value of the Assemblée Nationale's amendment decision is the introduction of a collective action for damage, which could benefit data subjects. The NDPA also tries to pragmatically implement the European data protection reform. This is why the Assemblée Nationale introduced provisions that take into account the impact of the reform on SMEs and lowered the threshold for the child's consent to 15 years old, in reflection of the age at which children routinely use information society services in France. Nevertheless, they are still legal uncertainties due to the French approach of the GDPR adaptation. It is most likely that the judges including the European Court of Justice will need to clarify to what extend some French provisions are conform to the GDPR.

73 Title V of the law n° 2016-1547 of November 18th, 2016 of modernization of justice of the 21st century (loi de modernisation de la justice du XXIe siècle).
74 See ch X of title VII of Book VII of the Administrative Justice Code (code de justice administrative) and ch I of title V of the law n° 2016-1547 of 18 November 2016 on modernisation of justice of the 21st century (loi de modernisation de la justice du XXIe siècle).
75 See dépôts de plaintes collectives contre les GAFAM, La Quadrature du Net, https://www.laquadrature.net/fr/depot_plainte_gafam
76 See art. 26 NDPA.
77 See our comment on the European Data Protection Law Review 1/2019, forthcomming
78 See CC Decision n°2018-765 DC point 47-53.

THE DANISH ADAPTATION OF THE GDPR

By Tenna Overby
Head of Section, POLITI, Danish National Police, Police Directorate, Data Protection Unit

I-INTRODUCTION

After several months of work, the Ministry of Justice finally presented the draft of the new Data Protection Act, which after three readings in Parliament was adopted with a majority on 17th May 2018. No members of Parliament voted against it. It entered into force on 25 May 2018 and replaced the existing Act on Processing of Personal Data and adapt the GDPR.

The purpose of this paper is to introduce the main content of the Data Protection Act. The paper briefly introduces the origin of the Danish data protection legislation, presents the Data Protection Act project and summarises key provisions and comments on the most interesting use of opening clauses in the Data Protection Act.

II-LEGAL FRAMEWORK BEFORE THE GDPR

The first Danish data protection laws, the Public Authorities' Registries Act and the Private Registry Act[1], were adopted in 1979. With this legislation Denmark was one of the first countries in Europe, together with West Germany, Sweden, Norway and France, which implemented a regular data protection law.

In 2000, the Registries Acts were repealed with the adoption of the Act on Processing of Personal Data (hereinafter the Privacy Act), [2] which implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [3] In the implementation process, it was decided to codify the two pre-existing data protection laws into one consolidated law that included both public authorities and private actors, as this was deemed more accessible for the data subjects.

In the past 18 years, the Privacy Act has with its continuous amendments provided the framework for data protection law.

III. THE DATA PROTECTION ACT PROJECT AND THE MAIN CONTENT

The Data Protection Act was drafted by Ministry of Justice's Data Protection Office. The Data Protection Act is based on a recommendation report from the Ministry of Justice published on 24 May 2017 containing an analysis on existing data protection regulation and the GDPR, including the possibility of using opening clauses. [4] The first draft of the Data Protection Act was published for public consultation on 7 July 2017, and finally, with a few amendments the draft was presented for the Parliament on 25 October 2017 for its first of three readings.

The Data Protection Act supplements the GDPR and consists of 48 articles distributed in seven sections. The seven sections are dedicated, respectively, to 1) introductory provisions, 2) processing of personal data, 3) rights of the data subject, 4) additional provisions to Chapter IV of the GDPR, 5) prior consultation, 6) independent supervisory authorities, 7) remedies, liability, penalties and concluding remarks.

The Data Protection Act introduces provisions referring to the GDPR and provides provisions developing the GDPR opening clauses. Further the Data Protection Act continues several provisions and principles carried over from the Privacy Act.

1 Public Authorities' Registers Act, law no. 294 of 8 June 1978 and Private Registers Act, law no. 293 of 8 June 1978.
2 https://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ (English)
3 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 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (English)
4 *Recommendation no. 1565 on GDPR and the legal framework for Danish legislation.* (24 May 2017). http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa (Danish)

DANISH ADAPTATION OF THE GDPR by, *Tenna Overby*

Several provisions in the Data Protection Act repeat the language of the GDPR, which makes for a case of double regulation. The rationale behind is to avoid any misinterpretations between the GDPR and the national data protection law. However, this might result in a complex legal position, since two legal texts must be consulted and compared before deciding what the legal position in an area is.

IV-MATERIAL SCOPE AND GEOGRAPHICAL SCOPE

The material scope of the Data Protection Act is broader than the material scope of the GDPR and includes manual disclosure of personal data between public authorities, processing of company data if the processing is performed for credit agencies, and all processing of personal data in connection with television surveillance. Further, it includes processing of personal data of deceased persons in up until 10 years after their death.[5] The GDPR applies to all areas set out in the Data Protection Act.

The Data Protection Act applies only for processing of personal data by a data controllers and data processors established in Denmark. This means that data processing activities in Greenland and the Faroe Islands - which both are part of the Danish Kingdom - are not covered in the geographical scope of the Data Protection Act. Due to the two countries legal status in EU as non-members of the EU, Greenland and the Faroe Islands has their own national data protection legislation. This position has resulted in some fairly complex legal issues over the years as some public authorities across Denmark, Greenland and the Faroe Island to a some extend is exchanging personal data due to unity of the Realm.

V-USE OF OPENING CLAUSES

Due to its direct applicability in national law, the GDPR leaves no possibility for derogating national legislation of the EU member states except when explicitly allowed for it by the GDPR.[6] The GDPR's opening clauses have allowed the Ministry of Justice, pursuant to the specific terms of each provision, to replace, complement or further specify the provisions of the GDPR. As a result the Data Protection Act contains a significant number of provisions that either modify or derogate from the GDPR. These modifications and derogations are largely used for the purpose of giving public authorities a wider access to process personal data and to limit data subject rights. To some extent, this undermines the harmonisation objectivities in regard to harmonisation between the public- and private sector. Further, the use of opening clauses limits the objectivities in regard to data subjects' rights. Nonetheless, it follows from the GDPR that the right to protection of personal data is not an absolute right but must be balanced against other fundamental rights and must be considered in relation to its function in society.[7] It seems that the latter has had an especially big impact in the drafting process of the Danish Data Protection Act.

A-Extension of public authorities' right to process person data

Under Article 5, para 1 (b) of the GDPR personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, change of the data processing purpose after the data has been collected can be lawful under certain conditions set out in Article 6, para 4 GDPR, including if the change of purpose is based on member state law that constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives laid down in Article 23 GDPR. On this basis, the Data Protection Act empowers any minister under its relevant political area to issue executive orders, in negotiation with the Minister of Justice, and legislate on when personal data can be used for other purposes than they initially were collected for.[8] The provision constitutes an extension of public authorities' right to process personal data, which may include the right to re-use personal data and to disclose personal data to other public authorities. In comparison to the pre-existing Privacy Act, the provision gives the relevant minister more legislative power than previous, whereas certain processing of personal data for other purposes than they initially were collected for, must rely on legislation adopted in the Parliament.

B- Restrictions of data subject rights

According to Article 23 GDPR, member states are allowed to restrict the scope of the data subject rights and corresponding obligations when such restrictions respect the essence of the fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard certain objectives that are enumerated in the provision. Based on this provision, member states can introduce legislation that limits subject

5 Recital 27 GDPR.
6 P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, (2017) 219-223.
7 Recital 4 GDPR.
8 The Data Protection Act § 5, para 3.

DANISH ADAPTATION OF THE GDPR by, *Tenna Overby*

rights to a rather large extent, particularly under the objective "other important objectives of general public interest".[9] In a Danish context this provision has been used to restrict the data subject's right with regard to the information obligation of the controller prior to processing. This implies that public authorities are exempted from giving information to the data subject when the authorities are processing personal data for purposes other than for which it was initially collected. As a consequence, the data subject will not be informed if his or her personal data is disclosed to another public authority. This restriction was criticised during the public consultation stage of enacting the Data Protection Act.[10] However, the Ministry of Justice did not revoke or change the provision. According to the general remarks set out in the Data Protection Act regarding the provision, the Ministry of Justice stated that from a data controller's point of view, the information obligation would be too administratively burdensome. Furthermore, the remarks state that it is questionable whether the information obligation of the controller posed by the GDPR actually provides for legal certainty for the data subjects when public authorities are changing the purpose of data processing.

Additionally, the Data Protection Act provides that the subject's right to information and to access to information can be restricted with regard to processing of personal data by the courts, processing of data for scientific research purposes and processing of personal data in criminal investigation as compliance with such rights may be damaging to public interest or too burdensome on the respective processor.

C-Processing for scientific research purposes

Danish data protection legislation has always provided a fairly wide legal framework for processing of personal data for scientific research purposes based on personal data included in various registries. This includes registries as for example the Civil Registration System (CPR), containing basic personal data on all who have a civil registration number[11] or the Danish Neonatal Screening Biobank (DNSB) that has been collecting blood sample material from all newborns who have been tested for serious congenital disorders[12] since 1982. On 29 May 2018, the Danish Parliament adopted a new Act to establish a National Genome Center whose main objective is to analyse genetic data for the purpose of research and for the purpose of customising future medicine and treatments that match the individual patient.[13]

Under the negotiations leading up to the GDPR, processing for scientific research purposes was a sensitive issue from a Danish perspective. In Denmark scientific research – namely health research – is common and widely accepted as it is considered reasonable to use these data for the purpose of scientific research.[14] The pre-existing Privacy Act provided that processing for scientific research was allowed without consent from the data subject.[15] This is not considered to be a violation of the personal integrity of the data subject if the research result is not published in a way that can identify the data subject. Conversely, it is almost considered as indefensible not to re-use collected personal data for legitimate purposes for scientific research. While this may not be widespread in other EU member states, the prospect of maintaining the legal basis for such processing was of major concern for Denmark under the negotiations of GDPR.[16] As a result, one of the most important Danish imprints on the GDPR is found in Article 89.

Article 89 GDPR provides the legal basis for processing activities for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and lays down minimum standards applicable for such processing. Article 89, para 2 and 3 GDPR contain opening clauses enabling member states to introduce legislation that provides for derogations from the data subjects rights insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purpose and such derogations are necessary for the fulfilment of those purposes.

9 Article 23, para 1 (e) GDPR.
10 The IT Political Association of Denmark's remarks on the Data Protection Act. https://itpol.dk/hoeringssvar/databeskyttelseslov (Danish)
11 The CPR register contains data on civil reg. no., name, address, birth registration, citizenship, church membership, parentage, marital status as well as information on the status of the individual registration. The CPR register was established in 1968; however, there have been civil registrations in Denmark since 1924 in municipal registers. https://www.cpr.dk/english/ (English).
12 If a person does not wish the sample to be retained in the biobank, he or she can request the Department of Congenital Disorders, Center for Neonatal Screening for deletion. https://www.ssi.dk/~/media/Indhold/DK%20-%20dansk/Diagnostik/Klinisk%20information/Blodproeve%20fra%20nyfoedte/The%20Danish%20Neonatal%20Screening%20Biobank%2007082015.ashx
13 http://www.genomedenmark.dk/english/ (English).
14 P. Blume, *Den nye persondataret, Forordning 2016/679 om personbeskyttelse* (2016) 190-192 (Danish data protection literature).
15 The Privacy Act § 10.
16 P. Blume, *Den nye persondataret, Forordning 2016/679 om personbeskyttelse* (2016) 190-192 (Danish data protection literature).

DANISH ADAPTATION OF THE GDPR by, *Tenna Overby*

On the basis of Article 9, para 2 (j) and Article 89 GDPR, the Data Protection Act provides a legal basis for processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. [17] The provision is basically a continuation of the pre-existing legal basis for such processing as set out in the Privacy Act. However, the provision in the Data Protection Act includes a legal basis for the Minister of Health, in negotiations with the Minister of Justice, to issue specific rules in compliance with Article 9, para 2 (j) and Article 89 GDPR on processing for other purposes than for scientific or statistical research purposes when a such processing is necessary to protecting vital interests of the data subject.[18]

D-Minors' consent in relation to information society services

Processing based on consent was one of the lawful bases in the pre-existing Privacy Act and is now carried over to the Data Protection Act referring to Article 6, para 1 (a-f) GDPR. Regarding the specific protection in Article 8 GDPR on children's consent in relation to information society services, the Ministry of Justice have made use of the opening clause in Article 8 GDPR and set a minimum age of 13 years for valid consent to be obtained directly from a minor. The decision on adapting the minimum age level under that of the GDPR is based on considerations to the amount of experience Danish children have with regards to using online media[19] and their participation in online activities has both an educational and social impact on children. In this regard the Ministry of Justice considered that a higher age for legal consent could pose a risk in that children would be excluded from online activities if the holder of parental responsibility over the child refuse to consent, which might result in children pretending to be older than they are. Further the Ministry of Justice considered that the GDPR provides robust protection for children regardless of consent from the holder of parental responsibility over the child.

VI-OTHER KEY PROVISIONS

A-Data Protection Officer

The obligation to designate a Data Protection Officer (DPO) is a new requirement in Danish data protection law. Pursuant to Article 38, para 5 GDPR the Data Protection Act contains a provision on the duty of confidentiality whereby the DPO may not pass on information that acquired in the role of DPO. However, this provision only applies for DPOs in the private sector as confidentiality for public employees is regulated in the Public Administration Act and the Criminal Code. Data Protection Act does not extend the scope for when private actors should designate a DPO, which was an option under the GDPR.[20]

B-Independent Supervisory Authorities

The Chapter on Supervisory Authorities in the Data Protection Act is mainly a continuation of previous law in the Privacy Act. The two supervisory authorities are the Data Protection Agency and the Court Administration.[21] Both authorities are organisationally under the purview of the Ministry of Justice, however, as independent organs. The Data Protection Authority has supervisory competence in all areas of Danish jurisdiction covered by the GDPR and within the scope of the Data Protection Act including areas subject to Danish special regulation established in accordance with the GDPR. However, the Data Protection Authority has no supervisory competence on the courts' processing of data, which are subject to the supervisory power of the Court Administration.

Decision of the supervisory authorities cannot be brought before another administrative authority. However, this does not affect the possibility of bringing a decision before the Danish Parliamentary Ombudsman or the ability to bring the decision before the national courts. [22]

C-Penalties

The GDPR regime on administrative fines is in conflict with the fundamental principle in the legal system of Denmark, whereby only the national courts can impose fines that constitute a criminal penalty. This principle is based on the threefold division of power as set out in Constitutional Act of Denmark, whereby the legislative

17 The Data Protection Act § 10.
18 The Data Protection Act § 10, para 5.
19 A survey from The National Council for Children from 2014 shows that 97 % of all 13 year old children in Denmark are active on one or more social medias. https://www.boerneraadet.dk/nyheder/nyheder-2014/97-procent-af-13-aarige-bruger-sociale-medier (Danish).
20 Article 37, para 4 GDPR.
21The Danish Business Authority is supervisory authority for data protection in regard to the ePrivacy Directive. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058 (English), and will presumably be the supervisory authority under the under the Regulation on Privacy and Electronic Communications http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 (English).
22 According to Article 78 GDPR and the Constitutional Act of Denmark § 63, the courts of justice shall be empowered to decide any question relating to the scope of the executive's authority. http://www.stm.dk/_p_10992.html (English)

DANISH ADAPTATION OF THE GDPR by, *Tenna Overby*

authority is vested in the Government and the Parliament conjointly, the executive authority is vested in the Government and the judicial authority is vested in the courts of justice.[23] As a consequence the Data Protection Agency cannot impose any administrative fines for infringements of data protection legislation. The Data Protection Agency must instead turn in a police report if it finds it necessary. However, in practice, the usual reaction to suspected infringements of the pre-existing Privacy Act was for the Data Protection Agency to pronounce commands or prohibitions for the entity in question. If such commands or prohibitions were not followed the next step for the Data Protection Agency was be to turn in a police report in preparation for the national courts to sentence a fine.

This approach is continued under the GDPR due to recital 151, which recognises that fines that constitute a criminal penalty can only be sanctioned by the national courts. Therefore, the Data Protection Agency is obliged to submit a police report in case of infringements of the GDPR and the Data Protection Act. However, as a new provision, the Data Protection Act provides that the Data Protection Agency can impose minor administrative fines extra-judicially if the case is uncomplicated, without evidentiary disputes and the processor subject to the fine accepts.[24]

One of the main topics discussed with regards to the adaption of the GDPR to the Danish legal system was whether or not public authorities should be subject to fines.[25] The Ministry of Justice had not decided on this in the first draft of the Data Protection Act that was published for public consultation. However, just before the first parliamentary reading the Ministry of Justice added a section in § 41 of the Data Protection Act that provides that public authorities can be sanctioned with fines as well as private actors. Under the first reading in Parliament, the Minister of Justice, Søren Pape Poulsen, stated that the government found it reasonable and fair to sanction public authorities as well as for private actors for infringements of the Data Protection Act and the GDPR.[26]

As Article 83, para 4-6 GDPR contains a detailed regulation on which actions and omissions constitute an infringement of the GDPR, the Data Protection Act also provides for which actions and omissions may result in a penalty. This provides a secure legal basis for the Danish Data Protection Agency as well as providing guidance for the data subjects, data controllers and the data processors. Pursuant to recital 151, national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive. A review of annual reports from year 2008-2010, compiled by the Data Protection Agency, shows that the level of fines imposed varied from 270 euro to the maximum of 3,355 euro depending on the degree of the infringement.[27] Due to the regime on administrative fines in the GDPR, a change in the existing legal precedents on the level of fines imposed after 25 May 2018 is very likely.

VII-After 25th May

The purpose of this chapter was to give an introduction to the Danish adaption of the GDPR and to give an insight to key provisions in the Data Protection Act and to comment on the most interesting use of opening clauses. The developing of opening clauses in the Data Protection Act has given public authorities a wider access to process personal data and have in some areas restricted data subjects' rights. This may be undermine the main objectives of the GDPR, however, the right to data protection is not an absolute right, but must be considered in relation to its function in society and in this connection the Danish adaption of the GDPR has balanced data subjects right against the effectiveness for public authorities to process personal data. This has resulted in some provisions that gives ministers more legislative power than previously. It shall be interesting to see to what extent the ministers will make use of this empowerment to issue specific rules on certain areas as provided for in the Data Protection Act. This might potentially restrict the data subjects' rights even further.[28]

Finally, it shall be interesting to see how the GDPR and the Data Protection Act will be interpreted and if the double regulation will be subject to any issues in regard to deciding the legal position. So far, it has not been the subject of any known conflicts.

23 Article 3 Constitutional Act of Denmark. http://www.stm.dk/_p_10992.html (English).
24 The Data Protection Act § 42, para 2.
25 Article 83, para 7 GDPR.
26 First reading of the Data Protection Act in Parliament. http://www.ft.dk/samling/20171/lovforslag/L68/BEH1-20/forhandling.htm (Danish).
27 Numbers from *the Recommendation no. 1565 on GDPR and the legal framework for Danish legislation* (24 May 2017) 919.
28 The Data Protection Act § 5, para 3 and § 10, para 5.

THE GDPR IMPLEMENTATION IN THE NETHERLANDS

By Paul Breitbarth, LL.M.
Director of Strategic Research and Regulator Outreach at Nymity Inc., and Senior Visiting Fellow at Maastricht University's European Centre on Privacy and Cybersecurity. For correspondence: info@paulbreitbarth.eu

I-INTRODUCTION

On 22 May 2018, the GDPR Implementation Act was published in the Official Journal of the Netherlands[1], thereby completing the legislative process that started on 12 December 2017. In the accompanying Royal Decree[2], the Minister for Legal Protection[3] announced that the Act would apply as of 25 May 2018, the same date the GDPR would enter into application. The Netherlands therefore completed their main legislative procedure for the GDPR just in time, unlike the implementation of Directive 95/46/EC, which was implemented three years late, or the Police and Justice Data Protection Directive (EU) 2016/680, which was adopted by the Senate 16 October 2018 and entered into application on 1 January 2019[4]. The GDPR Adaptation Bill, readjusting references to the previous Dutch Data Protection Act to the GDPR and the Implementation Act, and the accompanying Royal Decree, were published in the Official Journal on 27 July 2018[5], with their application backdated to 25 May 2018.

II-A NEW LAW, THE SAME RULES

To facilitate the transfer from the old to the new data protection regime, the Dutch Government 'decided to build on the existing norms from Directive 95/46/EC and the Dutch Data Protection Act' while implementing the GDPR. 'The smaller the differences, the easier the transfer from the existing to the new [data protection] regime' will be.[6] The way the GDPR is embedded in Dutch law is therefore considered to be policy-neutral. This approach fits the general attitude regarding the implementation of EU law. Both the House of Representatives and the Senate have in the past criticised the practice of *gold plating* EU legislation with additional national requirements, since this would impinge on the level playing field that is supposed to exist in EU Member States.

The GDPR Implementation Bill was not the first time the Members of Parliament got to discuss the GDPR. On the contrary: from the moment the GDPR was published in January 2012, both Houses of Parliament have discussed it on many occasions in order to provide input to the Government for the Dutch position during the negotiations. Both Houses of Parliament have a long-standing tradition of being involved with EU legislation early on, having realised that European legislation can only be influenced if you get involved in time. Specific procedures have been set up to deal with EU legislative proposals, allowing both the House and the Senate to mark proposals for scrutiny, requiring a more in-depth consideration. The GDPR received this status. During the negotiations, the Government therefore sent quarterly updates to Parliament, discussing the state of play in the negotiations.[7]

A-The Legislative Process

The legislative process to implement the GDPR in the Netherlands was started in parallel to the final negotiations on the text of the Regulation. The

1 Available at <https://www.officielebekendmakingen.nl/stb-2018-144.html> accessed 13 January 2019.
2 Available at <https://www.officielebekendmakingen.nl/stb-2018-145.html> accessed 13 January 2019.
3 In the current Dutch Government, the Minister for Legal Protection, Sander Dekker, is responsible for Data Protection and Privacy. He is the second Minister attached to the Ministry of Justice and Security.
4 Legislative proposal 34.889 amending the Police Data Act and the Judicial and Criminal Procedural Data Act to implement European rules on the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties - A legislative monitor is available on the website of the Senate <https://www.eerstekamer.nl/wetsvoorstel/34889_verwerking_persoonsgegevens> accessed 13 January 2019.
5 Stb 2018, 247-250.

6 Parliamentary Documentation - Kamerstukken II 2017-2018, 34851 nr 3/4.
7 A full file on Parliament's involved on the GDPR is available on the European website of the Senate (file E120003): <https://www.eerstekamer.nl/eu/edossier/e120003_voorstel_voor_een> accessed 13 January 2019.

THE GDPR IMPLEMENTATION IN THE NETHERLANDS by, *Paul Breitbarth, LL.M.*

Ministry of Justice and Security, which is responsible for data protection, started the inventory of legal provisions that would require an update in light of the GDPR. Also, the first drafts of what would become the Implementation Bill were created.

As to the material scope of the GDPR, the Dutch Government confirmed in the Explanatory Memorandum to the Implementation Bill that data processing in the light of national security and by the armed forces are considered to be out of scope. This would also include the (mandatory or voluntary) transfer of personal data to the Intelligence and Security Services. However, data processing by other public authorities in the light of national security, including for counter-terrorism purposes, would fall under the GDPR. The national implementation in the Netherlands would not cover the Common Foreign and Security Policy of the EU, nor processing for personal or household purposes. Finally, no provisions are created to provide data protection rights to the deceased, as would be allowed following Recital 27 GDPR.[8]

B-Public Consultation

Contrary to what is customary for legislation implementing directly applicable EU provisions, the draft Implementation Bill was subjected to a public consultation via the internet.[9] This consultation started on 9 December 2016 and was concluded on 20 January 2017. In total, 111 responses were received, which mainly called for further clarification of the material provisions of the Bill and the GDPR. However, according to the Government, the public consultation did not lead to major changes in the text of the draft Bill. After the public consultation, the Dutch Data Protection Authority (DPA) and the Council for the Judiciary were also consulted. Finally, the Government's official legal advisor, the Council of State, was asked for its views on the draft Implementation Bill.

In its advice[10], the Dutch DPA raised quite a number of points, mainly of a technical nature. On some issues, including the relation between the Implementation Bill, the DPA's powers and the Netherlands' administrative procedural legislation, further clarification was recommended. Most of the recommendations of the Dutch DPA were followed by the Government in the final draft of the Implementation Bill. Initially, the Government did not follow two main points of the DPA. The first concerned the independent position of the Authority, including its wish for a separate budget. The debate on this point is described in more detail below. The other point regarded the Authority's wish to enshrine in law the principle that all investigatory reports are to be made public upon conclusion. This is currently included in the publication guidelines of the Authority[11] and has been discussed with the competent Minister many times in the past. The Government until now has however refused to codify the mandatory publication, for reasons unclear. Because of the policy-neutral character of the Implementation Bill, the Government decided not to include the requested provision in the Bill. Possibly, codification could follow at a later date, once a more general discussion on government transparency and the debate on the Members Initiative Bill on Open Government[12] has been concluded.

Once the official consultation process was concluded and the desired technical and substantive changes to the draft bill were made, the Government could finally propose the bill to Parliament. The Implementation Bill was sent to the House of Representatives for its consideration on 12 December 2017.

C-The House of Representatives

In the Netherlands, a bill proposed to Parliament is first examined in the House of Representatives by one of the standing committees. In the case of the Implementation Bill, the standing Committee on Justice and Security took the lead, starting off with a round of written questions. In the so-called *Report*, all political parties represented in the House get the opportunity to ask the Government to clarify why certain choices were made in the Bill. Many parties also use this opportunity to float ideas to amend the Bill, for example to impose additional restrictions, or to provide more clarity to stakeholders.

Notably, in the Report, many parties raised the issue of the proposed age of consent for information society

8 Parliamentary Documentation - Kamerstukken II 2017-2018, 34851 nr 3/13-14.
9 Available at <https://www.internetconsultatie.nl/uitvoeringswetavg/details> accessed 13 January 2019.
10 Legislative advice on the GDPR Implementation Bill, 6 april 2017 – Available at <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_uitvoeringswet_avg.pdf> accessed 13 January 2019.
11 Guidelines on Publication by the Dutch Data Protection Authority, Stcrt 2016, 1380 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_openbaarmaking_door_de_autoriteit_persoonsgegevens_staatscourant.pdf> accessed 13 January 2019.
12 Initiative Bill by the Members Snels and Van Weyenberg on Open Government <https://www.eerstekamer.nl/wetsvoorstel/33328_initiatiefvoorstel_snels_en> accessed 13 January 2019.

THE GDPR IMPLEMENTATION IN THE NETHERLANDS by, *Paul Breitbarth, LL.M.*

services (Article 8 GDPR). Other questions concerned the rules surrounding profiling, the role, tasks and size of the supervisory authority, and the administrative burdens caused by the GDPR, especially for small and medium sized enterprises (SMEs) and small associations. It is clear that some of the questions raised and amendments proposed led to changes, because together with the written responses to the questions, the Government published a Memorandum of Amendment.[13] Apart from technical changes, the Memorandum contained an exception to the age limit for online services offering counselling or advice to minors, as well as the possibility for the Dutch DPA to issue an order under threat of a financial sanction to foster compliance.

The plenary debate on the Implementation Bill took place on 8 March 2018. A large part of the debate concerned the independent position, work and budget of the supervisory authority. The age of consent was also discussed at length. Many Members of Parliament referred to the fact that, because the GDPR is norms-based legislation, it is not as clear as many would have hoped. Especially for SMEs, but also for sports clubs and other non-profit organisations, it is a challenge to understand their legal requirements and meet them. The Minister understood these concerns but had to refer to the Dutch DPA for practical guidance. Another topic raised by multiple parties was the need to appoint a Data Protection Officer (DPO) and to maintain a processing activities register, i.e. whether this obligation would also apply to SMEs, and the need for further guidance on the 'do's and don'ts' to be issued by the DPA to organisations.

At the end of the debate, several members proposed further amendments to the Implementation Bill, of which two gained a majority. One amendment covered the need to take into account the specific character of SMEs when enforcing the law, while the other made it mandatory to appoint a college of three commissioners at the top of the Dutch DPA – the Bill had proposed appointing 'up to' three commissioners, whereas the DPA since June 2013 had two commissioners: A Chair and a Vice-Chair.

Shortly before the summer of 2018, it was announced the Government had appointed the Vice-Chair as the new Chair of the Dutch Whistleblowers Authority, leaving his seat vacant effective immediately.[14] The Minister for Legal Protection confirmed two vacancies for new Commissioners for the Dutch DPA would likely be published in fall, which indeed he did.[15, 16] Two new Commissioners were appointed by the King, upon nomination by the government following a recommendation from the Dutch DPA, just before Christmas.[17]

During the vote on the Implementation Bill, Parliament also passed two resolutions, the first one calling upon the Dutch DPA to be lenient with enforcement during the initial phase, issuing warnings rather than fines if no deliberate breaches were discovered. The second resolution called on the Dutch DPA to provide more clarity on the position of the DPO, especially in smaller organisations. The Dutch DPA will likely take note of this expression of the will of the House of Representatives, but given his independent statute, these resolutions are not binding.

D-The Senate

With the vote on 13 March 2018, the legislative process in the House of Representatives was concluded. From this moment on, the text of the Implementation Bill was also final, since in the Netherlands the Senate can only adopt or reject a Bill. It does not have the right to propose further amendments, or to send the Bill back to the House to make changes. The main role of the Senate of the Netherlands in the legislative debate is to assess the lawfulness, the enforceability and the practicality of a Bill.

Because of the Senate's involvement with the negotiations on the GDPR and the fact that the Implementation Bill was largely policy-neutral, the debate on the Implementation Bill was limited. Only four of the 12 political groups in the Senate prepared questions for the Report, and no plenary debate was deemed necessary. One of the interesting issues raised

13 Parliamentary Documents - Kamerstukken II 2017-2018, 34851, nr 8.

14 Rijksoverheid, 'Benoeming voorzitter Huis voor de Klokkenluiders' (29 June 2018) <https://www.rijksoverheid.nl/actueel/nieuws/2018/06/29/benoeming-voorzitter-huis-voor-de-klokkenluiders> accessed 13 January 2019.

15 Dion Mebius, 'Tweede Kamer is bestuurlijke rommel bij Autoriteit Persoonsgegevens zat' *de Volkskrant* (3 August 2018) <https://www.volkskrant.nl/nieuws-achtergrond/tweede-kamer-is-bestuurlijke-rommel-bij-autoriteit-persoonsgegevens-zat~b34f71f1/> accessed 13 January 2019.

16 Autoriteit Persoonsgegevens, 'De AP werft twee bestuursleden' (31 August 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/de-ap-werft-twee-bestuursleden> accessed 13 January 2019

17 'AP verwelkomt Monique Verdier en Katja Mur als nieuwe bestuursleden' (21 December 2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwelkomt-monique-verdier-en-katja-mur-als-nieuwe-bestuursleden> accessed 13 January 2019

THE GDPR IMPLEMENTATION IN THE NETHERLANDS by, *Paul Breitbarth, LL.M.*

by multiple parties that did not get as much attention in the House, is the so-called journalistic exception according to Article 85 GDPR. The Netherlands have chosen to provide a specific provision in the Implementation Bill, Article 43, which is similar to a provision that existed under the Dutch Data Protection Act. The provision states that the GDPR Implementation Act *does not apply to exclusive journalistic purposes*. At the request of the Senate, the Government confirmed this will include the preparatory work a journalist needs to do before a publication. Also, it was confirmed this is considered to be a broad exception, in order to allow the free press to do their work.[18]

Another matter raised in the Senate, is the role of the European Data Protection Board (EDPB). One of the parties criticised the amount of soft law coming from the EDPB, without any possibility for Parliament, the main legislator, to influence the decisions, even though these may have far-reaching effects. The Government confirmed this is a broad competence of the Board, which is also the result of the independence of data protection authorities. However, since all decisions, guidelines and opinions will be made public, everyone has the opportunity to access information on their obligations, and thus to understand what it is they are expected to do. Also, the consultations by the Board on draft guidelines, would allow all interested parties, including national parliaments, to present their views.[19]

III-THE NATIONAL IMPLEMENTATION OF GDPR IN THE NETHERLANDS

As mentioned before, the Government has chosen a policy-neutral introduction of the GDPR in the Netherlands. This means that many of the so-called *opening clauses* have not (yet) been used. This is also clear from the conversion table included in the Explanatory Memorandum to the Implementation Bill.[20]

Nevertheless, some of the opening clauses have been used. The following is an overview of some of the situations where the Dutch Government has decided to use an exception offered by the GDPR:

- The prohibition on processing data concerning health does not apply for processing that is relevant in social security related matters;
- The Implementation Act offers multiple examples of a substantial public interest, overriding the prohibition to process special categories of personal data;
- The processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (as referred to in Article 9(2)j GDPR) will be allowed, but is tied to specific conditions enshrined in Article 24 GDPR Implementation Act;
- The Dutch DPA has been given additional powers in line with Article 58(6) GDPR. As was the case under the old Dutch Data Protection Act, the supervisory authority will be able to issue an order under threat of a fine or administrative coercion. Also, the staff of the DPA will be able to not only enter the premises of a data controller, but also private houses if there is a legitimate reason to do so. Prior notification or a warrant from the court are not required.

The opening clauses that have been used, generally allow for the continuation of practices that already existed under the Dutch Data Protection Act. Nevertheless, there are some notable elements in the Implementation Act, mainly due to the attention that was given to the issues during the parliamentary debate.

A-The Age of Consent

One of the most debated issues during the legislative process in the Netherlands, was the age of consent for minors when using information society services. Article 8 GDPR determines 16 as the relevant age but allows Member States to lower the age to 13 years. Many Member States have done so[21], but not the Netherlands. In the Explanatory Memorandum, the Government explained it proposed to maintain the age of consent at 16 years, as was already the case under the Dutch Data Protection Act, because of the policy-neutral implementation of GDPR. This was despite the fact that during the consultation of the Implementation Bill, various parties had requested a lower age of consent, since the social views on children's capacity to consent

18 Parliamentary Documents – Kamerstukken I 2017-2018, 34851 D, 7, 15 and 25-26.
19 Parliamentary Documents – Kamerstukken I 2017-2018, 34851, D, 12-14.
20 Parliamentary Documents – Kamerstukken II 2017-2018, 34851, nr 3/ 83-89.
21As of 13 January 2019, five countries have not finalised their GDPR implementing legislation. Of the countries that have, six have included 13 years as the age of consent in their implementing laws, whereas eleven have chosen 16 years. Five countries have opted for 14 years, and one country for 15 years. (Source: Age of Consent to Processing of Personal Data – European Union Map & Chart, available in Nymity Research™).

THE GDPR IMPLEMENTATION IN THE NETHERLANDS by, *Paul Breitbarth, LL.M.*

have changed over the years. This was also the opinion of multiple political parties in Parliament.

In the Memorandum on the Report, the Government explained that in the Implementation Bill, the age of consent was set at 16 years for both the use of information society services and other situations. This is in line with the previous data protection legislation, as well as with other laws in the Netherlands, for example the application of adolescent criminal law and sexual self-determination. Furthermore, the Government reminded the Members of Parliament that the consent would only apply to the processing of personal data. For most other acts with legal consequences, such as entering into a contract, parental consent would still be required until the age of 18.

One of the main reasons some members of Parliament pushed for a lower age of consent, is the need for children to be able to get (online) advice for things they cannot discuss with their parents. This would include telephone hotlines and forum websites where children can talk with their peers, or professional counsellors, about their sexuality, bullying or other problems they encounter. With the stricter enforcement regime of the GDPR, some existing support websites had indicated they were concerned they could no longer offer their services without parental consent, where the child's relationship with the parents often was a reason for the child to come to the website in the first place. The Government appreciated this concern, and even though Recital 38 GDPR states that *the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child,* it agreed to add a specific provision in the Implementation Bill. In a Memorandum of Amendment[22], Article 5(5) was introduced, stipulating that the age of consent does not apply to support and counselling services offered directly and at no cost to a child.

This is however not the end of the discussion. The Minister for Legal Protection in the plenary debate on the Implementation Bill in the House of Representatives also stated that he is willing to review the age of consent at a later date. Because of the policy-neutral implementation of the GDPR, he considered the Implementation Bill was not the moment to change the age, but with further study into the consequences and legal effects of lowering the age threshold, he is open to continuing the debate.[23]

B-The Role and Independence of the Dutch Data Protection Authority

In his legislative advice, the Dutch DPA asked the Government to create a separate budget for the Authority, instead of including it in the general budget of the Ministry of Justice and Security, as has been the situation for many years. By creating a separate budget, the independence of the supervisory authority would be emphasised. The Government did not agree with this proposal, stating that the independence was sufficiently assured by the stipulation in Article 52 GDPR and the applicability of various provisions of the Framework Law on Independent Regulatory Bodies. In the Memorandum on the Report of the House of Representatives, the Government further elaborated on this issue. The formal independence of the Dutch DPA was reconfirmed in response to multiple questions. However, legal independence does not mean the responsible Ministry would have no say at all regarding the DPA's budget. On the contrary: the need to ensure sufficient means for the DPA as well as the requirements to ensure supervision of the spending of government funds require involvement of the ministry in the budget, it was explained.

The Memorandum on the Report was published on 13 February 2018, about one month before the plenary debate on the Implementation Bill in the House of Representatives. What happened during that month is not completely clear, but it can safely be assumed that lobbying to allow for further independence for the Dutch DPA, including a separate budget, was continued by both the Members of Parliament involved and the Dutch DPA itself. This is not part of the public record, but on the eve of the plenary debate, on 7 March 2018, the Government suddenly published a second Memorandum of Amendment.[24] Without explaining their sudden turn, the Government now proposed some further changes to the Implementation Bill to make the independent position of the Dutch DPA perfectly clear, including the attribution of legal personality and commitment to a separate budget.

The legal personality of the Dutch DPA has not been effectuated from the moment the GDPR Implementation Bill entered into application, because a number of practicalities needed to be arranged first, including the establishment of a list of employees who would no longer be employed by the Ministry of Justice and Security, but directly by the Dutch DPA. Also some other arrangement, for example the lease of the office premises and the preparations for the budget, had

22 Parliamentary Documents - Kamerstukken II 2017-2018, 34851, nr 8.
23 Parliamentary Documents – Handelingen II 2017-2018, 59, p. 18-19.
24 Parliamentary Documents - Kamerstukken II 2017-2018, 34851, nr 9.

THE GDPR IMPLEMENTATION IN THE NETHERLANDS by, *Paul Breitbarth, LL.M.*

to be taken care of. On 28 December 2018, the King approved the entry into application, as of 1 January 2019, of article 48a GDPR Implementation Act, providing the Dutch DPA with legal personality. It can therefore be expected that the 2020 Budget of the government of the Netherlands will include a separate chapter for the Dutch DPA.

Whether or not 2020 will also bring an increase of the DPA's budget remains to be seen. The size of the budget was addressed at length during the legislative debate on GDPR. To prepare for the Regulation, the Authority had commissioned a report from *Andersson Elffers Felix*[25], a public sector strategy consultancy, providing insight in various growth scenarios due to the additional tasks and responsibilities attributed by GDPR. It was predicted the number of employees of the DPA should grow from 73 full time employees (fte) late 2016 to somewhere between 185 and 270 fte, which corresponds to a budget increase from around €8 million in 2017 to €20-30 million per annum. In the 2018 Annual Budget, it was announced that the budget for the Dutch DPA would indeed grow by €7 million per annum as of 2019. However, the total amount – around €15 million – would still fall short of the lowest calculated scenario. Many Members of Parliament questioned this decision of the Government and made an argument for a further increase of the Dutch DPA's financial means. On this issue, the Government did not change its position. During the debate, the Minister for Legal Protection explained that, for now, the increased budget should suffice because hiring the right people for the right positions at the Dutch DPA is a real challenge. Also, new employees need to be trained and integrated in the daily work, and that could not be done with a 'big bang'. The Minister did however confirm that he would closely monitor the budgetary situation, in order to be able to amend the budget if a lack of funds is established.[26]

IV-NEXT STEPS

The Netherlands have concluded the main legislative process to enshrine the GDPR in their legislation just in time. For now, the legal framework is sound and the Dutch DPA has started his enforcement actions under the new law. Several investigations have been started, and some included, for example on the availability of the Records of Processing Activities Registers[27] and the appointment and registration of data protection officers in the public and healthcare sectors[28] and at banks and insurance companies[29]. An investigation into the privacy policies of local chapters of political parties and health care providers is ongoing.[30] The first enforcement notice under the GDPR was published against the Netherlands' Tax Authority, which was found to process the national identification number as part of the VAT number of self-employed persons. Not only does this increase the risk of identity theft – the Tax Authority also lacks the required explicit legal basis to process the national identification number for this purpose. A processing ban has been imposed as of 1 January 2020.[31]

During the parliamentary debate, the Minister for Legal Protection advised it is likely a second GDPR Implementation Bill will be proposed to Parliament in 2019. As yet it is unclear how extensive it would be, and when a draft will be published.

25 Autoriteit Persoonsgegevens, 'Nieuwe Europese privacywetgeving vereist groei Autoriteit Persoonsgegevens' (1 June 2017) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuwe-europese-privacywetgeving-vereist-groei-autoriteit-persoonsgegevens> accessed 13 January 2019.
26 Parliamentary Documents – Handelingen II 2017-2018, 59, p. 26.
27 'AP start onderzoek naar naleving privacyregels door private sectoren' (17 July 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-start-onderzoek-naar-naleving-privacyregels-door-private-sectoren> accessed 13 January 2019
28 'AP gestart met controles functionarissen voor gegevensbescherming' (1 June 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gestart-met-controles-functionarissen-voor-gegevensbescherming> accessed 13 January 2019
29 'AP controleert banken en verzekeraars op FG-verplichting' (20 November 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-controleert-banken-en-verzekeraars-op-fg-verplichting> accessed 13 January 2019
30 'Controle op privacybeleid bij zorginstellingen en politieke partijen' (10 December 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/controle-op-privacybeleid-bij-zorginstellingen-en-politieke-partijen> accessed 13 January 2019
31 'Belastingdienst mag BSN niet meer gebruiken in btw-identificatienummer' (21 December 2018) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/belastingdienst-mag-bsn-niet-meer-gebruiken-btw-identificatienummer> - accessed 13 January 2019

THE IRISH ADAPTATION OF THE GDPR: THE IRISH DATA PROTECTION ACT 2018

By Dr. Maria Helen Murphy,
Lecturer in Law, Maynooth University, Ireland.
For correspondence: maria.murphy@mu.ie

As the Irish Data Protection Bill was published just 114 days before the General Data Protection Regulation (GDPR) commencement date, the Bill moved through the various legislative stages of the Oireachtas (Irish legislative branch) at an accelerated pace.[1] In spite of the rapid rate of the passage of the law through the Oireachtas, multiple amendments were tabled throughout the process, including notable contributions by Senator Alice Mary Higgins.[2] In addition to implementing necessary elements of the GDPR into Irish law, the Irish Data Protection Act 2018 (DPA 2018) also transposed the Law Enforcement Directive.[3] The Data Protection Acts 1988 and 2003 had previously provided the legal framework for data protection in Ireland. The Data Protection Act 1988 was initially designed to implement the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). Further to the adoption of the Data Protection Directive 95/46/EC, Ireland amended the 1988 law and passed the Data Protection (Amendment) Act 2003. While the majority of the pre-existing data protection rules were repealed by the DPA 2018, in certain limited circumstances the older Acts will retain legal force.[4]

The DPA 2018 is comprised of eight parts and numbers 182 pages (including three schedules). Part 1 contains preliminary and general provisions including an interpretation section; Part 2 provides for the establishment of the new supervisory authority and sets out its structure and functions; Part 3 gives further effect to the GDPR in a number of areas where a margin of flexibility has been given to the member states; Part 4 provides for practical matters – such as the transfer of rights and liabilities – arising out of the replacement of the Data Protection Commissioner with the Data Protection Commission; Part 5 transposes the Law Enforcement Directive; Part 6 sets out provisions concerning the enforcement of data protection law; Part 7 is comprised of miscellaneous provisions including the application of data protection rules to the courts; Part 8 sets out the consequential amendments to existing legislation. Within its 182 pages, the Act also makes provision for the adoption of secondary legislation in a number of instances.[5] Completing the picture, the domestic law will, of course, have to be read in light of the GDPR itself. This chapter considers some of the most notable adaptations of the GDPR by the DPA 2018. Due to the prominent role Ireland plays in the supervision of compliance with the GDPR by large internet companies based in the jurisdiction, the chapter begins with a discussion of the choices

1 Indeed, an early signature motion was agreed in order to meet the deadline. Irish Constitution, art 25.2.2; Corbet R., Expert Comment, Data Protection Ireland (2018) 11(1) 2; As pointed out by Hutchinson, much of the content of the Bill was outlined in the General Scheme of Data Protection Bill 2017 which was published in May 2017. Hutchinson B., 'Editorial' Commercial Law Practitioner (2018) 25(2) 26-27.

2 O'Halloran M., 'Data Protection Bill passed after Seanad accepts 105 amendments from Dáil' (Irish Times, 22 May 2018) https://www.irishtimes.com/news/politics/oireachtas/data-protection-bill-passed-after-seanad-accepts-105-amendments-from-dáil-1.3504878

3 TJ McIntyre criticised this decision in the Oireachtas, arguing that the perceived overlap and similar language used in implementing both instruments risks confusion. Joint Committee on Justice and Equality Deb 5 July 2017 https://www.oireachtas.ie/en/debates/debate/joint_committee_on_justice_and_equality/2017-07-05/2/.

4 Section 8 states that the 1988 Data Protection Act will 'cease to apply to the processing of personal data' other than '(a) the processing of such data for the purposes of safeguarding the security of the State, the defence of the State or the international relations of the State, or (b) the processing of such data under the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 or the Vehicle Registration Data (Automated Searching and Exchange) Act 2018 to the extent that the Act of 1988 is applied in those Acts. The decision to retain the existing rules – albeit in limited circumstances – is a disappointment from the perspective of clarity. Moreover, the old laws will continue to apply to complaints made, contraventions committed, and investigations begun before the commencement of the DPA 2018.

5 Section 51 of the DPA 2018, for example, provides that secondary legislation may be made authorising the processing, where necessary for reasons of substantial public interest, of special categories of personal data, and/or Article 10 GDPR data. DPA 2018, s 51(3). Thus far, the only statutory instrument made under the Act (apart from the establishment order) has been the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 (SI No 314 of 2018)

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

made by the DPA 2018 in relation to supervision and enforcement of data protection law.

I-DATA PROTECTION ENFORCEMENT UNDER IRISH LAW

The Irish data protection supervisory authority has been the subject of much scrutiny in recent years. As the supervisory authority for many global internet companies – including Facebook and LinkedIn – the Irish Data Protection Commission (DPC)[6] has a significant role to play in the protection of personal data of individuals throughout Europe. The office has not been immune from criticism, perhaps most notably from Max Schrems who famously took the DPC to court for refusing to investigate his complaint against Facebook on the grounds that the Safe Harbor agreement was clear law.[7] In a widely reported decision, the Court of Justice of the European Union subsequently found that the Safe Harbor agreement was no longer valid.[8] Following this decision, the DPC has sought clarity from the CJEU on the status of other international data transfer mechanisms.[9] In recent years, funding for the DPC has increased markedly and a Dublin office has been established in addition to the decentralised office based in Portarlington – the location and size of which had previously been ridiculed.[10] While the DPC has been an important protector of data protection in Ireland, the independence of the body has also been challenged.[11]

The DPA 2018 established the Data Protection Commission to replace the Office of the Data Protection Commissioner.[12] While the former Data Protection Commissioner, Helen Dixon, remains as the head of the DPC, the change in the office is more than simply nominal. One structural change is that the Commission may now be led by up to three Data Protection Commissioners – although Helen Dixon remains as the sole Commissioner for now.[13] If an additional Commissioner is appointed, one of the Commissioners will be appointed as chairperson with a casting vote in the case of decisions to be taken by the Commission in the event of a tied vote.[14] Some commentators have criticised the DPC for being overly business-friendly in its approach and toothless from an enforcement perspective.[15] While the DPA 2018 continues to support the facilitation of amicable resolutions between parties, it also provides the new DPC with more robust supervision and enforcement powers, 'greatly exceeding those of the Commissioner, including the power to publish details of convictions and sanctions imposed'.[16] It is hoped that the perception of the DPC's enforcement effectiveness can be improved with the additional corrective powers granted under the DPA 2018.

II-FINES AND THE PUBLIC BODY EXEMPTION

While the increased thresholds of administrative fines has attracted significant popular attention throughout Europe, the change is particularly noteworthy in the Irish context where under the previous regime the DPC did not have the capacity to directly issue fines. While not a new power in the majority of member

6 Prior to the Data Protection Act 2018, the supervisory authority was the Data Protection Commissioner.

7 The DPC had initially declined to investigate on the grounds that the complaint was 'frivolous and vexatious'. Under Irish law, this legal term is not used in a pejorative sense. As explained in *O'N v McD*, the term means 'that the plaintiff has no reasonable chance of succeeding and that, because there is no reasonable chance of success, it is frivolous to bring the case'. [2013] IEHC 135. *Schrems v Data Protection Commissioner* [2014] IEHC 310.

8 *Schrems (Judgment)* [2015] EUECJ C-362/14.

9 *Data Protection Commissioner v Facebook Ireland Limited* [2017] IEHC 545. It should be noted that Facebook has undertaken an unprecedented appeal against the referral to the Supreme Court. Carolan M., 'Facebook's court appeal over data transfer case set for January' (Irish Times, 1 November 2018) https://www.irishtimes.com/business/technology/facebook-s-court-appeal-over-data-transfer-case-set-for-january-1.3683038

10 Mirani L., 'How a bureaucrat in a struggling country at the edge of Europe found himself safeguarding the world's data' (Quartz, 7 January 2014) https://qz.com/162791/how-a-bureaucrat-in-a-struggling-country-at-the-edge-of-europe-found-himself-safeguarding-the-worlds-data/; McAleer M., 'Data Protection Commissioner gets extra €1.2m funding' (Irish Times, 15 October 2015) https://www.irishtimes.com/business/technology/data-protection-commissioner-gets-extra-1-2m-funding-1.2393311; There have been a series of funding increases with the 2019 Budget providing for a further increase of funding of €3.5 million allowing for the recruitment of 40 additional staff. 'Funding increase of €3.5m for Data Protection Commission in Budget 2019' (Irish Examiner, 9 October 2018) https://www.irishexaminer.com/breakingnews/business/funding-increase-of-35m-for-data-protection-commission-in-budget-2019-874736.html; Weckler A., 'German jeers at Irish data privacy may help us' (Irish Independent, 31 May 2015) https://www.independent.ie/business/technology/news/german-jeers-at-irish-data-privacy-may-help-us-31266778.html

11 Edwards E., 'Independence of Data Protection Commissioner questioned' (Irish Times, 28 January 2016) https://www.irishtimes.com/business/technology/independence-of-data-protection-commissioner-questioned-1.2513682.

12 Section 14 DPA 2018 provides that all functions that before the establishment day were vested in the Data Protection Commissioner are transferred to the Commission. DPA 2018, s 14.

13 DPA 2018, s 15.

14 DPA 2018, s 16.

15 Robinson D., 'US Tech Groups Spawn a Fight between Europe's Data Regulators' (Financial Times, 28 April 2015) https://www.ft.com/content/99eea7a2-e282-11e4-aa1d-00144feab7de; Kennedy R. and M.H. Murphy, *Information and Communications Technology Law in Ireland* (Clarus 2017) 103.

16 Hutchinson B., 'Editorial' Commercial Law Practitioner (2018) 25(2) 26-27.

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

states, it is significant that the Irish Supervisory Authority now has, for the first time, the power to impose administrative fines. Under the DPA 2018, administrative fines can be appealed in the courts by the subject of the decision.[17] Where the administrative fine does not exceed €75,000, the appeal will be to the Circuit Court. Where the administrative fine exceeds that threshold, the appeal will be to the High Court.[18] The court has the power to

> (a) confirm the decision the subject of the appeal,
>
> (b) replace the decision with such other decision as the court considers just and appropriate, including a decision to impose a different fine or no fine, or
>
> (c) annul the decision.

In a much criticised early position, the Data Protection Bill exempted public bodies from administrative fines.[19] This position was defended on the grounds that Article 83 GDPR states that 'each 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'.[20] During the pre-legislative scrutiny stage of the DPA 2018, the Data Protection Commissioner, Helen Dixon, had argued that the exemption was a 'serious matter of concern' as the

> *purpose of the punitive fines provided for in the new law is to act as a deterrent to all types of organisations, and we see no basis upon which public authorities would be excluded, particularly given that arguably higher standards in the protection of fundamental rights are demanded of those entities.*[21]

In spite of this clear statement from the head of the supervisory authority, section 136(3) of the Bill as originally published stated that the DPC 'may decide to impose an administrative fine on a controller or processor that is a public authority or body only where the authority or body acts as an undertaking within the meaning of the Competition Act 2002'.[22] While the Minister for Justice, Charlie Flanagan asserted that he believed it to be 'important in the context of public and State involvement that we lead by example here and that the State, all the public bodies and agencies attached thereto, would be fully compliant'; the decision to exempt public bodies suggested a lack of confidence in existing government compliance.[23] Following much criticism and opposition in parliament, the provisions on fining public bodies were amended and a limited fining regime was provided for in the context of public bodies. Under Section 141(4) DPA 2018, where the DPC decides to impose a fine on a public authority or a public body, the amount of the administrative fine concerned shall not exceed €1,000,000.[24]

The increased enforcement power of the GDPR is not only contained in the possibility of large fines, but also under the Article 82 GDPR right to seek compensation. This is further supported by the fact that Article 80 GDPR also provides for a limited right to engage in class actions. The issue of the public body fine exemption was not the only minimalist adaptation of the GDPR to be reconsidered in the course of the Irish parliamentary process. While section 115 of the initial version of the Data Protection Bill permitted a data subject to mandate a not-for-profit 'body, organisation or association' to exercise the rights of the data subject to pursue a remedy on his or her behalf, section 123(7) of the Data Protection Bill stated that where a court action has been brought on behalf of a data subject by such a body, compensation for material or non-material damage suffered shall not be awarded.[25] Even though injunctive relief would still have been possible under the initial draft, the removal of the threat of damages where actions are taken on behalf of data subjects would clearly have hindered the enforcement power of the Irish law. It is positive, therefore, that legislative debates led to a change in the final Act. Under section 117 DPA 2018, where the action of a data subject is being brought by a not-for-profit body, the court shall have the power to grant to the relevant data subject one or more of the following reliefs:

> (a) relief by way of injunction or declaration; or
>
> (b) compensation for damage suffered by the

17 DPA 2018, s 142.
18 DPA 2018, s 142(6).
19 Data Protection Bill 2018 (as initiated), s 136(3).
20 GDPR, art 83(7).
21 Edwards E., 'Public bodies not subject to fines under new Data Protection Bill Minister for Justice says he expects State bodies to be "fully compliant" with new EU law' (Irish Times, 1 February 2018) https://www.irishtimes.com/news/crime-and-law/public-bodies-not-subject-to-fines-under-new-data-protection-bill-1.3377063
22 Data Protection Bill 2018 (as initiated), s 136.
23 Edwards E., 'Public bodies not subject to fines under new Data Protection Bill Minister for Justice says he expects State bodies to be "fully compliant" with new EU law' (Irish Times, 1 February 2018) https://www.irishtimes.com/news/crime-and-law/public-bodies-not-subject-to-fines-under-new-data-protection-bill-1.3377063
24 The limit does not apply where the public body is operating in competition with a private entity offering similar services.
25 Data Protection Bill 2018 (as initiated), s 123(7).

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

> plaintiff as a result of the infringement of the relevant enactment.

This was a welcome amendment that should enhance the ability of individuals to vindicate their data protection rights under Irish law.

III-CHILDREN AND THE IRISH DATA PROTECTION ACT

In the debates concerning the DPA 2018, there was significant political interest in providing a number of enhanced protections for the data of children. At times in the public discussion, however, the issue of data protection for children appeared to be conflated with the related but different matter of protecting children online generally. For the purposes of the application of the GDPR in Ireland, a reference to 'child' in the Regulation is taken to be a reference to a person under the age of 18 years.[26] One example of an attempt to provide additional protection for the data of children is found in section 32. This section provides for the drawing up of codes of conduct intended to contribute to the proper application of the Data Protection Regulation with regard to—

> (a) the protection of children,
>
> (b) the information to be provided by a controller to children,
>
> (c) the manner in which the consent of the holders of parental responsibility over a child is to be obtained for the purposes of Article 8,
>
> (d) integrating the necessary safeguards into processing in order to protect the rights of children in an age-appropriate manner for the purpose of Article 25, and
>
> (e) the processing of the personal data of children for the purposes of direct marketing and creating personality and user profiles.[27]

Under the DPA 2018, the DPC will have a role in considering whether a draft code of conduct or an extension or amendment to an existing code of conduct provides appropriate safeguards.[28] When assessing a code of conduct concerning children, the DPC may consult with such persons as it considers appropriate including—

> (a) children and bodies who appear to the Commission to represent the interests of children,
>
> (b) the holders of parental responsibility over children, and
>
> (c) the Ombudsman for Children.[29]

As in other jurisdictions, the age of consent in relation to information society services was the subject of much debate in Ireland. On the introduction of the Bill, the government had set the age of consent in relation to information society services at the minimum age of 13.[30] This decision was supported by the Ombudsman for Children, the Joint Oireachtas Committee on Justice and Equality, several child-focused charities, and a range of academics.[31] The age of 13 was retained as the threshold until the report stage of the Bill where the proposals of opposition parties led to the relevant digital age of consent being specified as the maximum age of 16 years.[32]

26 DPA 2018, s 29.
27 DPA 2018, s 32(1). This section is said to operate 'without prejudice' to the generality of Article 40 GDPR.
28 The issues that arose in the Oireachtas debates concerning the data protection rights of children are set to be further examined following the DPC's launch of a consultation on the subject. 'Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR' (DPC, 19 December 2018) https://www.dataprotection.ie/en/news-media/latest-news/public-consultation-processing-childrens-personal-data-and-rights-children
29 DPA 2018, s 32(2).
30 Data Protection Bill 2018 (as initiated), s 29.
31 Statement: Ombudsman for Children, Dr Niall Muldoon, expresses concern about a potential amendment to the proposed digital age of consent (1 May 2018) https://www.oco.ie/ga/news/ombudsman-for-children-dr-niall-muldoon-expresses-concern-about-a-potential-amendment-to-the-proposed-digital-age-of-consent/; Joint Committee on Justice and Equality Report on pre-legislative scrutiny of the General Scheme of the Data Protection Bill 2017 (November 2017) https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_justice_and_equality/reports/2017/2017-11-23_report-on-pre-legislative-scrutiny-of-the-general-scheme-of-the-data-protection-bill-2017_en.pdf; Fitzgerald C., 'Children's rights groups angry at Dáil vote setting digital age of consent at 16 (they wanted it to be 13)' (The Journal, 16 May 2018) https://www.thejournal.ie/digital-age-of-consent-3-4017307-May2018/; Mc Mahon C., 'Open Letter on the Digital Age of Consent' (Medium, 1 May 2018) https://medium.com/@CJAMcMahon/open-letter-on-the-digital-age-of-consent-223696b317b0. See also, many of the responses to the Government Consultation on Data protection safeguards for children ('digital age of consent') www.justice.ie/en/JELR/Pages/Consultation_on_Data_protection_safeguards_for_children_Digital_Age_of_Consent. Alternative perspectives that were prominent in the public debate included those of academics Mary Aiken and Barry O'Sullivan, Aiken M. and B. O'Sullivan, 'We need to talk about the Irish "digital age of consent"' (Irish Times, 13 July 2017) https://www.irishtimes.com/opinion/we-need-to-talk-about-the-irish-digital-age-of-consent-1.3152388
32 O'Halloran M., 'Government loses vote as Dáil backs 16 as age of digital consent' (Irish Times, 16 May 2018) https://www.irishtimes.com/news/politics/oireachtas/government-loses-vote-as-dáil-backs-16-as-age-of-digital-consent-1.3497921. Section 31(2) further specifies that the term 'information society services' does not include a

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

The influence of opposition parties in the legislative debates was enhanced by the current political situation in Ireland which sees the minority Irish government led by Fine Gael often supported by the existence of a 'confidence and supply' arrangement with Fianna Fáil. TDs (Members of the Irish lower house of parliament, Dáil Éireann) from Fianna Fáil, the Social Democrats, Labour, and Sinn Féin opposed setting the digital age of consent at 13. This revised position was successful on a vote and the government accepted the position of the lower house. Representatives from other opposition parties – including Independent Senator Lynn Ruane – continued to note their objection to the increased threshold at the final report stage in Seanad Éireann (upper house).[33] As pointed out by the Minister for Justice, Charles Flanagan, the section 31 review mechanism – initially introduced in response to worries expressed in the Seanad regarding the setting of 13 years of age as the threshold – will now review the suitability of 16 years rather than 13 years. The DPA 2018 requires this review to take place no later than three years after the section's operation and the review should be completed within one year.[34]

An ill-fated attempted at enhanced protection for the data of children would appear to be found in section 30 of DPA 2018 which was successfully introduced at the later stages of the Oireachtas debates by opposition politicians. Section 30 states that:

> It shall be an offence under this Act for any company or corporate body to process the personal data of a child as defined by section 29 for the purposes of direct marketing, profiling or micro-targeting.[35]

The DPA 2018 provides that an offence under section 30 shall be punishable by an administrative fine.[36] Explaining the decision to defer or delay the commencement of section 30, the Minister for Justice stated that the Office of the Attorney General has advised that section 30 appears to go beyond the margin of discretion afforded to member states in giving further effect to the GDPR and would conflict with Article 6(1)(f) GDPR when read in conjunction with Recital 47 GDPR.[37] As this advice indicates that the commencement of section 30 could result in a risk of infringement proceedings against Ireland, the Department of Justice is seeking clarity on the matter before considering commencement.[38] Corbet suggests that this 'leaves Ireland in the curious position of having introduced a last minute offence into section 30 of the Act which seems destined never to become law'.[39]

IV- FREEDOM OF EXPRESSION EXEMPTION

Responding to its duty to reconcile the right to data protection with the right to freedom of expression, the Irish legislature provided for a broad freedom of expression exemption in DPA 2018.[40] The freedom of expression exemption formerly in place was contained in section 22A of the Data Protection Acts 1988 to 2003. This was a structured exemption that applied to personal data processed 'only for' journalistic, artistic or literary purposes and 'undertaken solely with a view to the publication of any journalistic, literary or artistic material'. The now repealed Section 22A exemption also required the data controller to reasonably believe that the processing was 'in the public interest' and that 'compliance with that provision would be incompatible with journalistic, artistic or literary purposes'.[41] The DPA 2018 exemption is of broader application, designed to apply to the processing of personal data that is 'for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression'.[42] Section 43 DPA 2018 states that such processing shall be exempt from compliance with aspects of the Data Protection Regulation – including

reference to preventative or counselling services in the Irish context.

33 Minister for Justice Charles Flanagan stated that he acknowledged 'the will and wish of Dáil Éireann as far as this issue is concerned' and that while he did not 'agree' with the majority view of the House, he had no 'intention to revisit the debate' in the Seanad. Seanad Deb 22 May 2018, Data Protection Bill 2018: [Seanad Bill amended by the Dáil] Report and Final Stages https://www.oireachtas.ie/en/debates/debate/seanad/2018-05-22/11/?highlight%5B0%5D=data&highlight%5B1%5D=bill&highlight%5B2%5D=2018&highlight%5B3%5D=bill

34 DPA 2018, s 31(3). Seanad Deb 22 May 2018, Data Protection Bill 2018: [Seanad Bill amended by the Dáil] Report and Final Stages https://www.oireachtas.ie/en/debates/debate/seanad/2018-05-22/11/?highlight%5B0%5D=data&highlight%5B1%5D=bill&highlight%5B2%5D=2018&highlight%5B3%5D=bill

35 DPA 2018, s 30.

36 See DPA 2018, s 141.

37 Some, including Senator Alice Mary Higgins, contested this interpretation. Seanad Deb 22 May 2018, Data Protection Bill 2018: [Seanad Bill amended by the Dáil] Report and Final Stages https://www.oireachtas.ie/en/debates/debate/seanad/2018-05-22/11/?highlight%5B0%5D=data&highlight%5B1%5D=bill&highlight%5B2%5D=2018&highlight%5B3%5D=bill

38 Dáil Deb 12 June 2018, Written answers (Question to Justice) 524 https://www.oireachtas.ie/en/debates/question/2018-06-12/524/#pq-answers-524

39 Corbet R., Expert Comment, Data Protection Ireland (2018) 11(3) 2.

40 See GDPR, art 85.

41 Data Protection Acts 1988 to 2003, s 22A.

42 DPA 2018, s 43(1).

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

from certain aspects of Chapter II and Chapter III GDPR.[43] In order to be eligible for this exemption, compliance with the relevant data protection provision would have to be deemed to be incompatible with freedom of expression. In conducting this unstructured compatibility test, the DPA 2018 requires regard to be had to 'the importance of the right of freedom of expression and information in a democratic society'.[44] The section further states that in order 'to take account of the importance of the right to freedom of expression and information in a democratic society that right shall be interpreted in a broad manner'.[45] Clearly, section 43 of the DPA 2018 contains a challenging test to apply in practice and provides little guidance to those wishing to avail of the exemption. Cases – before the DPC and the courts – are likely to play a significant role in the formulation of more detailed guidelines on the operation of the exemption in Irish law. Notably, the DPA 2018 explicitly provides for the DPC to be able to refer to the High Court 'any question of law which involves consideration of whether processing of personal data is exempt' on freedom of expression grounds.[46]

V-POLITICS AND DATA PROTECTION

Another area of significant public discussion in Ireland was the special provision for data processing carried out in the context of electoral activities. It is unsurprising that legislators often seek to make provision for their own practices when legislating. For example, section 39 of the DPA 2018 provides that:

> A specified person may, in the course of that person's electoral activities in the State, use the personal data of a data subject for the purpose of communicating in writing (including by way of newsletter or circular) with the data subject.[47]

Moreover, the section goes on to state that: 'Communicating in accordance with subsection (1) shall, for the purposes of Article 6(1)(e), be considered to be the performance of a task carried out in the public interest'.[48] Accordingly, the DPA 2018 provides an extremely broad 'public interest' ground for such communications that negates consideration of other lawful grounds such as consent. Additional electoral activity carve outs are contained in sections 40, 58, and 59. Corbet suggests that the decision of the body politic to exempt itself from certain data protection requirements occurs in spite of '(or perhaps because of) a number of previous cases investigated by the DPC relating to political canvassing'.[49]

The topic of the Cambridge Analytica scandal arose frequently in the course of the DPA 2018 debates, unsurprisingly considering the timing of the stepping forward of the whistleblower, Christopher Wylie, just shortly after the initiation of the Data Protection Bill in the Oireachtas.[50] In the wake of the Cambridge Analytica scandal, section 43 of the sixth of March version of the Bill (as amended in Seanad Committee) drew widespread criticism. At that time, the Bill stated that

> the processing of personal data revealing political opinions shall be lawful where the processing is carried out in the course of election activities for the purpose of compiling data on peoples' political opinions by—
>
> (a) a political party,
>
> (b) a body established by or under an enactment (...), or
>
> (c) a candidate for election to, or a holder of, elective political office.[51]

This very broad assertion of lawfulness regarding the processing personal data in the course of 'electoral

43 Article 43(2) DPA 2018 states that the 'provisions of the Data Protection Regulation specified for the purposes of subsection (1) are Chapter II (principles), other than Article 5(1)(f), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries and international organisations), Chapter VI (independent supervisory authorities) and Chapter VII (cooperation and consistency)'.

44 DPA 2018, s 43(1).

45 DPA 2018, s 43(5).

46 A right to appeal a determination from the High Court to the Court of Appeal is explicitly affirmed in DPA 2018, s 43(4).

47 DPA 2018, s 39(1). A 'specified person' is defined to mean: a political party, a member of either House of the Oireachtas, the European Parliament or a local authority, or a candidate for election to the office of President of Ireland or for membership of either House of the Oireachtas, the European Parliament or a local authority. DPA 2018, s 39(3).

48 DPA 2018, s 39(2).

49 Corbet R., Expert Comment, Data Protection Ireland (2018) 11(3) 2.

50 Cadwalladr C. and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (The Guardian, 17 March 2018) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Reporting on the Cambridge Analytica scandal had of course occurred prior to Wylie's stepping forward, Cadwalladr C., 'The great British Brexit robbery: how our democracy was hijacked' (The Guardian, 7 May 2017) https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. Minister for Justice Charles Flanagan introduced the Bill for the Second Stage reading on 17 April 2018.

51 Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects. Data Protection Bill 2018 (As amended in Committee [Seanad Éireann]), s 43.

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

activities' sparked criticism – particularly in light of the fact that personal data 'revealing political opinions' constitutes special category data under Article 9 GDPR. In defending the Bill, the Department of Justice argued that the provision should be read in light of section 33 which set out 'suitable and specific measures for processing'.[52]

While the final version of the provision on personal data and electoral activities closely resembles the criticised text, section 48 DPA 2018 does contain some amendments:

> Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of personal data revealing political opinions shall be lawful where the processing is carried out—
>
> **(a)** in the course of electoral activities in the State for the purpose of compiling data on peoples' political opinions by—
>
> (i) a political party, or
>
> (ii) a candidate for election to, or a holder of, elective political office in the State,
>
> and
>
> (b) by the Referendum Commission in the performance of its functions.[53]

A key point of contention regarding the original exemption was the absence of a definition of the term 'electoral activities'. In an article by Elaine Edwards, Daragh O'Brien[54] is quoted as saying that the failure to define the term supported the creation of a 'free-for-all for organisations like Cambridge Analytica to set up shop here and influence voters and elections anywhere in the world with impunity and no possibility of sanction'.[55] While the enacted version of the legislation states that the term 'electoral activities' 'includes the dissemination of information, including information as to a person's activities and policies, that might reasonably be of interest to electors', a clear and limited definition of the term would have been desirable in order to better ensure the appropriate and purpose-bound use of such information.[56] A notable change in the final text of the DPA 2018 is the limitation requiring that such processing be carried out in the course of electoral activities 'in the State'. This should act as some bulwark against the threat of Ireland becoming a 'global capital of election manipulation' as warned against by O'Brien.[57] Notwithstanding this improvement, stronger protection of personal data in the context of electoral processing would have put Irish democracy in better stead to withstand the threat of electoral manipulation. Moreover, questions remain as to whether the broad scope of processing activities liable to be caught by the electoral exemption can be considered to be necessary and proportionate for reasons of a substantial public interest.[58]

VI-CONCLUSION

In the final report of the Data Protection Commissioner, Helen Dixon looks forward to a 'new era of the DPC with increased powers and a new legal framework'.[59] The report notes that a consultation regarding the regulatory strategy for the DPC under the GDPR will be launched in order to 'provide a sustainable and transparent underpinning for what are inevitable resource deployment options and choices'.[60] In light of increased awareness and stricter GDPR notification requirements, it is unsurprising that there has been a significant increase in the reporting of data breaches to the DPC since the passage of the DPA 2018.[61] The regulation of large internet companies is likely to remain a key area of focus for Irish data protection

52 Edwards, E. 'Data Bill would "create free-for-all" for harvesting data on political views' (Irish Times, 20 March 2018) https://www.irishtimes.com/news/ireland/irish-news/data-bill-would-create-free-for-all-for-harvesting-data-on-political-views-1.3432975
53 DPA 2018, s 48.
54 O'Brien is a data ethics expert and the CEO of Castlebridge, a data privacy and governance consultancy https://www.castlebridge.ie/what-we-do/
55 Edwards, E. 'Data Bill would "create free-for-all" for harvesting data on political views' (Irish Times, 20 March 2018) https://www.irishtimes.com/news/ireland/irish-news/data-bill-would-create-free-for-all-for-harvesting-data-on-political-views-1.3432975
56 DPA 2018, s 39(4).
57 Edwards, E. 'Data Bill would "create free-for-all" for harvesting data on political views' (Irish Times, 20 March 2018) https://www.irishtimes.com/news/ireland/irish-news/data-bill-would-create-free-for-all-for-harvesting-data-on-political-views-1.3432975
58 GDPR, art 9(g).
59 Among several guidance documents released concerning the application of the GDPR, the DPC has released preliminary guidance addressing the consequences of a 'no deal' UK exit from the EU for any Irish entities that transfer personal data to the UK. 'DPC issues important message on personal data transfers to and from the UK in event of a "no deal" Brexit' (DPC, 21 December 2018) https://www.dataprotection.ie/en/news-media/latest-news/dpc-issues-important-message-personal-data-transfers-and-uk-event-no-deal
60 Data Protection Commissioner, 'Final Report 1 January - 24 May 2018: Presented to each of the Houses of the Oireachtas, pursuant to Section 66(4) of the Data Protection Act 2018' (December 2018) 6 https://www.dataprotection.ie/sites/default/files/uploads/2018-11/DPC%20annual%20Report%202018_0.pdf
61 Edwards E., 'DPC receives over 1,100 reports of data breaches since start of GDPR rules' (Irish Times, 30 July 2018) https://www.irishtimes.com/business/technology/dpc-receives-over-1-100-reports-of-data-breaches-since-start-of-gdpr-rules-1.3580240

THE IRISH ADAPTATION OF THE GDPR by, *Dr. Maria Helen Murphy*

law. By way of example, since 25 May 2018, the DPC has opened statutory inquiries into the compliance of both Twitter and Facebook with the GDPR following receipt of a number of breach notifications.[62]

The DPA 2018 was enacted following a vibrant legislative debate that demonstrated the power of opposition parties in times of minority government. In spite of the efforts of several legislators, the debate was unfortunately truncated due to the immense time constraints surrounding the passage of the legislation. The limited review and discussion possible was particularly problematic due to the complex nature of the legislation. Not only did the Irish government choose to both adapt the GDPR and implement the Law Enforcement Directive in one Bill, but other aspects of the Data Protection Bill – including a reliance on cross-referencing – further hindered cogent debate in an already technical and challenging area of law. The 2018 DPA also makes substantial provision for the use of secondary legislation which means that the governing law will continue to evolve as regulations are promulgated. There is scope for abuse of some of these powers, including under the broadly drafted section 38 which allows regulations to be made allowing for the 'processing of personal data which is necessary for the performance of a task carried out in the public interest by a controller or which is necessary in the exercise of official authority vested in a controller'. While some protective measures were introduced to oversee the production of secondary legislation, doubts as to the effectiveness of the constraints remain.[63] It is clear that a full picture of the new data protection landscape in Ireland will take time to develop and a vigilant watch for secondary legislation and DPC action will be necessary in the interim.

62 'Data Protection Commission announces statutory inquiry into Twitter' (DPC, 19 December 2018) https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-statutory-inquiry-twitter; 'Data Protection Commission announces statutory inquiry into Facebook' (DPC, 17 December 2018) https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-statutory-inquiry-facebook

63 In addition to provision made in section 38 requiring consultation with the DPC and others (s 38(4)-(7)), other constraints include the requirement of DPC consultation in other areas (such as creating regulations limiting access rights) and straitened Oireachtas approval requirements applicable to regulations made under sections 51, 60 or 73. DPA 2018, s 60(10); DPA 2018, s 6(5).

THE ADAPTATION OF THE GDPR IN SPAIN: THE NEW DATA PROTECTION ACT (LOPDGDD)

By Dr. Cristina Pauner
Associate Professor in Constitutional law at the Universitat Jaume I and member of the PRODADEF Research Group (Data Protection and Fundamental Rights). For correspondence: pauner@uji.es

By Jorge Viguri
PhD researcher in Constitutional Law at the Universitat Jaume I of Castellón (UJI). For correspondence jviguri@uji.es

I-INTRODUCTION

Spain is a country where the culture in data protection matters is strongly rooted thanks to its norms published from 1992[1]. The Organic Law 5/1992, of 29th October, of the Automated Treatment of Data (LORTAD), the Organic Law 15/1999, of 13 December, of Data Protection (LOPD), the Royal Decree 994/1999, of 11 June, that approved the Regulation on Security Measures for automated files that contain personal data (RSM) and the Regulation of Development, Royal Decree 1720/2007, of 21 December, which approved the Regulation implementing the LOPD (RLOPD).

This entire legislative compendium constitutes a consolidated framework that develops article 18 (4) of the Spanish Constitution of 1978 (CE) which states that "*the law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights*". Those norms have strengthened the foundations for a legal and institutional framework effectively and efficiently for the protection of personal data in Spain.

The new GDPR represents a legal review of the European data protection model and is posing a significant challenge to Spain, which commenced in February 2018 the first discussion of the Draft before the Parliament, four months before the application of the new GDPR[2]. Currently, the Spanish Organic Law 3/2018 for the Protection of Personal Data and for the granting of digital rights (hereinafter, LOPDGDD) was adopted on December 5. This new Act repeals not only the former LOPD 15/1999 but also a Royal Decree-Law, which was adopted given the urgency of adapting the national legal system to certain issues foreseen in the GDPR. In this regard, the Ministry of Justice validated this Royal Decree in order to avoid a legislative void until the new LOPDGDD was approved.[3]

The approval of this new Spanish Law was an important and significant step for two reasons: firstly, the increasing of the principle of legal certainty (on a positive way), which obliges Member States to integrate the European framework into their national legislation in a clearly and publicly way to allow legal practitioners and citizens their full knowledge. On a negative side, it implies the obligation on Member

1 VVAA, *20 años de Protección de Datos en España,* AEPD, 2015.

2 Other European countries have already adapted their national legislations to the new European legal framework. For example, the German government passed an implementation *Act to Adapt Data Protection Law to regulation (EU) 2016/679 and to implement Directive (EU) 2016/680* dated 30 June 2017; in Austria, the Data Protection Amendment Act 2018 was published on 31 July 2017; Belgium passed its GDPR implementing legislation on 3 December 2017 *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*; on 29 November 2017, the Slovak Parliament adopted a Bill which repealed the incumbent Act on Data Protection, n. 122/2013 and implements the GDPR effective 25 May 2018. Italy approved the Law n.167/2017 to reform the *Codice in materia di protezione dei dati personali*, that was approved in 2003. Adjoining the Code, the Garante per la protezione dei dati personali has published a Guide (*Guida all applicazione del Regolamento UE 2016/679*) where explains in detail the values changes that the new GDPR will demand for citizens and organisations.

3 The Royal Decree-Law 5/2018, of July 27th was approved more than 6 months after the moment the GDPR started to be applicable and aimed at regulating its inspection and penalty regime. It already reflected the main specificities of this Act compared to the GDPR for example, the age underage individuals need to have to grant consent for the processing of their data, the possibility to provide information by means of a layered system, the concrete conditions in which a data protection officer needs to be appointed, etc.). Besides, among the measures included in the Royal Decree-Law, it can be highlighted the following: 1. The infringing subjects are listed and the infractions foreseen in the former LOPD are replaced by those of the RGDP; 2. Rules for the prescription terms and applicable sanctions are specified, and all according to the GDPR; 3. Particular characteristics of procedures such as: the automatic suspension for a period of time or preliminary research proceedings; 4. It distinguishes between three different proceedings depending on the treatment at stake: national treatment, cross-border treatment and cross-border treatment with local relevance in a Member State. 5. The Spanish representation in the European Data Protection Board.

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

States to eliminate uncertainty resulting from the existence of rules of domestic law incompatible with the European model (in this case, there is an obligation to "depurate" the legal system.[4] Secondly, regulations, despite its direct applicability in domestic law, may require additional national rules for full effective implementation. Consequently, it should be possible to speak of "development" rather than incorporation.

Until the adoption of this act, the Spanish Data Protection Agency (AEPD) made and continues to make a fundamental effort to facilitate the adequately implementation of the measures required by the GDPR. Among many other initiatives[5], it has brought forward a new *Guide* by creating an efficient and innovative tool to help organisations to comply with the requirements stipulated by the GDPR[6]. They are available to citizens and public and private organisations and was developed for a wide range of different purposes: to help data controllers to carry out their work, comply with the duty to inform, prepare the contract between a controller and a processor, perform risk analysis and Privacy Impact Assessment (PIAs) and to implement relevant techniques to facilitate public authorities switching to the GDPR.

II-LEGISLATIVE PROCESS. KEY DATES

On 10 November 2017, the former Spanish Government, led by Mariano Rajoy, in the meeting of the Council of Ministers, approved the preliminary draft law amending the LOPD (APLOPD) [7] at the behest of the Ministry of Justice. The APLOPD was followed by the mandatory impact reports[8] and the consequent opinion of the Council of State[9]. On 24 November 2017, the new draft LOPD was presented for the corresponding parliamentary procedure[10].

After three months of inactivity and the successive postponements, on 15 February, during the first session of debate in the Chamber of Deputies, different positions of the political groups were presented and the proposal for rejection tabled by the Mixed Parliamentary Group (PDeCAT) was discussed. It focused on the competence issue, that is, the lack of legal guarantees and competences performed by the supervisory authorities of the Autonomous Communities. This issue and the delay of the government to submit the draft before the chambers were conveyed in the whole discussion. The overall amendment was passed[11] moving to the reading in the Committee of Justice where the partial amendments to the enacting terms were discussed.

A total of 362 amendments were presented in the Congress of Deputies[12] and 32 in the Senate, which were intended to make substantial improvements to certain relevant points in the final text of the Spanish Act. During the months of November 2017 to March 2018, the Committee of Justice received a large number of parliamentary hearings related to the field of data protection, not only assessing the draft LOPD but also providing substantive input that have been reflected in the partial amendments, as it is explained in this paper. During the following eight months, the parliamentary procedure approved the Act without undue delays thanks to the broad parliamentary support, which was more than 93% between deputies and senators. The new LOPDGDD was published in the Official State Gazette on 6 December and entered into force on 7 December 2018.

4 In the words of the Court of Justice, the principle of legal certainty obligues Member States to withdraw domestic legislation if it is incompatible with European Union Law "through mandatory internal provisions that have the same legal value as the internal provisions that shall be modified" (see Preamble III of the new LOPDGDD, par. 10).

5 The AEPD has placed the following link containing a complete section concerning the implementation of the GDPR in Spain (http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php).

6 https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_06-iden-idphp.php

7 Ministry of Justice, Preliminary Draft amending the LOPD [in Spanish, Anteproyecto de Ley Orgánica De Protección de Datos de Carácter Personal (ALOPD)]. The information is available at: http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%A2%7F%8B%99tt%84sm%A3%91

8 Ministry of Justice, "Memorandum on the Regulatory Impact Analysis" de concerning the preliminary draft law amending the LOPD (APLOPD), Executive Summary. Information available at: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428491985?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DMAIN.PDF

9 Council of State, num. 757/2017, 30 October, 2017. http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/3.pdf

10 BOCG. Congreso de los Diputados, serie A, num. 13-1, 24 November 2017. http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-12-A-13-1.CODI.%29#(P%C3%A1gina1)

11 Overall, amendments can be described as the opposition to the whole text, which enables the submission of a new one. In contrast, partial amendments propose modifications to the specific articles. In this specific scenario, the results of the voting were 318 votes against and 16 votes in favour (Diario de Sesiones. Congreso de los Diputados, num. 104, 15 February 2018. Pleno, Debate de totalidad, num. 104. http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28DSCD-12-PL-104.CODI.%29#(P%C3%A1gina28).

12 Congreso de los Diputados, Boletín Oficial de las Cortes Generales (BOCG), serie A, num. 13-2, 18 April, 2018 http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

III-NOTEWORTHY ASPECTS

The LOPDGDD is adapted to the new GDPR but it does not reproduce its content requiring a common reading of both legal texts. In fact, it starts with an explanatory statement and consists of 97 articles structured in 9 titles, 22 additional provisions, 6 transitory provisions, 1 derogatory provision and 16 final provisions. In addition, it introduces important changes to the following key questions:

1. A change of the compliance model of data protection provisions: from the traditional model of verification of compliance towards a new dynamic perspective based on active **security measures.**

Data protection flows will be monitored instead of the structure of the filing systems in order to establish protection measures. Among others, a "register of processing operations/activities" is established in article 31 LOPDGDD. A revision of data processing is included before commencing the authorized activities carried out in the process.

The register of processing activities is performed in two phases. The first stage consists of a revision of the data treatment carried out by the organisation. The second stage revises the new obligations provided in the GDPR, specifically those imposed for the responsible for processing personal data, which shall be included in the registration activities.

2. The data´s consent and the **consent needed to process personal data** are strengthened (article 6 LOPDGDD). According to the GDPR, the new LOPDGDD aims to ensure that the user´s consent for the data processing is supported by an express declaration of agreement or by a strong affirmative action. This new provision excludes the "*implied consent*" arising from those actions, which are not explicitly voiced nor necessarily understood. Additionally, the consent of the data subject shall be given unequivocally, specifically for each purpose in the processing of data. Generic or diffuse consent for multiple purposes will be prohibited in the LOPDGDD.

3. The processing of **data pertaining to the deceased** constitutes another of the significant novelties in the new LOPD (article 3). The LOPDGDD regulates the processing of deceased persons' data in a particular and separate way by excluding from its scope the application the data pertaining to the deceased. However, it allows the direct heirs to access data pertaining to the deceased, including the rights of correction and deletion. This shall be subjected to the instructions given to them by the deceased and incorporated in a special register.

4. The new LOPDGDD adapts the **principle of transparency** that the GDPR foresees in article 11. It regulates the data subjects' right to be appropriately informed about any processing of personal data relating to themselves. Information double layer mechanism is also included to comply with the duty of information for data subjects, which aim at providing detailed information to the person concerned, allowing a direct and immediate access to information.

The principle of "exclusion of the eligibility of the controllers" is also included in the LOPDGDD. It establishes the adoption of all reasonable measures to guarantee the rectification or removal of relevant data. The rights of access, rectification, cancellation or objection (known as ARCO rights) adding the concept of "data blocking" in the **catalogue of data protection rights** for the deletion of data, the limitation principle of the processing of personal data or data portability, which is also set out in articles 13-18[13].

5. The existence of black lists shall be prohibited for the **"special categories of data"**. Consequently, the LOPDGDD limits the consent granted regarding these sensitive data, in such a way that it will be insufficient to process certain types of personal data. This involves data concerning ideology, union membership, religion, beliefs, racial origin, health or sex life (article 9).

To avoid discriminatory situations, the subject's mere consent will not be enough to avoid the general prohibition on processing sensitive data. Nevertheless it will be permissible to process sensitive personal data for certain purposes. For example, the compliance with legal obligations, the protection of the vital interests of the data subject, the processing carried out as part of the activities of an establishment pertaining to the data controller with due guarantees by a foundation, a non-profit association or in any other circumstances contemplated in paragraph 2 article 9 GDPR.

6. The regulation of the credit information systems, known as **"credit blacklists"** is another provision referred to in article 20. This specific legal system is complemented by the 6th Additional Provision. It sets a minimum financial limit for the inclusion

13 Rallo Lombarte, Artemi, *The right to be forgotten on the Internet: Google v. Spain*, EPIC, Washington, 2018 y Simón Castellano, Pere, *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012.

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

of this personal data to specific type of files (50€), which strengthens the level of security and avoids the stigmatisation of debtors.

7. Strengthening the **exclusion files regarding advertisement**, the so-called "*Robinson lists*"[14] (article 23). These are files or folders created with the objective to assist individuals in presenting their complaints against "spam" (unsolicited marketing communications to an individual via telephone, fax, email, text message, etc.). The new LOPDGDD foresees that the processing of the personal data will be lawful in relation to the purposes for which they are collected in order to avoid the despatch of commercial communications to data subjects who have stated their refusal or objection to receiving advertising.

8. Efficient authorisation mechanisms that guarantee the rights of data subjects and the implementation of **extra-judicial settlement-of-conflicts policy** in order to resolve promptly disputes between citizens and the DPO regulated in 37 or the implementation of alternative dispute resolution systems through codes of conduct (article 38).

IV-DIGITAL RIGHTS CHARTER

One of the most relevant amendments to the LOPDGDD was presented by the Socialist Parliamentarian Group[15]. It aimed at transforming the Law into a Digital Rights Charter. To that end, Artemi Rallo, former Director of the AEPD and current member of the Spanish parliament, proposed the addition of a new Title X "Digital Rights Guarantees", which comprises of 18 articles (79 to 97). They not only reinforce the digital rights of citizens but also extend the application of the rights and liberties enshrined in the Spanish Constitution and by International treaties to the Internet.

The Title very much takes into account the characteristics of similar regulations approved in countries from the European area (specific legislation, sectoral rules, declaratory nature of some charters recognising these rights). Examples include the French Law No. 2016-1321 of October 7, 2016, for a Digital Republic[16], the "Right to Disconnect" recognised in the French Labour Code[17] or the Declaration of Internet Rights in Italy.[18]

The explanatory memorandum accompanying the proposal stated that the legislation should recognise a Digital Rights Guarantees System in a comprehensive and unified manner due to the absence of a constitutional reform that guarantees a new generation of digital rights.[19] This new Title was incorporated to address "the recognition of a digital rights guarantee system that, unequivocally is imposed by the fourth paragraph of Article 18 of the Spanish Constitution which, in in some cases, have already been shaped by the ordinary, constitutional and European jurisprudence". In fact, it has been conceived as a prior step to a "desirable future constitutional reform" by updating this text to the digital era and specifically, "giving constitutional status to the new generation of digital rights".

This Title sets forth the need to implement the following measures:

- The **right to neutral access to the Internet (article 80)**. Service providers shall offer, as much as possible, transparent services in order to avoid technical or economic discrimination.
- The **right to Internet access (article 81)**, which shall be universally, accessible, affordable and non-discriminatory.
- The **right to digital security (article 82)**. This right, which deals with holding technology companies accountable for digital security, has become public policy priority in an increasingly digital and data-dependent economy and society. It implies a guarantee of privacy and security of communications over the Internet

14 The "Robinson List of Advertising Exclusion" is a voluntary and free service which is available to all consumers. It aims at reducing personalised publicity. More information can be found at: https://www.listarobinson.es/

15 On May 30 2018, the Spanish parliament unexpectedly approved a constitutional motion of censure against the government of Rajoy in accordance with articles 113 and 114.2 of the Spanish Constitution and in articles 175 to 179 of the Rules of the Congress. Pedro Sánchez, Secretary general of the Socialist Group, was elected the president of the Spanish Government after winning the motion of censure.

16 *Loi n° 2016-1321, du 7 octobre 2016, pour une République numérique* (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&dateTexte=&categorieLien=id).

17 It is applicable with effects from the 1st January 2017. Article 55.I.2 de la *Loi 2016-1088, du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels*, introduces a new paragraph 7 (See in the Chapter II "The adaptation of labour law to the digital age".

18 http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf

19 Brazil has a similar proposal. The Internet Civil Framework introduces a procedure in order to encourage the respect of the civil rights in Internet through the mainstreaming of the network's neutrality, limitation of liability for intermediaries and Internet users' freedom of speech, privacy and security. Act num. 12.965, 23 April 2014. Further information available at: http://participacao.mj.gov.br/marcocivil/sistematizacao/

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

by providing information to users and the establishment of swift and uncomplicated complaint procedures.

- The **right to online education (article 83)** for students on safer use of new media through teacher training programmes and a learning respectful with the constitutional values, fundamental rights and personal and family privacy and the protection of personal data from digital media.

- The **protection of minors on the Internet (articles 84 and 92)** that prompts a whole series of measures that aim to ensure children's rights. It also acknowledges the huge impact of the Internet on children's rights in order to promote necessary guarantees to protect their safety and physical integrity.

- The **right of rectification in Internet (article 85)** that guarantees freedom of expression and information on the Internet and compels social networking site providersor other equivalent services to adopt appropriate protocols to allow this right to be exercised. Once the rectification is requested, the digital media company shall promptly publish a "warning" stating that the original new does not reflect the current situation of the person involved.

- The **right to update information in digital media (article 86)** recognizes each person's right to request digital media, giving reasons, the inclusion of notification to the news concerned to a person "when the information in the original news does not reflect his/her current situation as a result of circumstances that would have taken place after the publication, causing him/her a damage". In particular, when the original information refers to police or judicial actions that have been affected to the benefit of the interested party by a subsequent judicial decision

- The **right to privacy and the use of new digital devices in the labour field (article 87)** that protects civil servants, workers and employees against intrusion of their privacy.

- The **right to disconnect (article 88)**. It allows employees in companies of more than 50 people to ignore emails after work hours to guarantee personal and family privacy. For that purpose, the company shall publish an internal charter or similar internal rules, after seeking the opinion of the employees' representative bodies. In this case, the employer will be the only decision maker. Employers should not ignore the issues that can arise from excessive use of digital devices. Where possible, they should implement measures to promote the rational use of digital devices, so that employees adopt a healthy lifestyle, and to promote work/life balance.

- The **right to privacy in the use of audio-visual or geo-location systems in the working area (article 90)**. This right regulates the processing of personal data obtained by employers for labour control purposes through video-surveillance and geolocation systems. Prior information shall be given by the companies to the employees concerned including their rights to access, rectification and erasure of their personal data.

- The **digital rights of collective negotiation (article 91)** that foresee the possibility of establish additional protection of their rights and freedoms in regard to the processing of personal data of workers.

- The **right to be forgotten in internet search (article 93)**, which postulates that personal data shall be erased when it is inadequate, irrelevant and excessive in relation to the purposes for which it was collected. In these circumstances, a search engine operator would be obliged to delete the links to related pages.

- The **right to be forgotten in social network or equivalent services (article 94)** which recognises the right of deletion of personal data posted on social network by a written request from the party concerned. Also, personal data, that has been made available by minors, should be deleted at the request of the party concerned.

- The **right to data portability (article 95)**, which allows users to store, transmit, receive and transmit personal data they provide on social networking websites and other information society services.

- The **right to digital testament (article 96)**. It will allow the deceased's relatives or legal

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

successors to access to the personal data and to provide instructions for their use, destination or deletion.

- **Policies encouraging digital rights (article 97)** which sets out how the Government in cooperation with the Autonomous Communities, will establish the following two documents: a valid data plan (Internet access) to overcome digital gaps and a action plan to promote training awareness-raising and promotional actions of the responsible use of Internet networks, mobile devices and other digital platforms like social networks for minors.

V-CRITICAL ASPECTS.

The content of the LOPDDGG has been widely discussed. While this new text can be considered highly positive, it has been at the centre of discussions by a wide range of stakeholders.

They are summarised in the following seven action points:

1. The Spanish Government has been criticised for failing to reach agreement on better **protection of minors**.[20] The minimum age for giving valid consent has been set at 14 years (article 7) in contrast to Germany or France where their national legislation has set the age of consent at 16 and 15 years respectively. However, it follows the same tendency adopted in other EU countries, for example, in Ireland, children may legally sign up for services that process personal information at the age of 13. Minors are considered digital natives who share a common global culture defined less by age than by their ordinary activities growing up immersed in different technological platforms. In this regard, the age of 14 for children's consent in relation to information society services corresponds to the Spanish reality of internet use by Spanish children.

Although the Spanish Government has shown restraint in its response so far, it has claimed that the minimum age is a realistic in accordance with other national laws. The principle of the best interests of the child should require Spanish legislation to raise the minimum age and apply strict safeguards in respect of children.

Efforts need to be made to guarantee the security of minors and the minimum age for consent should be raised, in line not only with the Spanish experience but also following the *Facebook* and *Instagram* terms and conditions to create an account.

2. The regulation of the **Data Protection Officer** (DPO) (articles 34-37). This is structured in an open and flexible manner due to different features: a) its mandatory or voluntary nature, b) its operation within or outside the organisation and c) for both legal entities and individuals.

In any case, the LOPDGDD lists a series of concrete and potential scenarios that must be communicated to the competent authority who shall maintain a public and regularly updated list accessible by any person. It is considered that the new LOPD is undermining the figure of the new DPO[21]. This legal uncertainty could undermine their effective implementation as it is not fully regulated in the GDPR nor in the current LOPD[22].

3. Impediments to **scientific and biomedical research**. Article 6 of the LOPDGDD imposes the requirement of different types of consent for different purposes of processing personal data[23].

20 Fernández Pérez, Ana, "La protección de los derechos fundamentales de los menores en Internet desde la perspectiva europea", *Ius et Praxis*, vol. 22, n. 1, 2016, pp. 377-416.

21 In fact, they are configured as a flexible body as they can be a natural or legal person. Also, it can be accredited on a voluntary basis by the new certification scheme (in compliance with the standards UNE-ISO/IEC 17024:2012) issued by the AEPD in cooperation with the National Accreditation Body (ENAC). Further information about the certification scheme can be found at: https://www.enac.es/esquema-delegado-proteccion-datos-aepd. In addition, the Draft qualifies the narrow list of entities that must have a DPO which includes the following: big companies, network operators and other electronic communications services providers (only if they process large-scale personal data regularly and systematically), information society services (if undertaking large-scale profiling of the service›s users) and organisations operating with commercial reports concerning natural persons.

22 As evidence of the doubts raised by the DPO figure, during the procedure of the LOPD project, some members have registered official questions addressed to the Government and related to the requirements required to be DPD (Chamber of Deputies, Parliamentarian Group of *Unidos Podemos - En Comú Podem* – In Marea, 31 January 2018. http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW12&PIECE=IWB2&FMT=INITXD1S.fmt&FORM1=INITXLUS.fmt&NUM1=&DES1=&DOCS=9-9&QUERY=%28I%29.ACIN1.+%26+%28PROTECCION+DE+DATOS%29.ALL.) (Chamber of Deputies, Parliamentary Group of *Esquerra Republicana*, 14 February 2018, http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW12&PIECE=IWB2&FMT=INITXD1S.fmt&FORM1=INITXLUS.fmt&NUM1=&DES1=&DOCS=8-8&QUERY=%28I%29.ACIN1.+%26+%28PROTECCION+DE+DATOS%29.ALL)

23 Martínez Martínez, Ricard, "Big data, investigación en salud y protección de datos: ¿un falso debate?", *Revista Valenciana d'Estudis Autonòmics*, n. 62, 2017, pp. 235-280; Díaz Revorio, Francisco J., *Los*

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

This legal requirement may become an insurmountable obstacle to the further development of the biomedical research in Spain. Article 9 LOPDGDD regulates that the mere consent of the data subject shall maintain the general prohibition on processing sensitive data. Also, data processing described in article 9 (2) sub-paragraphs g), h) e i) GDPR shall be covered by the Law, which may set further requirements for the security and confidentiality of the data.

This regulation is somewhat restrictive for the investigation of cases relating to the public health and the reutilisation of personal data within the public sector (health, occupational health, national health systems, biomedical research, trials of medications and general research). A broad consent in this field is claimed in order to ensure the protection of the rights to data subjects. However, the consent shall have legitimate uses (a report issued by the AEPD establishes that the broad consent shall be included in the current LOPD). This includes technical measures, access restrictions, ethical committees or the legality in the re-use of personal data or documents containing anonymous data for research purposes and access thereto by unauthorised third parties.

4. The LOPDGDD regulates also the scope of use of **video-surveillance** data. It clarifies that these images can only be obtained by employers in specific cases, for example, where there is a reasonable suspicion that an employee has committed unlawful (Article 22) .[24].In addition, personal information recorded by a natural person in his own home is excluded.

However, contributors are unanimous about the need to prevent the serious regression of workers' rights in the current regulation. It is manifestly diverging from the existing protections recognised in the *ruling* of the *European Court of Human Rights* in the case of *López Ribalda and Others v. Spain*.[25] It should be specified that information must be given in advance including the right to information for workers' representatives. The data protection regulation should not be the appropriate legal instrument for assessing the evidential value of the images. The requirements for processing personal data should be delimited appropriately.

5. Treatment processing conducted by **Public Administrations**. The payment of all financial sanctions is not foreseen, pursuant to the "cash unit principle". This principle implies that the funds collected by the AEPD are directly transferred to the General Administration of the State. This means that in the case of infringement committed by a public office, the public administration that imposed the corresponding penalty would not have its own resources to compensate for damages resulting from its actions and acts. Consequently, citizens would bear the economic burden. This is compatible with article 77 of the LOPDGDD, which establishes the sanctions regime in the public sector.

6. The **obligation to block** as an interim measure (article 32). Blocking is an obligation imposed on data controllers to retain personal data that has been erased so that it may be made available to judicial or administrative authorities. This provision prevents the erasure of personal data that could cover-up potential breaches. However, this measure is not laid down in the GDPR and other EU countries have not included this provision in their national legislations.

In Spain, this provision has given rise to serious misgivings for the following reasons: a) the recognition of the right to purpose limitation principle for the processing of data, which has a similar effect to blocking for those who ensure data subjects' rights in the event of possible claims, b) the lack of time limits and c) the need to specify when a derogation from this obligation could be feasible.

7. Lack of modernisation of the Spanish Data Protection Agency (Articles 44-56). In the new LOPD, the AEPD is established as an independent administrative authority, whose relations with the Spanish Government is carried out though the Ministry of Justice. A greater cooperation and coordination with the corresponding autonomous community of data protection authorities is required to increase efficiency and improve the internal functioning and transform the structure, staffing and resources. LOPDGDD contains what seems to be a hierarchical relationship between the AEPD and the *de facto* subordination of the Basque

derechos humanos ante los nuevos avances científicos y tecnológicos: genética e internet ante la Constitución, Tirant lo Blanch, Valencia, 2009 and Morales Barceló, Judith, "Big data y protección de datos: especial referencia al consentimiento del afectado", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 44, 2017.

24 Goñi Sein, José Luis, "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores. Análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", *Revista de Derecho Social*, n. 78, 2017, pp. 15-42 and Martínez López-Sáez, Mónica, "La vigilancia electrónica en el contexto laboral europeo y estadounidense: perfilando el derecho a la protección de datos en el trabajo", *Revista General de Derecho del Trabajo y de la Seguridad Social*, n. 47, 2017.

25 ECHRs, Case of *López Ribalda and Others v. Spain* (Applications num. 1874/13 and 8567/13), Third Section, 9 January 2018.

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

and Catalan Data Protection Agencies. Article 56 LOPDGDD states that only the AEPD is responsible for the foreign policy. Articles 57 to 62 establishes clearly that both agencies will be competent to exercise the functions set out in article 57 and 58 GDPR as regards the processing of personal data of the public sector for entities in their territory or those providing services relating directly or indirectly in their territory (paragraph a) article 57), data processing carried out by natural or legal persons in the in the exercise of public functions in relation to matters that are within the competence of the regional or local administration (paragraph b) and data processing foreseen in the Statute of Autonomy (paragraph c).

Finally, the processing of personal data according to Directive (EU) 2016/680 shall continue to be governed by the former LOPD 15/1999 according to article 22 and its implementing provisions, until new legislation, incorporates the content of the aforementioned directive into Spanish law enters into force. Besides, articles 23 and 24 of the former LOPD regulate a series of exceptions in the field of the protection of national security, defence, or public security. Those provisions, which passed in application of Article 13 of Directive 95/46/EC, remain in force until expressly amended, replaced or repealed.

VI-CONCLUSIONS

A "new inflection point" in the development of a data protection culture took place during 2018 not only because the GDPR came into force on 25 May 2018 in all member states to harmonize data privacy laws across Europe but also in the fact that Spain complied with the approval of the new Data Protection Act, which entered into force on 7 December 2018 by adapting the GDPR at the last moment. It reflects the political consensus that was achieved with the support of the lower house.

The LODPGDD does not reproduce the full content of the GDPR so both legal texts will have to be read together to ensure the correct application of the GDPR at Spanish level. However, the new LOPD takes advantage of a number of derogations under the GDPR including sensitive personal data, children's Data, digital rights or DPOs.

Furthermore, the following substantive changes have been incorporated in the new Act compared to the former LOPD.

- Firstly, new security measures aimed at adapting appropriately the level of security to the potential risk.
- Secondly, the requirement of consent is reinforced. The explicit consent in article 6 LODPGDD requires the express and unconditional consent given in an intelligible, easily accessible form and also with the purpose for data processing attached. Besides, information layers allow users to have access to basic information and personal data easily through email.
- Thirdly, the implementation of the right to access, correction and deletion of data pertaining to the deceased are included in the new LOPD.
- Fourthly, the prohibition of black list concerning sensitive data and the transparency requirement shall constitute an important safeguard as Internet users will be better informed about what happens to their personal data but it will also become easier for them to exercise their ARCO rights (access, rectification, erasure and objection).
- Fifthly, the exclusion files regarding advertisement will be strengthened, so spamming will be prohibited except with respect to subscribers who have indicated that they want to receive unsolicited e-mails for direct marketing purposes.
- Sixthly, the Spanish LOPD will include some references to the need for am extra-judicial settlement of conflicts policy to "promptly" resolve disputes.
- Seventhly, the new AEPD will have a rank of Secretariat-General and will be in charge of the protection of some citizen digital rights, ensuring compliance with articles 89 to 94 to perform their duties and exercising its statutory powers. The presidency election procedure is amended since the person proposed by the Government shall be ratified in the Congress (3/5 majority and absolute majority in the runoff election).
- Finally, the LOPDGDD updated video surveillance treatment and promotes the figure of the DPO. Specifically, it includes a full catalogue of sectors in which its appointment is mandatory with the obligation to report the appointment to the AEPD within a maximum period of 10 days.

THE ADAPTATION OF THE GDPR IN SPAIN by, *Dr. Cristina Pauner and Jorge Viguri*

(for example, credit institutions, insurance companies or investment services companies, among others).

The Socialist Group (currently the Spanish Government) presented the most relevant amendments to the LOPDGDD, especially with regard to the new catalogue of digital rights, which encompasses net neutrality, universal internet access, digital security, digital literacy, the protection of minors from internet dangers, privacy of employees and their right to digital disconnection, the amendment or updating of information online, the right to be forgotten on search engines and social networks and the regulation of the right to a digital last will and testament. They have been firmly committed to the transformation of the current law towards a Digital Rights Charter.

At the time of writing, the controversial issue concerning the LOPDGDD application is concerned with the third final provision that modifies article 58 of the Spanish Electoral Law, which establishes that political parties, electoral coalitions and groups "may use the personal data obtained through the access websites and other web-based sources to implement political activities during the electoral period".[26]

Certain associations and representatives of political parties have expressed reservations regarding electoral manipulation in the use of marketing techniques through instant messaging and social networks. Faced with these expressions, the AEPD issued a statement before the enactment of the LOPDGDD stating that the new Act "does not allow the processing of personal data for profiling based on political opinions" and "does not allow the personalised sending of information based on ideological or political profiles". [27] Specifically, the LOPDGDD only allows using such information in line with Recital 56 of the GDPR, which states that "the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established". The text allows the sending of electoral propaganda as long as its content is not based on aforementioned profiling technique. It shall be identify the electoral nature ensuring the free exercise of the right of opposition. In any case, the provisions of this article included in the Electoral Act shall comply with all the guarantees established in the GDPR.

Ultimately, the AEPD has just publicised an updated list in its website allowing to search for the DPO registered with it[28], which mark a very important step for extra legal certainty in a key sector for the consistent implementation of the data protection legislation.

26 *Podemos* political party has announced it will file an appeal before the Constitutional Court.

27 *Criteria of the Spanish Data Protection Authority concerning electoral issues in the LOPD Project*, November 21, 2018. The note is available only in Spanish at: https://www.aepd.es/prensa/2018-11-21.html

28 For an individual DPO search, visit the following link: https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf

REPORT ON THE HARMONIZATION OF ITALIAN LAW WITH THE ENFORCEMENT OF THE EU GENERAL DATA PROTECTION REGULATION 2016/679

By Monica A Senor
Staff member of the Italian Supervisory Authority. The opinions expressed in this article are those of the author and do not reflect the official policy or position of the Authority, the Garante per la protezione dei dati personali.

By Dr. Massimo Durante
Associate Professor of Jurisprudence and Legal Informatics, Department of Law, University of Turin. For correspondence: massimo.durante@unito.it

I-INTRODUCTION

The right to privacy and the right to data protection do not find direct and explicit recognition in the Italian Constitution. These rights were originally the result of jurisprudential elaboration, mainly through reference to the principle of the development of human personality as enshrined in Article 2 of the Italian Constitution. Those rights are then entered into the Italian legal system through their recognition at the European level in the European Convention on Human Rights (1950) and in the Charter of Fundamental Rights of the European Union (2000), known as the Charter of Nice, which has the same legal value as the European Union Treaties following the entry into force of the Treaty of Lisbon in 2009.

The Italian Data Protection Act n. 675 of 31.12.1996 (directed to the "protection of people and other subjects with regard to the processing of personal data") was the first Italian law adopted in the field of privacy and data protection as a part of the process of transposing EU Data Protection Directive n. 95/46/EC (the Data Protection Directive). Other legal statutes were adopted within the framework established by the Data Protection Directive in addition to the Italian Data Protection Act. However, the Italian Data Protection Act of 1996 – which was necessary in order to comply with the requirement of Schengen Convention to protect personal data – did not actually amount to a full implementation of the Data Protection Directive. Indeed, it led some to comment that "The origin of this legislation, somehow 'instrumental' to the full achievement of the Internal Market, including the free movement of people, well explains because in some countries of the Union, among which unfortunately Italy, the protection of personal data, often simply referred to as the protection of privacy, has been, for quite a long time, hardly understood and shared"[1].

For this reason and following the digital evolution that occurred in the 1990s, this law was superseded by a more comprehensive Italian law in the field of privacy and data protection, namely the legislative decree no. 196 of 2003, that is, the Italian Personal Data Protection Code (also known as the Italian Code of Privacy), which fully implemented the Data Protection Directive on personal data processing, as well as the further EU directives issued in the field, in particular the e-privacy Directive (02/58/EC). The provisions of the Italian Personal Data Protection Code has ensured that personal data has been processed by respecting data subjects' rights, fundamental freedoms and dignity with specific regard to confidentiality, personal identity and the right to personal data protection[2]. The processing of personal data has been regulated in a very detailed and systematic way in the Italian legislation, by affording a high level of protection for the rights and freedoms of individuals, in line and compliance with the principles of simplification, harmonization and effectiveness of the protection granted to data subjects. Even if Italy was very late in the full implementation of the EU Data Protection Directive n. 95/46/EC, the Italian Personal Data Protection Code has been considered one of the most comprehensive and in-depth legislation on data protection in Europe.

However, the Italian regulation in the field of data protection has largely rested on an authorization scheme based on the paradigm of notice and consent and on the prior consultation of the Supervisory authority, which characterized the Italian Personal Data Protection Code. Moreover, the fulfillment of the obligations deriving from such a Code were mostly conceived of and carried out as a process of compliance with a checklist of formal requirements, based on a static view of the subjects involved (data subjects, data processors or data controllers). The Italian implementation of the privacy and data protection regulation must therefore adapt to the radical change in perspective determined by the risk-oriented approach and by the principle of accountability, on

1 F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, p. 61.

2 P. Guarda, "Data Protection, Information Privacy, and Security Measures: An Essay on the European and the Italian Legal Frameworks", in *Ciberspazio e diritto*, 2008, pp. 65-92. Available online at: https://ssrn.com/abstract=1517449.

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

which the GDPR is based. This requires data processors and controllers as well as the supervisory authorities to keep up with the technological evolution in the processing of personal data, which the European regulator could not directly address in the GDPR (that is the reason why the GDPR does not even mention, for instance, Big Data, Cloud Computing, Intelligent Ambient, or the Internet of Things).

Against this backdrop, it is important that the current harmonization of the Italian law with the GDPR take into account the abovementioned constant technological evolution in the processing of personal data. It is exactly in this framework that national supervisory authorities are called upon to verify data controllers and processors' compliance with GDPR. This point has been stressed by Franco Pizzetti, a former Italian Supervisory Authority President, who remarked that: "[...] in view of the development of new technologies and of Artificial Intelligence, the resources given to the supervisory authority should be attributed, by taking into account that this authority needs to avail itself of adequate data scientists, technical and IT experts, who will support the Supervisory Authority in exercising its powers of control and supervision also in the abovementioned technological fields"[3].

In the following sections, we have focused our attention on the main points established by the Italian legislative decree no. 101 of 10 August 2018 (henceforth the decree[4]) concerning the harmonization of the Italian law with the enforcement of the EU General Data Protection Regulation 2016/679, which provides, at the art 27, the partial abrogation of the legislative decree n. 196 of 2003, that is the Italian Personal Data Protection Code. The Code was amended by the decree adapting the national Italian legal system to the GDPR and a some provision has been added, according to the derogations allowed by the "opening clauses" provided by the GDPR.

II-GENERAL PROVISIONS

A-The definition of "communication" and "dissemination"

The Italian legislature intervened, diverging partially from the EU Regulation 2016/679, introducing two specific definitions with reference to the notion of "communication" and "dissemination".

Article 4(1)(2) of the GDPR provides for the definition of "processing" as "*any operation or set of operations which is performed on personal data or on sets of personal data*", among which "disclosure" and "dissemination" are mentioned without any specific definition.

The Italian legislature defines communication as "*disclosing personal data to one or more identified entities other than the data subject, the data controller's or data processor's representative not established in the Union, the data processor and any persons who, under the direct authority of the controller or the processor, are authorised to process personal data, in any form whatsoever, including by making available or interrogating or interconnecting such data*".

It is a much broader definition than that of "disclosure by transmission" provided by the GDPR, as communication shall occur in any form.

Dissemination, instead, shall mean "*disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data*". It is a definition very close to "*dissemination or otherwise making available*" provided by the GDPR: we can even say that it is simply a specification of the meaning underlying the concept of dissemination.

The Italian legal system always kept these two processing operations separate from the others by reserving them with particular regulation for processing related to data concerning health or criminal convictions and offences, as well as with reference to the household exemption, that, in Italy, did not apply in the case of systematic communication and dissemination.

Likewise, under the current legislative decree, communication and dissemination operations are regulated more strictly than others with reference to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, to

3 F. Pizzetti, "La protezione dei dati personali e la sfida dell'intelligenza artificiale", in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, pp. 1-186, notably, par. 2.2. "La legislazione integrativa degli Stati e i vincoli posti dal Regolamento", cit. p. 12.

4 See the official Italian text of the decree at http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg. For a detailed and systematic commentary on the decree see G. Cassano, V. Colarocco, G.-B. Gallus, F.-P. Micozzi (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Giuffré Francis Lefebvre Editore, Milano, 2018.

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

processing related to genetic and biometric data and data concerning health (for which dissemination is prohibited) and with reference to a specific criminal offence.

III-PRINCIPLES

A-The lawful basis for the processing

Article 6 of the GDPR lists six lawful bases to process personal data.

Among these, Article 6(1) provides that processing shall be lawful if is: (c) necessary for compliance with a legal obligation to which the controller is subject, (e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and (f) necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

According to Article 6(2) "*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 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX*".

Article 2-*ter* of the decree provides that the basis for the processing referred to Article 6(1) of the GDPR in point (c) and (e) shall be laid down by Italian law or regulation (i.e. sources of law of primary and secondary level).

Moreover, disclosure between data controllers that process data, other than special categories of personal data and data relating to criminal convictions and offences, under the Article 6(1)(e) basis is lawful solely where a law or a regulation provides it. Failing this, disclosure is allowed only if it is necessary for the performance of tasks of public interest or in the exercise of official authority vested in the controller, it starts 45 days after the notification to the Italian Supervisory Authority ("Garante per la protezione dei dati personali") and any safeguard measures have been imposed by the Supervisory Authority to protect the data subjects.

Regarding the legitimate interest pursued by the controller as lawful basis [6(1)(f)] the Italian legislature introduced restrictions to the GDPR not provided by any open clauses.

The Italian 2018 Budget Law (Law no. 205 of 27th December 2017) provided that data controllers which processed personal data through automated means or "new technologies" on the basis of legitimate interest should send prior notification to the Italian Supervisory Authority, and wait 15 days for its approval (before commencing processing). During the 15 days, the Supervisory Authority should investigate and decide whether to approve, suspend or even stop the processing where the legitimate interests of the data controller were overridden by the interests or fundamental rights and freedoms of the data subjects.

The provision was harshly criticized because it did not seem to fall within the scope of discretionary power granted to Member States by the GDPR and, above all, the requirement for a prior check by the Supervisory Authority appeared to be at variance with the principle of accountability that characterizes the entire GDPR.

Article 22 of the decree states that from 25 May 2018, the above mentioned provision shall apply exclusively to the processing related to children' personal data for the purpose of authorizing the change of their name and surname, within the limits and according to the procedures set out in Article 36 of the GDPR.

B-Conditions applicable to child's consent in relation to information society services

Under GDPR, Article 8(1), where data subject's consent is the lawful basis for the processing, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old.

The same Article prescribes that "*Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*".

After some hesitation, adhering to the opinion expressed on the issue by the Italian Supervisory Authority, the final version of the decree, at Article 2-*quinquies*, provides that the processing of children' personal data shall be lawful where the child is at least 14 years old. It also provides that, where the child is below that age, the processing is lawful only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child.

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

Moreover, the data controller shall provide children with intelligible and easily accessible information and use clear and plain language.

C-Processing of particular categories of personal data necessary for reasons of significant public interest

Article 2-*sexies* of decree, which refers to Article9, paragraph 1, of the GDPR, sets specific conditions for the legitimate processing of particular categories of personal data, which are processed for reasons of significant public interest. More specifically, Article 2-*sexies* of the decree provides that the processing of the particular categories of personal data referred to in Article 9(1) of the GDPR, necessary for reasons of significant public interest, pursuant to the letter g), paragraph 2, of the same Article, are allowed if they are provided for by law of the European Union or, in the internal legal system, by provisions of law or, in the cases provided by the law, of regulation specifying the types of data that can be processed, the operations that can be carried out and the reason of significant public interest. It is important to remark that, pursuant to Article 2-*sexies*, paragraph 1, of the current decree, the provisions allowing the processing of such particular categories of personal data may be established, in the internal legal system, by *primary* or *secondary* sources of law.

Article 2-*sexies*, paragraph 2, sets out a legal presumption, by providing that, without prejudice to what established by paragraph 1, the processing carried out in the following areas or in others expressly identified by the law are considered carried out for reasons of public interest (that is, areas where a provision of law or regulation that envisages a reason of public interest already exists):

a) access to administrative documents and civic access;

b) keeping of records and records of civil status, of the registry of the population residing in Italy and of Italian citizens residing abroad, and electoral lists, as well as issuing identification or travelling documents or change of personal details;

c) keeping of the public registry of movable and immovable property

d) keeping of the national registry of drivers and of national vehicle archives;

e) citizenship, immigration, asylum, condition of the foreigner and refugee, state of refugee;

f) active and passive electorate and exercise of other political rights, diplomatic and consular protection;

g) exercise of the mandate of the representative bodies;

h) carrying out the functions of control, political address, parliamentary inquiries and access to documents for purposes connected with the carrying out of an elected mandate;

i) activities of public entities directed to the enforcement, also through their subsidiaries, of the provisions on taxation and customs;

l) control and inspection activities;

m) granting, winding up, modifying and revoking economic benefits, facilitations, donations, other emoluments and qualifications;

n) awarding of honors and rewards, recognition of the legal personhood of associations, foundations and institutions, including of worship, of ascertainment of the requisites of honorability and professionalism for the appointment, as for the profiles of competence of the public bodies, also for offices of cult and directives of legal persons, business and non-state education, as well as for the issuing and revoking of authorizations or qualifications, the granting of patronage and representation awards, membership of honorary committees and admission to ceremonies and institutional meetings;

o) relations between public entities and third sector entities;

p) conscientious objection;

q) sanctions and protection activities in administrative or judicial fora;

r) institutional relations with religious institutions, religious confessions and religious communities;

s) social-welfare activities for the protection of minors and persons in need, not self-sufficient and

incapable individuals;

t) administrative activities related to activities of diagnosis, assistance or health or social therapy;

u) tasks of the national health service and of bodies operating in the health sector, as well as tasks of

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

hygiene and safety in the workplace and health and safety of the population, civil protection, safeguarding of life and physical safety;

v) planning, management, monitoring and evaluation of health care;

z) supervision of trials and drugs, authorization to trade and import medicines and other health products

aa) social protection of motherhood and voluntary interruption of pregnancy, addictions, assistance, social integration and rights of the disabled;

bb) education and training in professional, university or higher education;

cc) data processing carried out for archiving purposes in the public interest or for historical research, concerning the conservation, organization and communication of documents held in the State archives, in the historical archives of public bodies, or in private archives declared of significant historical interest, for the purposes of scientific research, as well as for statistical purposes by subjects that are part of the national statistical system (Sistan);

dd) establishment, management and extinction, by subjects who perform tasks of public interest or related to the exercise of public authority, of work relations of any kind, also unpaid or honorary, and other forms of employment, trade union matters, employment and compulsory placement, retirement planning and assistance, protection of minorities and equal opportunities in the context of employment relationships, fulfillment of the remuneration, tax and accounting obligations, hygiene and safety at work or safety or health of the population, ascertainment of the civil liability, disciplinary and accounting, inspection activity.

Article 2-*sexies*, paragraph 3, of the decree, further provides that processing of genetic, biometric or health-related data take place in compliance with the provisions of Article 2-*septies* of the decree.

D-Safeguards measure for the processing of genetic data, biometric data or data concerning health

Article 2-*septies* of the decree, which refers to Article 9, paragraph 4, of the GDPR, sets specific conditions for the lawful processing of genetic data, biometric data or data concerning health. Notably, it calls for the adoption of *safeguard measures* by the Italian Supervisory Authority. Pursuant to Article 9, paragraph 4, of the GDPR, "*Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health*", Article 2-*septies*, paragraph 1, of the decree provides that the processing of genetic data, biometric data or data concerning health is legitimate when:

a) one of the conditions set out in Article 9, paragraph 2, of the GDPR applies;

b) the processing of such particular categories of data is compliant with the safeguard measures adopted by the Supervisory Authority.

Article 2-*septies*, paragraph 2, of the decree provides that the provisions that establishes the safeguard measures referred to in paragraph 1 shall be adopted at least every two years and take into account:

a) the guidelines, recommendations and best practices published by the European Committee for the Protection of Data and the best practices in the field of processing of personal data;

b) the scientific and technological evolution in the sector covered by the measures;

c) the interest in the free movement of personal data in the territory of the Union European.

Let us focus our attention on the paragraphs 3-6 of Article2-*septies*, of the decree, detailing the safeguard measures adopted by the Supervisory Authority:

- Article 2-*septies*, paragraph 3, provides that the provision scheme – through which the Supervisory Authority adopts the safeguard measures – shall be subject to public consultation for no less than sixty days.

- Article 2-*septies*, paragraph 4, redundantly provides that safeguard measures shall be adopted in compliance with Article 9, paragraph 2, of the GDPR, and also concern the safeguard measures to be taken regarding:

  a) markings on vehicles and access to restricted traffic areas;

  b) organizational and management profiles in the health sector;

  c) modalities for the direct communication to the interested party of the diagnoses and data related to own health;

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

d) prescription of medicines.

- Article 2-*septies*, paragraph 5, provides that the safeguard measures shall be adopted in relation to each category of personal data referred to in paragraph 1, having regard to the specific purposes of the processing and may identify, in compliance with paragraph 2, further conditions on the basis of which the processing of such data is permitted. The safeguard measures shall provide for security measures, including pseudonymisation and encryption, minimisation measures and selective access to personal data.

- Article 2-*septies*, paragraph 6, provides that safeguard measures related to genetic data and those referred to in paragraph 4, letters b, c, and d, shall be adopted after consulting the Minister of Health who, for this purpose, acquires the opinion of the Health Care Superior Council. For genetic data, in case of particular and high risk, the safeguard measures can identify consent as an additional measure to protect the data subject's rights, pursuant to Article 9 (4) of the GDPR, or other specific safeguards.

- Article 2-*septies*, paragraph 7, provides that biometric data shall be used for physical and logical access controls, according to specific safeguard measure and in the context of security measures provided by Article 32 of the GDPR.

- Finally, Article 2-*septies*, paragraph 8, provides that personal data referred to in paragraph 1 shall not be disseminated. This means that dissemination of such data is presumed to be a risky activity per se, which needs to be prohibited.

IV-RIGHTS OF THE DATA SUBJECT

Under Article 23 of GDPR, 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 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard a well-specified list of public interest.

Article 2-*undecies* establishes a list of restrictions to the rights provided for in Article 15 to 22 where, asserting them, detriment may occur to:

a) interests protected by money laundry laws;

b) interests protected by provisions on support for victims of extortion;

c) activities carried out by Inquiry Parliamentary Committees;

d) activities carried out by Public Authorities, except for profit-seeking Public Authorities, for monetary and financial purposes;

e) investigations carried out by defence counsels or establishing or defending a legal claim;

f) protecting a whistleblower' s identity, pursuant to the Italian law n.179 of 2017.

Restrictions to the rights provided for in Article 12 to 22 and 34 have been introduced in order to safeguard the protection of judicial independence and judicial proceedings (Article 2-*duodecies*).

V-DATA CONTROLLER AND DATA PROCESSOR

A-Attribution of roles and tasks to designed subjects

Article 2-*quaterdecies*, paragraph 1, of the decree, which refers to Article 4, paragraph 1, num. 10, and Article 29 of the GDPR, establishes that the controller or processor may provide, in the context of their own organizational structure, which specific tasks and functions related to the processing of personal data are attributed to specifically designated natural persons operating under the their authority.

Article 2-*quaterdecies*, paragraph 2, of the decree, provides that the controller or processor shall identify the most appropriate methods for to authorize the processing of personal data by persons who operate under their own direct authority.

The former national law (the Italian Personal Data Protection Code) used to define, under the Article 4, paragraph 1, letter h), this figure as the "designed person for the data processing" ("incaricato del trattamento dei dati"), i.e., the natural person authorized by the controller or processor to perform specific processing of personal data under the direct authority of the controller or processor. Pursuant to Article 30, paragraph 2, of the Italian Personal Data Protection Code, their designation was necessarily written and it identified the scope of the authorized processing, whereas, pursuant to Article 2-*quaterdecies*, paragraph 2, of the decree, it is left to the controller or processor to identify "the most appropriate methods" for to authorize the processing of personal data by persons operating under the controller's or processor's direct authority.

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

B-Processing presenting specific risks for the performance of a task carried out in the public interest.

Article 2-*quinquiesdecies* of the current decree, which refers to Article 35 and Article 36, paragraph 5, of the GDPR, provides that, with regard to the processing of personal data carried out for the performance of a task of public interest that may present particularly high risks pursuant to Article 35 of the Regulation, the Supervisory Authority can, on the basis of the provisions of Article 36, paragraph 5, of the same Regulation and with general measures adopted ex officio, prescribe

measures and actions to guarantee the data subject, that the data controller is required to adopt.

This provision tends to require, in this particular context (i.e. the processing of personal data carried out for the performance of a task of public interest that may present particularly high risks) – more than a prior consultation or authorization (as provided by Article 36, paragraph 5, of the GDPR), i.e. an *ex ante* power of intervention of the Supervisory Authority through the adoption of general measures *ex officio* and the injunction of specific measures and actions to be adopted by the data controller.

VI-REMEDIES, LIABILITY AND PENALTIES

Article 141 of the Italian Personal Data Protection Code provided three kinds of administrative remedies: complaints, reports and claims. The first remedy (*complaint*) consisted in a procedure set out in order to point out an infringement of the most relevant provisions of Data Protection Code. The second remedy (*report*) allowed the data subject to lodge a report, if no circumstantial complaint might be lodged, in order to call upon the Italian Supervisory Authority to check up on the aforementioned provisions of Data Protection Code. The third one (*claim*) was a non-judicial remedy set out, in order to ask for the enforcement of the data subject's rights, by lodging a claim before the Supervisory Authority, which prevented the data subject to bring an action for the same matter before the judicial authority.

Under the GDPR, the only remedy is the right to lodge a complaint before the Supervisory Authority so the decree removes any reference to the claim procedure, provides how the data subject can lodge a complaint before the Italian Supervisory Authority and re-establishes reports, providing that whoever may lodge a report before the Italian Supervisory Authority, who is called upon to assess it for the purpose of the corrective powers referred to in Article 58 of the GDPR.

With regard to penalties, Article 84 of the GDPR provides that Member States shall regulate the other penalties applicable to the infringements of the Regulation, and in particular, for infringements, which are not subject to administrative fines pursuant to Article 83. Furthermore, Member States shall take all measures necessary to ensure that penalties apply. Such penalties shall be effective, proportionate and dissuasive.

Under the former Italian Personal Data Protection Code, four criminal offences were regulated:

1. unlawful data processing;

2. untrue declarations and notifications submitted to the Italian Supervisory Authority;

3. failure to comply with security measures;

4. failure to comply with provisions issued by the Italian Supervisory Authority.

In order not to impinge on the fundamental "*ne bis in idem*" principle (i.e. the right not to be subject to trial or punishment twice), as the European Court of Human Rights applied it in the *A and B v. Norway Judgment*[5], the Italian legislature, in the first version of the legislative decree of harmonization, chose to provide only one criminal offence (instead of the four above mentioned ones).

The final version of the decree, on the contrary, provides several criminal offences.

The previous crimes, provided by Article 167 of the Italian Personal Data Protection Code, titled "*Unlawful data processing*", have been replaced by three new ones, which are partially different.

Under the new Article 167, paragraph 1, "*any person who, with a view to gain for himself or another, or with the purpose to cause damage to the data subject, by processing personal data in breach of Articles 123, 126 e 130 or of the provision made further to Article 129 of the Italian Data Protection Code, causes harm to the data subject, shall be punished by imprisonment for between six and eighteen months, unless the offence is more serious*".

Articles 123, 126, 129 and 130 of the Italian Personal Data Protection Code are provisions related to electronic communication services, which remain in

5 https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-168972%22]}

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

force until the e-privacy Regulation will be approved.

Under the new Article 167, paragraph 2, "*any person who, with a view to gain for himself or another, or with the purpose to cause damage to the data subject, by processing special categories of personal data or personal data relating to criminal convictions and offences in breach of Articles 2-sexies, 2-octies, or in breach of the safeguard measures provided by Article 2-septies, or in breach of the measures adopted pursuant Article 2-quinqiuesdecies of the Italian Data Protection Code, causes harm to the data subject shall be punished by imprisonment for between one and three years, unless the offence is more serious*".

Article 2-*sexies* of the Italian Personal Data Protection Code, as seen above (see Section 3.3), is an Italian special provision related to the processing of particular categories of personal data necessary for reasons of significant public interest. Article 2-*septies* is an Italian special provision concerning safeguard measure (see Section 3.4). Article 2-*octies* is an Italian special provision related to the processing of personal data relating to criminal convictions and offences. Articles 2-*quinquiesdecies* is an Italian special provision that provides general application orders of the Supervisory Authority with regard to types of data processing that are likely to result in a high risk according to Article 36 of the GDPR (see Section 5.2).

Under the new Article 167, paragraph 3, "*any person who, with a view to gain for himself or another, or with the purpose to cause damage to the data subject, by transferring personal data to a third country or an international organization in breach of Articles 45, 46 or 49 of the GDPR, causes harm to the data subject, shall be punished by imprisonment for between one and three years, unless the offence is more serious*".

Two other new criminal offences are now provided by Article 167-bis of the new Italian Personal Data Protection Code, titled "*Unlawful communication and dissemination of personal data related to a large number of people*".

Under the new Article 167-bis, paragraph 1, "*any person who, with a view to gain for himself or another or with the purpose to cause damage, disclose or disseminate personal data related to a large number of people, in breach of Articles 2-tre, 2-sexies and 2-octies of the Italian Personal Data Protection Code shall be punished by imprisonment for between one and six years, unless the offence is more serious*".

Under the new Article 167-bis, paragraph 2, "*any person who, with a view to gain for himself or another or with the purpose to cause damage, disclose or disseminate, without the data subject's consent, personal data related to a large number of people shall be punished by imprisonment for between one and six years, if the consent is the legal basis for communication and dissemination, unless the offence is more serious*".

Article 167-ter of the edited Italian Personal Data Protection Code provides a new criminal offence titled "*Fraudulent acquisition of personal data*".

Under that Article, "*any person who, with a view to gain for himself or another or with the purpose to cause harm, acquire with fraud personal data related to a significant number of people shall be punished by imprisonment for between one and four, years, unless the offence is more serious*".

The new Article 168 provides two criminal offences titled "*Untrue declarations to the Italian Supervisory Authority and interruption of the execution of the tasks or the exercise of the powers of the Italian Supervisory Authority*".

Under the new Article 168, paragraph 1, "*any person who declares or attests to untrue information or circumstances, or else submits forged records or documents, in connection with communications, records, documents or statements that are submitted or made, as the case may be, in a proceeding before the Italian Supervisory Authority and/or during inquiries, shall be punished by imprisonment for between six months and three years, unless the offence is more serious*".

Under the new Article 168, paragraph 2, "*any person who, outside the cases above referred, intentionally interrupts or disturbs the regularity of a proceeding before to the Italian Supervisory Authority or of an investigation carried out by the Italian Supervisory Authority shall be punished by imprisonment up to one year*".

The new Article 170 provides a criminal offence titled "*Failure to comply with provisions issued by the Garante (the Italian Supervisory Authority)*".

Under the new Article 170 "*Any person who, fails to comply with a provision issued by the Garante according to its corrective powers provided for by Article 58, paragraph 2, letter f) of the GDPR, or by Article 2-septies of the Italian Data Protection Code or by Article 21 of*

ITALIAN ADAPTATION OF THE GDPR by, *Monica A Senor and Dr. Massimo Durante*

the decree, shall be punished by imprisonment for between three months and two years".

VII-OPENING CLAUSES: A GENERAL OVERVIEW

In the present and last paragraph, we briefly expound to the so-called "opening clauses", which are strictly considered as the clauses that allow the Member States to fill in some provisions of the GDPR, by establishing some derogations to those provisions.

We identified fifteen opening-clauses of this kind: notably, Article 6(2); Article 8(1); Article 9(4); Article 23(1); Article 35(10); Article 36(5); Article 49(5); Article 80(2); Article 83(7); Article 84(1); Article 85(2); Article 87(12); Article 88(1); Article 89(2); Article 90(1).

As seen above, the Italian legislature introduced some more specific provisions, in order to implement Article 6(2) (see Section 3.1), Article 8(1) (see Section 3.2), Article 9(4) (see Section 3.4), Article 23(1) (see Section 4), Article 36(5) (see Section 5.2), and Article 84(1) (see Section 6).

According to Article 85(2), the Italian legislature saved, with few changes, exemptions and derogations related to the processing of personal data for journalistic purposes as well as for academic, artistic or literary purposes as provided by the Italian Personal Data Protection Code.

According to Article 88(1), the Italian legislature saved, with few changes, exemptions and derogations related to the processing of personal data in the context of employment as provided by the Italian Personal Data Protection Code.

According to Article 89(2), the Italian legislature saved, with some changes, exemptions and derogations related to the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as provided by the Italian Personal Data Protection Code.

Last December, the Italian Supervisory Authority, according to the decree, verified compliance with the GDPR of the previous ethical Codes for the processing of personal data for journalistic purposes, archiving, historical, statistical and scientific purposes. They have been renamed ethical rules (Regole deontologiche) and they are in the process of being published in the Italian Official Journal[6].

6 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069732

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR: TOWARDS THE EFFECTIVE PRIVATE ENFORCEMENT OF COLLECTIVE DATA PROTECTION RIGHTS

By Dr. Alexia Pato
Research fellow at the Institute for German and International Civil Procedure, University of Bonn (Germany). For correspondence: apato@uni-bonn.de

I- INTRODUCTION

Article 80 of the General Data Protection Regulation (GDPR) requires Member States to introduce collective redress[1] – in the form of the representative action– into their procedural legal order with the objective of filling the private enforcement gap.[2] This provision enables representative entities, such as consumer associations, to exercise some rights on behalf of data subjects.

The present chapter provides an interpretation of Article 80 GDPR (section 2) and analyses how Member States have incorporated that provision into their laws (section 3). In particular, the laws of France, Belgium, Spain, Germany, Austria and the United Kingdom (UK) are examined. Then, some practical examples regarding the application of Article 80 GDPR are presented (section 4). Section 5 concludes that Member States have adopted requirements departing from the wording of Article 80 GDPR. However, this chapter argues that the room for manoeuvre allocated by Article 80 GDPR is limited and therefore, the misalignment between national and European laws should be tackled thanks to the principles of direct effect and supremacy of EU law. Alternatively, legislative amendments will be needed.

II- ARTICLE 80 GDPR: AN INTERPRETATIVE GUIDE

Article 80 GDPR requires Member States to include representative actions in their procedural legal order. It promotes a specific collective redress model, which acknowledges the importance of intermediaries for the private enforcement of individuals' rights. Such a choice is reasonable as the representative model, whereby an entity protects general or collective interests[3] is largely dominant across the European Union (EU). The adoption of the Injunctions Directive in 1998 –replaced by the Directive 2009/22/EC–, which implements the mutual recognition of qualified entities' legal standing in the consumer field, contributed to the widespread adoption of such model. Within the data protection field, this means that other collective redress models, whereby a single individual represents numerous victims,[4] or whereby no representation system is implemented, such as test case procedures,[5] fall outside the scope of the Regulation.

According to Article 80 GDPR, a body, organisation or association (hereafter, (representative) entities) properly constituted under the law of a Member State may bring a representative action on behalf of

1 Collective redress must be understood as '(i) a legal mechanism that ensures a possibility to claim cessation of illegal behaviour collectively by two or more natural or legal persons or by an entity entitled to bring a representative action (injunctive collective redress); (ii) a legal mechanism that ensures a possibility to claim compensation collectively by two or more natural or legal persons claiming to have been harmed in a mass harm situation or by an entity entitled to bring a representative action (compensatory collective redress)'. See the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law.

2 M Karg, 'DS-GVO Artikel 80 Vertretung von betroffenen Personen' in H A Wolff and S Brink (eds), *Beck'scher Online-Kommentar Datenschutzrecht* (19th ed, CH Beck 2017), paras 6-7; B Kreße, 'Artikel 80 Vertretung von betroffenen Personen' in G Sydow (ed), *Europäische Datenschutzgrundverordnung* (Nomos 2017), para 1.

3 This chapter distinguishes general interests from the collective ones, based on Article 1 of the Latin-American Model Code on Class Actions. All the websites and hyperlinks were last accessed on 4 January 2019. General interests are those which concern society or a group of people as a whole, such as damages to the environment. As for collective interests, they represent the aggregation of homogenous individual rights.

4 For example, such a scheme was used by Max Schrems, in his pursuit to litigate on behalf of thousands of victims in Austrian courts. See Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] ECLI:EU:C:2018:37.

5 For example, the test case procedure has been adopted in the United Kingdom and Germany. The first implemented the Group Litigation Order (GLO) and the second drafted the *Kapitalanlager Musterverfahrensgesetz (KapMuG)* available in the financial sector. Under the test case procedure, a court receives a multiplicity of similar claims. For procedural efficiency purposes, it usually picks up a case and solves common issues, while suspending related individual proceedings. Once the competent court rules on these common issues, individual proceedings are retaken and solved according to these findings.

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

data subjects. The number of actors who potentially have standing to sue is broad.[6] However, since this provision requires that the "statutory objectives" of a representative entity pursue public interests, only legal persons are likely to meet this criteria.[7] In addition, the representative entity must be active in the data protection field.[8] Consumer associations will usually meet those requirements easily. Other entities, such as trade unions, may be included in the scope of this provision as well.[9] Finally, the representative entity must be not-for-profit in order to avoid the emergence of a litigation market. Therefore, special purpose vehicles, such as *Cartel Damage Claims (CDC)*, dedicated to the enforcement of victims' rights in the competition law sector are to be excluded from the GDPR.[10] However, this must not preclude entities from seeking the reimbursement of their costs or seeking litigation funding opportunities.[11]

The representative action of Article 80 GDPR can be exercised in two ways:

First, Article 80(1) GDPR allows representative entities to exercise the right to lodge a complaint with a supervisory authority (Article 77 GDPR); the right to an effective judicial remedy against a supervisory authority (Article 78 GDPR)[12] a controller or a processor (Article 79 GDPR); and the right to compensation and liability (Article 82 GDPR), where provided for by national law.[13] In order to exercise those rights collectively, data subjects must give a mandate to the representative entity. Such a norm seems to have the opt-in system in mind, according to which victims must manifest their intention to be bound by the outcome of a collective redress action.[14] It has to be highlighted that the terms "mandate", "representation" and "on behalf of" should not be understood as designating a specific procedural mechanism. Therefore, Article 80 may encompass both collective redress mechanisms and the assignment of claims. An excessively narrow approach would allow national procedure(s) to unreasonably frustrate the application of this European norm.

Second, Article 80(2) GDPR offers Member States a dispositive right: they may allow entities to exercise the rights of Articles 77-79 GDPR without data subjects' mandate. In light of this, Article 80(2) GDPR supports collective redress schemes, such as the French *action de groupe* (group action), whereby entities bring their case first before national courts that will rule on the alleged wrongdoer's liability and offer victims the right to opt-in after the judgment on liability is issued (Articles L.623-1 to L.623-32 of the French Consumer Code). Additionally, the wording of Article 80(2) is broad enough to permit national legislators to set forth opt-out-based representative actions.[15] It has to be highlighted that the right to compensation and liability is excluded from Article 80(2) GDPR.

In all cases, it is unlikely that Article 80 GDPR covers actions, which aim to protect general interests.[16]

6 Kreße (n 2), para 4.
7 Karg (n 2), para 10; Kreße (n 2), para 5.
8 The conditions that a representative entity must fulfil have significantly changed throughout the legislative process. The comparative table of the GDPR published by the European Data Protection Supervisor highlights those changes. See also the explanations of Karg (n 2), paras 4-5; EM Frenzel, 'Art. 80 Vertretung von betroffenen Personen' in BP Paal and DA Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz* (CH Beck 2017), paras 3-5.
9 A Neun and K Lubitzsch, 'Die neue EU-Datenschutz-Grundverordnung – Rechtsschutz und Schadensersatz' (2017) *Betriebs-Berater*, p 2566; Karg (n 2), para 11.1.
10 Karg (n 2), para 11.2; Frenzel (n 8), para 8.
11 Neun and Lubitzsch (n 9), p 2566.
12 Articles 77 and 78 shall fall within the public enforcement sphere. Therefore, they remain outside the scope of this chapter.
13 The wording of Article 80(1) GDPR creates some confusion: since the paragraph contains only one sentence, which ends with an optional right allocated to Member States, it is not clear whether this makes the whole paragraph non-mandatory. A comparative analysis between Articles 80(1) and (2) GDPR seems to show that only the possibility to extend the representative action to the right to compensation and liability is discretionary. On the contrary, one can conclude that paragraph (2) is entirely optional since it starts with the sentence 'Member States may provide that (...)'. If paragraph (1) was also optional, one can imagine that it would start with the same kind of sentence. Additionally, the historical development of Article 80 shows that it was never intended to be entirely left to the hands of Member States. Finally, the Italian version of the text, which states that a representative entity may '*esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82*' isolates more clearly the right to compensation and liability at the end of the sentence, which reinforces the idea that only that right is dispositive. See also the explanations of Frenzel (n 8), para 9; Kreße (n 2), para 11; Neun and Lubitzsch (n 9), p 2566, who seem to come to the same conclusion. *Contra*: P Nemitz, 'Art. 80 Vertretung von betroffenen Personen' in E Ehmann and M Selmayr (eds), *Datenschutz-Grundverordnung* (CH Beck 2017), para 2.
14 Conversely, under the opt-out system, victims are automatically bound by the outcome of the collective redress action unless they say otherwise.
15 In other documents, such as the Commission Recommendation of 2013 (n 1) the EU has referred to the opt-in and out dichotomy. In the GDPR, however, another concept was introduced: representative entities act with or without mandate. This chapter contends that the term "without mandate" that is used in Article 80(2) GDPR is broader than a reference to the opt-out mechanism. It encompasses all situations where the start judicial proceedings is not submitted to the authorisation of the data subject(s).
16 Frenzel (n 8), para 11; Neun and Lubitzsch (n 9), p 2566.

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

Rather, the wording of this provision indicates that litigation is possible only where individual victims are involved. This is clear as far as Article 80(1) GDPR is concerned, inasmuch as a mandate from data subjects is necessary. Nevertheless, since Article 80(2) GDPR allows entities to act without any mandate in certain cases, the scenario that was in the European legislator's mind is not obvious. A first indication that general interests are not encompassed in that provision can be found in the title of Article 80 GDPR, which permits the *representation* of data subjects. Indeed, the representation scheme is normally used when individual victims are harmed. Conversely, entities usually *protect* or *defend* general interests but do not *represent* them. Moreover, the title of Article 80 GDPR states that *data subjects* are the ones to be represented – as opposed to public interests. Finally, Article 80(2) GDPR makes clear that an entity may litigate 'if it considers that the rights of a data subject (...) have been infringed', thereby reinforcing the idea that only collective interests are covered by Article 80 GDPR.

III-COUNTRY BREAKDOWN

In principle, European regulations do not need to be implemented by Member States. However, the GDPR has created a special situation by enacting approximately fifty open clauses, thereby allocating some freedom to derogate to national legislators.[17] Additionally, in light of the principle of procedural autonomy, the protection of data subjects' rights can only be ensured through effective national procedural rules.

This chapter examines the national adaptations of Article 80 GDPR in France (section 3.1), Belgium (section 3.2), Spain (section 3.3), Germany (section 3.4), Austria (section 3.5) and the UK (section 3.6).

A-France

In 2014, the French legislature created the group action,[18] whereby qualified entities may bring collective proceedings on an opt-in basis without a mandate from affected individuals.[19] To be more precise, data subjects may opt-in a group action after the judgment on liability is issued by the court (Article L.623-8 of the French Consumer Code). Therefore, the commencement of judicial proceedings by qualified entities does not depend on data subjects' authorisation. The group action was formerly limited to the consumer field. In 2016, however, the Law on Modernisation of Justice in the XXI Century[20] extended the substantive scope of the group action: henceforth, victims of data protection violations may use this procedural mechanism too. While such a mechanism was initially open to actions for injunctive relief, the French law adapting the GDPR[21] modifies the state of affairs: according to Article 25, group actions may be used in order to obtain damages.

Overall, the French group action complies with some of the conditions imposed by Article 80 GDPR. Specifically, the representative model was adopted to enhance the private enforcement of data subjects' rights –not only consumers– and representative entities are able to exercise both actions for injunctive relief and damages. However, one might wonder whether national law may take a step further and allow representative actions for compensation without previous mandate, in opposition to the wording of Article 80(2) GDPR.

Additionally, conditions that must be fulfilled by entities in order to bring group actions are more stringent than the ones imposed by the GDPR. In particular, Article 43ter (IV) of the Law on Information Technology, Data Files and Civil Liberty establishes that three different types of entities may exercise the group action: the first category is associations duly declared for at least

17 On the specific nature of the GDPR, see O Tambou, 'Règlement général de la protection des données : l'après 25 mai 2018' (25 May 2018) Dalloz Actualité, as well as the paper mentioned in her post: J Wagner and A Benecke, 'National Legislation within the Framework of the GDPR - Limits and Opportunities of Member State Data Protection Law' (2016) 2 *European Data Protection Law Review*, p 353-361.

18 Created by the Consumer Law of 2014 (*Loi n° 2014-344 du 17 mars 2014 relative à la consommation, also called loi Hammon*).

19 For an overview on the functioning of this procedural mechanism in English, see D Fairgrieve and A Biard, 'Country report for France', available on the British Institute of International and Comparative Law (BIICL) website; BIICL, 'The State of Collective Redress in the EU in the Context of the Implementation of the Commission Recommendation' (2017), p 583-595; A Biard and RP Amaro, 'Resolving Mass Claims in France: Toolbox & Experience', Empirical Evidence on Collective Redress Conference, Wolfson College, Oxford University, 12-13 December 2016; C Sportes and V Ravit, 'Class and Group Actions 2019 – France', available on the International Comparative Legal Guides; European Parliament, 'Collective Redress in the Member States of the European Union' (2018), p 151-167.

20 In particular, Article 91 of the Law on Modernisation of Justice in the XXI Century (*Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle*) that introduces a new Article 43ter in the Law on Information Technology, Data Files and Civil Liberty (*Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) states that several, similarly-situated victims who suffered harm stemming from a similar illegal behaviour caused by a controller or a processor may bring a group action in the civil or administrative courts.

21 Law on Data Protection (*Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*).

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

five years and having as their object the protection of privacy and the protection of personal data. The second category is consumer associations which are representative at national level and approved pursuant to Article L. 811-1 of the Consumer Code, when the processing of personal data affects consumers.[22] Thirdly, representative trade unions also have the right to bring group actions in the data protection field, when the interests of people defended by their statutes are violated. Conversely, the GDPR only requires that statutory objectives be in the public interest and does impose requirement regarding years of existence or certification. It is not clear whether Article 80 GDPR offers some room for manoeuvre that may be used by Member States to adopt more stringent requirements on standing to sue.

B-Belgium

In Belgium, the new Law on the Protection of Individuals Regarding the Processing of their Personal Data, the aim of which is to comply with the GDPR, entered into force on 5 September 2018.[23] According to Article 220 of said Law, data subjects may mandate a representative entity to act in their name and on their behalf. Entities may bring administrative complaints, as well as judicial actions. In particular, since Article 216 of the Law specifies that data subjects may seek compensation after an action for injunctive relief is brought, representative entities should therefore be able to represent them in exercising this right. Nevertheless, Belgian law imposes more stringent conditions on entities as far as standing to sue is concerned[24] and does not indicate which procedural tools those entities can use in order to enforce data subjects' rights.

Additionally, the Belgian legislature did not take the opportunity to transpose Article 80(2) GDPR. One might wonder whether this legislative choice prevents data subjects from using the *action en réparation collective*[25] introduced by the Law of 28 March 2014,[26] whereby representative entities may bring actions on behalf of victims without obtaining a mandate.[27] Through the collective action, only monetary or in kind compensation may be claimed and it is limited to the defence of consumers.[28] According to Article XVII.37(10°/1) of the Economic Code, the collective action is available in case of violation of the GDPR. This means that collective actions in the data protection field are technically available to representative entities. Nevertheless, such a solution directly contradicts the European legislator's refusal to promote actions for compensation without previous mandate. It remains to be seen how such contradiction will be solved.

C-Spain

In Spain, the recent Law on Data Protection[29] that aims to implement adaptations to the GDPR does not mention the possibility of data subjects bringing collective redress actions. Consequently, one can safely say that the default regime contained in the Spanish Procedural Law[30] is applicable. It allows a group of consumers or a

22 Accordingly, consumer associations must have one year of existence, a minimum number of members and actively defend consumers' interests.

23 *Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.*

24 In particular, the representative entity must be properly constituted according to Belgian law. The application of such condition might be problematic, as far as foreign entities are concerned. Additionally, according to Article 220 of the Belgian Law on the Protection of Individuals Regarding the Processing of their Personal Data, the entity must have been active in the data protection field for at least three years. However, this requirement is not imposed by Article 80 GDPR.

25 For an overview on the functioning of this procedural mechanism in English, see BIICL (n 19), p 392-402; O Vanhulst, 'Country report for Belgium', available on the BIICL website; S Voet and P Gillaerts, 'Resolving Mass Disputes: Belgian Report', Empirical Evidence on Collective Redress Conference, Wolfson College, Oxford University, 12-13 December 2016; European Parliament (n 19), p 133-139.

26 *Loi portant insertion d'un titre 2 'De l'action en réparation collective' au livre XVII 'Procédures juridictionnelles particulières' du Code de droit économique et portant insertion des définitions propres au livre XVII dans le livre 1er du Code de droit économique.*

27 Depending on the location of the victims (in or outside Belgium) or the type of damage to be redressed, the collective action might be based on the opt-in or opt-out model. In all cases, the representative entity may start proceedings without previously gathering victims' authorisation. Although the victims will be able to opt-in or out before a judgment on the alleged wrongdoer's liability is issued (contrary to the French group action), we consider that such scheme falls into Article 80(2) GDPR's scope, since the relevant point of reference should be the start of the action/complaint and not the judgment on liability.

28 Recently, however, a new law has been enacted (*Loi portant modification, en ce qui concerne l'extension de l'action en réparation collective aux P.M.E., du Code de droit économique*), the aim of which is to extend the application *rationae personae* of the provisions of the Economic Code regarding the collective action. In particular, the Belgian collective action can also be brought by small and medium enterprises. In case the collective action is made available for data protection breaches under the GDPR, those actors will, in any case, remain out of its scope, since the Regulation applies only to natural persons.

29 *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

30 *Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.* For an overview on the functioning of the Spanish collective action in English, see M Otero Crespo, 'The collective redress phenomenon in the European context: the Spanish case' in L Cadiet, B Hess, M Requejo Isidro (eds), *Procedural science at the crossroads of different generations*

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

representative entity, such as a consumer association, to instigate collective proceedings in Spanish courts (Article 11 of the Spanish Procedural Law). The list of potential claimants is therefore broader than that provided by Article 80 GDPR as it includes group of victims. Nevertheless, the Spanish collective action is only available to data subjects who qualify as consumers. This does not accord with the GDPR, which offers representative actions to data subjects, regardless of their status as consumers. Finally, it has to be highlighted that both collective and general interests are covered by Spanish law and both injunctive relief and damages may usually be sought.[31]

It is not clear whether the Spanish system operates on an opt-in or opt-out basis. As regards actions protecting collective interests, the Spanish Procedural Law is probably intended to be an opt-in system as its Article 221(1)(a) requires that the judgment sets out a list of consumers who will be able to benefit from the collective judgment. At the same time, this also means that the representative entity may act without previous mandate. However, if the entity uses its right to start an action for compensation on behalf of data subjects without their previous authorisation, this contradicts the wording of Article 80(2) GDPR.

D-Germany

In Germany, the usual procedural regime has been amended in order to encompass claims against data protection violations.[32] In particular, section 2 of the Law on Actions for Injunctive Relief[33] (*UKlag*) allows certain entities (section 3 *UKlag*) to bring actions for injunctive relief. At first, the said Law only applied to consumer law cases. Hence, consumer associations could only start litigation against unfair data protection policy terms.[34] The amendment of February 2016[35] extended the material scope of this provision to allow actions in cases of violation of data protection laws (section 2(2)(11) *UKlag*) –including European legislation.[36] The German legislature did not make use of the discretionary power allocated by Article 80(1) GDPR and thus, the *UKlag* does not permit actions for compensation.[37] It is not clear whether the German Law on Actions for Injunctive Relief can be used in order to protect collective interests.[38] Rather, the norm seems to be built upon the idea that representative entities may litigate to protect general consumer interests. Nevertheless, Article 80(1) GDPR requires Member States to adopt a procedural tool, whereby data subjects can ask a body to act on their behalf. Since this provision is mandatory, all Member States should provide such a procedural mechanism.

Additionally, the material scope of section 2 of the Law on Actions for Injunctive Relief appears to be more limited than Article 80 GDPR. For example, only claims against the admissibility of the collection, processing or use of personal data may be raised and those activities must pursue a commercial goal. Therefore, claims arising from the violation of the right to information, to rectification and erasure are not covered, just to mention some examples.[39] The personal scope of this provision is equally limited, inasmuch as a consumer and a trader must be involved.[40]

Lastly, German law imposes different conditions

(Nomos 2015), Volume 4, p 193-224; MP García Rubio and M Otero Crespo, 'Country report for Spain' available on the BIICL website; BIICL (n 19), p 905-939; European Parliament (n 19), p 237-247.

31 For example, Article 53 of the Spanish Consumer Law explicitly states that an action for compensation can be coupled with an action whereby the representative entity seeks injunctive relief.

32 Note that the German law implementing the GDPR (*Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680*) does not make any reference to Article 80 GDPR.

33 *Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen, UKlag*. For an overview on the functioning of this procedural mechanism in English, see B Schneider, 'Class and Group Actions 2019 – Germany', available on the International Comparative Legal Guides; BIICL (n 19), p 599-600; E Lein, 'Country report for Germany', available on the BIICL website; A Stadler, 'National report Germany', Empirical Evidence on Collective Redress Conference, Wolfson College, Oxford University, 12-13 December 2016; European Parliament (n 19), p 168-179. Recently, a new Law that aims at introducing test case procedure in civil procedural law has been adopted (*Gesetzes zur Einführung einer zivilprozessualen Musterfeststellungsklage*). Although its scope is supposed to be general, it is however limited to cases involving consumers. Additionally, said Law severely restricts standing to sue. It therefore suffers from similar limits than the *UKlag*.

34 Karg (n 2), para 20.

35 The Law Improving the Civil Enforcement of Consumer Protection Provisions of Data Protection Law (*Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*) entered into force on 24 February 2016.

36 A Halfmeier, 'Die neue Datenschutzverbandsklage' (2016) *Neue Juristische Wochenschrift*, p 1127.

37 Which means that actions for compensation of moral damages, typical in the data protection field, are excluded. See B Hess, 'Die EU-Datenschutzgrundverordnung und das europäische Prozessrecht' in *Festschrift für Reinhold Geimer zum 80. Geburtstag, Fairness, Equity, Justice* (CH Beck 2017), p 263.

38 H Köhler, '§ 2 Ansprüche bei verbraucherschutzgesetzwidrigen Praktiken', in H Köhler, J Bornkamm and J Feddersen (eds), *Gesetz gegen den unlauteren Wettbewerb – Preisangabenverordnung, Unterlassungsklagengesetz, Dienstleistungs-Informationspflichten-Verordnung* (36th ed, CH Beck 2018), para 29a.

39 G Spindler, 'Verbandsklagen und Datenschutz – das neue Verbandsklagerecht Neuregelungen und Probleme' (2016) 3 *Zeitschrift für Datenschutz*, p 116.

40 Halfmeier (n 36), p 1127.

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

regarding standing to sue, which are not aligned with the GDPR. Section 4 *UKlag* enables different actors to protect consumers' interests, namely Chambers of Commerce/Industry, associations representing businesses and representative consumer associations. German law imposes strict conditions on the latter category. In particular, they must possess at least three associations active in the field or have at least 75 natural persons as members; have at least one year of existence; and statutorily defend consumer interests through non-professional education and counselling. Moreover, on the basis of its previous activity, it must appear that the consumer association will continue to fulfil its statutory duties in the long term in an effective and appropriate manner. As highlighted earlier, Article 80 GDPR does not impose conditions regarding size, years of existence or activities.

E-Austria

Section 28 of the Austrian Law on Data Protection[41] provides data subjects the right to mandate a not-for-profit body, organisation or association, which has been properly constituted, has statutory objectives that are in the public interest and is active in the field of data protection to lodge a complaint with the Data Protection Authority on their behalf (sections 24 to 26 of the Law on Data Protection) and to lodge a complaint with the Federal administrative Court (section 27 of the Law on Data Protection). However, representative entities shall not exercise the right to compensation and liability on behalf of data subjects (section 28 of the Law on Data Protection).[42]

The Austrian Law on Data Protection does not specify which procedural tool is available to representative entities, nor does it mention the representative entities' right to initiate judicial proceedings against a controller or a processor on behalf of data subjects pursuant to Article 79 GDPR. In the latter case, a default procedural mechanism that enables representative entities to seek judicial remedies may come into play. Specifically, under the collective redress action of Austrian type (*Österreichisches Modell der Sammelklage*),[43] individuals and associations can bring actions for injunctive relief and damages if this right was previously assigned to them. However, the scope of such procedural tool goes beyond the wording of section 28 of the Austrian Law on Data Protection according to which only representative entities can sue and no damages can be sought.

F-The United Kingdom

According to section 187(1) of the Data Protection Act 2018, data subjects may authorise a body or other organisation that meets the conditions set out in Article 80 GDPR to exercise the right to lodge complaints and to an effective judicial remedy (Articles 77, 78 and 79 GDPR) on their behalf. Data subjects may also authorise such a body or organisation to exercise the right to compensation (Article 82 GDPR). However, the right to bring actions without previous mandate is not available.

Yet the existing procedural tools in the UK do not permit the effective representation of data subjects in the meaning of section 187(1) of the Data Protection Act 2018. For example, although the Group Litigation Order[44] promotes the centralisation of individual claims, it does not allocate standing to representative entities. Under the Civil Procedure Rule (CPR) 19.6, a member of a 'class' of victims may sue on behalf of the whole group. This provision requires the representative claimant to have a direct cause of action. Representative entities of Article 80 GDPR will usually not fulfil that condition and hence, will rarely be able to use that procedural tool. Lastly, the representative action,[45] whereby a qualified entity has the power to apply to the courts for an enforcement order against traders, only applies where consumer protection laws have been infringed.[46] Moreover, it only provides for injunctive relief.

G-Dealing with National Adaptation Issues

Significant differences in approach are identifiable from the comparative law analysis above: first, some Member States have adopted procedural tools that offer more advantages than the GDPR. For example, the Spanish collective action allows representative entities to bring actions for compensation without previous mandate. The same is true in France and

41 *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.*

42 As G Leissler, P Reisinger and J Böszörmenyi explain in the Austrian national report (p 6), this legislative choice has been highly criticised.

43 Sections 227 and 502(5)(3) of the Austrian Code of Civil Procedure. For an overview on the functioning of this procedural mechanism in English, see H Bielesz and P Krepil, 'Class and Group Actions 2019 – Austria', available on the International Comparative Legal Guides; GE Kodek, 'Country report for Austria', available on the BIICL website; European Parliament (n 19), p 119-132; BIICL (n 19), p 376-385.

44 See Civil Procedure Rules 19.10 to 19.15. The GLO is a test case procedure as explained at n 5.

45 Part 8 of the Enterprise Act of 2002, as amended by the Consumer Rights Act of 2015.

46 Those laws are listed in Schedule 13 of the Enterprise Act 2002 and data protection is not encompassed.

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

Belgium. Additionally, Spanish law grants standing to sue to a broader range of actors under national law, since Article 11 of the Spanish Procedural Act enables a group of individual victims to start proceedings. One might wonder whether the GDPR admits the application of these differing, broader national provisions.

Second, many Member States have imposed more stringent conditions regarding standing to sue and scope of application. For example, the German Law on Actions for Injunctive Relief only allows actions in a number of cases and it is not even clear whether collective interests are encompassed at all within the material scope of that Law. Additionally, data subjects are only protected when they qualify as consumers. This limitation exists in Belgium and Spain as well. Are those additional restrictions valid in light of Article 80 GDPR?

The situation is even more complex in Member States where no procedural tool seems to adequately ensure the enforcement of data subjects' rights under the conditions imposed by Article 80 GDPR. Notably, section 187(1) of the UK Data Protection Act 2018 allows representative entities to bring actions for compensation in case the data subject(s) give(s) them a previous mandate. However, the current UK procedural law struggles to offer a corresponding appropriate tool.

There are two interpretations possible in order to tackle the misalignment between national and European laws. On the one hand, since the GDPR has been enacted under the form of a Regulation, one must admit that not much margin is left to national legislators, except where open clauses have been drafted.[47] As far as Article 80 GDPR is concerned, only the right to compensation in paragraph (1) and the entirety of paragraph (2) are open to adaptation. Following this reasoning, national rules that depart from the rest of this provision do not represent an appropriate adaptation of the GDPR.

On the other hand, one might argue that allowing the application of more advantageous national rules would strengthen private enforcement, which is at the heart of Article 80 GDPR.[48] Yet, this interpretation might be problematic as Article 80 GDPR seems to impose both minimum standards and limitations that Member States are not able to amend. For instance, the allocation of standing to sue to a broader range of actors under national law does not comply with the requirements of Article 80 GDPR, although this would foster private enforcement, because the very nature of such criteria is to guarantee the representative nature of a given entity. Similarly, it is unlikely that Member States can impose more stringent criteria on standing, since the Regulation creates a right for entities complying with the minimum requirements of Article 80 GDPR to bring representative actions.

As for Article 80(2) GDPR, it limits the possibility for entities to bring actions for compensation, in which is in all likelihood, an attempt to avoid abusive litigation and conflicts of interests. As a result, it is not possible for Member States to adopt more advantageous procedural terms. One might wonder whether such policy choice is fortunate as some Member States have already enacted provisions allowing the exercise of the right to compensation without a mandate, with the aim of enhancing private enforcement. Additionally, to the best of my knowledge, no abusive litigation has been observed where those mechanisms have been adopted.

Following this interpretation, how must differences between Article 80 GDPR and national laws be treated? Assuming that Article 80(1) GDPR has direct effect, more stringent national requirements, such as the ones regarding standing to sue, can be disregarded by a judge in horizontal conflicts following the principles of direct effect and supremacy of EU law (judicial discretion).[49] The same reasoning applies to the Spanish and Austrian collective actions, which offer broader advantages than Article 80 GDPR. If those instruments are used in the data protection field, an adjustment of procedure will be required. If this is not possible through judicial discretion, a new procedural tool will have to be created. The absence of adequate procedural instrument allowing the representation of data subjects –such as in the UK– is a trickier question. Only a legislative measure seems to be possible in order to reconcile substantive and procedural laws.

IV-ARTICLE 80 GDPR IN PRACTICE

Even though the present chapter focuses on the private enforcement of collective interests, it has to be highlighted that some significant complaints were

47 Wagner and Benecke (n 17) seem to favour such approach.
48 For example, De Waele thinks that if the national law goes further than the Regulation, but does not clash with it, it should be applied. Conversely, where national law imposes more stringent conditions, which clash with the Regulation, they should be discarded. See H De Waele, 'Implications of replacing the Data Protection Directive with a Regulation - a legal perspective' (2012) 12(4) *Privacy & Data Protection*, p 3-5.

49 PP Craig and G De Búrca, *EU Law - text, cases, and materials* (6th ed, Oxford University Press 2015), p 198-199; D Wyatt and A Dashwood, *Wyatt and Dashwood's European Union law* (6th ed, Hart 2011), p 248-252, 256-258, 270-278.

THE NATIONAL ADAPTATION OF ARTICLE 80 GDPR by, *Dr. Alexia Pato*

lodged as soon as the GDPR entered into force.[50] For example, in France, *Quadrature du Net* lodged several complaints with the French supervisory authority against GAFAM –the acronym for Google, Apple, Facebook, Amazon and Microsoft– on behalf of data subjects.[51] The association argues that said companies do not comply with their obligation to obtain the free consent of data subjects in order to process their personal data. In the documents available on its website, *Quadrature du Net* explicitly relies on Article 80 GDPR in order to represent victims.[52] This case underlines the important role of public enforcement in the data protection field.

Some judicial actions have popped up as well. Unfortunately, no comprehensive list of cases can be drafted in absence of any centralised register. Therefore, the remainder of this section discusses a selection of case examples related to the use of Article 80 GDPR.

Last November, Internet Society France –a French NGO– announced that it would bring a group action against Facebook.[53] The organisation listed seven infringements of the GDPR that the American company allegedly committed. Accordingly, Facebook will have to answer the NGO's complaint within four months. Otherwise, Internet Society France will start proceedings in the first instance court of Paris. The damages sought amount to EUR 1.000 per victim. Even though section 3 of this chapter concluded that a group action seeking compensation is not admissible without mandate, this has not deterred Internet Society France from bringing representative action. It remains to be seen whether this practice will be maintained in the future.

In Austria, NOYB –an organisation based in Vienna– represents the customer of a bank in the Austrian Federal Administrative Court on the basis of section 28 of the Law on Data Protection.[54] In short, the customer was denied free access to information regarding his/her bank account. The bank is arguing that, according to regulations of the banking sector, an additional fee may be charged to the customer in that case, and that banking sector rules override provisions in the GDPR.

In the UK, a group of victims –called Google You Owe Us (GYOU)– started a representative action (CPR 19.6) against Google in 2017,[55] i.e. before the entry into force of Article 80 GDPR and the Data Protection Act 2018. The group claimed that Google overrode privacy settings –thanks to a complex mechanism called the Safari Workaround– and unlawfully collected data of more than four millions of iPhone users between 2011 and 2012. GYOU sought GBP 750 per victim. The High Court of Justice rejected the claim on the ground that there was no evidence of loss and damage caused by Google[56] and that the victims did not have the same interests within the meaning of CPR 19.6(1).[57] The group of victims lodged an appeal against this decision in the Court of Appeal on 4 December 2018. In this chapter, it is argued that CPR 19.6 falls outside the scope of Article 80 GDPR. Therefore, it is unclear whether redress of future data protection violations will be possible through this procedural mechanism. In all cases, *Lloyd v Google* shows that many procedural barriers, such as the proof that a damage was caused and that the group of claims pose common questions of fact and law, have to be overcome in order for data subjects to obtain redress.

V-CONCLUDING REMARKS

This chapter has examined how Article 80 GDPR was incorporated into the law of some EU Member States. It concludes that Article 80 GDPR has often not been satisfactorily implemented by national legislators, who have enacted domestic provisions which often differ from the wording of the EU norm. However, given that the GDPR is a Regulation –and not a Directive–, this chapter contends that the adoption of differing requirements is not permissible where no open clause explicitly allows it. Accordingly, those national differences must be discarded following the principles of direct effect and supremacy of EU law. Alternatively, legislative amendments will be needed. In practice, Article 80 GDPR has allowed the representation of data subjects in several cases since the entry into force of the GDPR. However, the use of representative actions does not always respect Article 80 GDPR and it remains to be seen how the tension between theory and practice will be solved.

50 Overall, the entry into force of the GDPR has generated a significant rise in complaints in Europe. See A Hern, 'European regulators report sharp rise in complaints after GDPR' (26 June 2018) *The Guardian*.
51 S Mermilliod, 'L'association La Quadrature du Net lance une action de groupe contre les Gafam' (18 April 2018) *L'Obs*; J Deborde, 'Quadrature du Net : vers un recours inédit en matière de protection des données personnelles' (19 April 2018) *LeMonde.fr*.
52 All documents are available here.
53 M Untersinger, 'Données personnelles : action de groupe contre Facebook en France' (9 November 2018) *LeMonde.fr*; 'Une ONG lance une action de groupe contre Facebook' (9 November 2018) *LeFigaro.fr*.
54 A short summary of that case is available here.
55 *Lloyd v Google* [2018] EWHC 2599 (QB), available here.
56 Ibid, paras 54-81.
57 Ibid, paras 82-105.

SUMMARY TABLE

	Has Art. 80 GDPR been incorporated into national law?	Which procedural tool ensures the collective enforcement of data subjects' rights?	Are actions for compensation available (Art. Article 80(1) GDPR)?	Are actions without previous mandate available (Art. 80(2) GDPR)?	Sources of misalignment between Article 80 GDPR and national laws
FRANCE	Yes, see Article 43(ter) of the Law on Information Technology, Data Files and Civil Liberty.	The group action (action de groupe).	Yes.	Art. 80(2) GDPR has not been implemented into French law. However, the group action allows representative entities to sue without previous mandate.	National conditions on standing to sue are more restrictive than Art. 80 GDPR; Actions for compensation without previous mandate are allowed, contrary to the wording of Art. 80(2) GDPR.
BELGIUM	Yes, see Article 220 of the Law on the Protection of Individuals Regarding the Processing of their Personal Data.	The default procedural regime applies. According to Art. XVII.37(10°/1) of the Economic Code, the collective action (action en réparation collective) is available in case of data protection violations.	Yes.	Art. 80(2) GDPR has not been implemented into Belgian law. However, the collective action allows representative entities to sue without previous mandate.	National conditions on standing to sue are more restrictive than Art. 80 GDPR; Actions for compensation without previous mandate are allowed, contrary to the wording of Art. 80(2) GDPR; The collective action is limited to monetary relief and only protects consumers.
SPAIN	No.	The default procedural regime applies, ie the collective action (acción colectiva) of the Spanish Procedural Law.	Yes.	Art. 80(2) GDPR has not been implemented into Spanish law. However, the collective action allows representative entities to sue without previous mandate.	National law allocates standing to sue to a broader range of actors than Art. 80 GDPR; The personal scope of the collective action is limited to consumers.
GERMANY	No.	The default procedural regime applies, ie the action for injunctive relief (UKlag). The recently adopted test case procedure (Musterfeststellungsklage) is available too but suffers from similar criticism than the UKlag.	No.	No.	Conditions on standing to sue are more restrictive than Art. 80 GDPR; The personal scope of the action is limited to consumers and it is doubtful that collective interests are protected by the norm; The material scope only allows actions in limited cases.
AUSTRIA	Yes, see section 28 of the Law on Data Protection.	The default procedural regime applies, ie the collective redress action of Austrian type (Österreichisches Modell der Sammelklage).	No.	No.	National law allocates standing to sue to a broader range of actors than Art. 80 GDPR; The collective redress action of Austrian type allows actions for damages in opposition to section 28 of the Law on Data Protection.
THE UK	Yes, see section 187(1) of the Data Protection Act 2018.	The default procedural regime applies, but no procedural instrument seems to adequately ensure the enforcement of data subjects' rights in light of section 187.	Yes.	No.	No procedural instrument seems to adequately ensure the enforcement of data subjects' rights in light of section 187.

Part 2: Illustrations of the international influence of the GDPR

UK: GDPR ADAPTIONS AND PREPARATIONS FOR WITHDRAWAL FROM THE EU

By Dr. Karen Mc Cullagh
Lecturer in Law, University of East Anglia. For correspondence: k.mccullagh@uea.ac.uk

I-INTRODUCTION

Part I of this chapter traces the evolution of UK data protection legislation, outlines the UK government's rationale for enacting the Data Protection Act 2018 (DPA 2018) to supplement the GDPR even though the UK is on course to leave the European Union (EU), and comments on the most interesting derogations, exemptions, and adaptations to the GDPR in the DPA 2018 – some of which are controversial, and could prove problematic in the future.

Part II sets out the data protection implications of the UK leaving the EU with transitional withdrawal arrangements in place or on a 'no deal' basis. It outlines why the UK may struggle to obtain a finding of adequacy from the European Commission, and how the Information Commissioner's Office (ICO) will suffer a loss of status and influence when the UK becomes a 'third' country for data protection purposes. It concludes that departure from the EU will not result in significant UK divergence from the GDPR.

II-RATIONALE FOR ENACTING THE DATA PROTECTION ACT 2018

On 23 June 2016 a majority of eligible voters in the UK voted to 'Leave' the European Union (EU), and the UK is on course to leave on 29 March 2019.[1] However, as the General Data Protection Regulation (GDPR) was scheduled to be directly applicable in all member states beforehand i.e. from 25 May 2018, the UK Government decided to legislate to implement derogations, exemptions and adaptations in the GDPR into national law during the pre-withdrawal period.[2] Accordingly, a data protection bill was introduced in the House of Lords on 13 September 2017 where opposition parties broadly welcomed it, and after much debate and some revision, it received royal assent on 23 May 2018. The Data Protection Act 2018 (hereafter the DPA 2018) is the third generation of data protection legislation in the UK. It repealed and replaced provisions in the Data Protection Act 1998 that transposed the Data Protection Directive 95/46/EC into UK law.[3] The DPA 1998 had in turn replaced the Data Act 1984 which incorporated eight data protection principles in the Council of Europe Convention for the Processing of Personal data (hereafter referred to as Convention 108).

A-Scope & Structure of the Data Protection Act 2018

The DPA 2018 regulates the processing of individuals' personal data by private and public bodies, law enforcement entities, and intelligence service agencies. It does so by providing rules concerning general data processing, law enforcement data processing, data processing by the intelligence services, and regulatory oversight and enforcement by the national supervisory authority - the Information Commissioner's Office (ICO).

The DPA 2018, subject to minor exceptions, extends and applies to the whole of the UK.[4] This complex and lengthy (339 pages) Act is set out in seven parts: **Part 1** explains the structure of the Act and contains some general definitions; **Part 2** has three chapters, the first of which contains definitions and general material. Chapter 2 (which must be read alongside the GDPR and is known as 'the applied GDPR') sets out national derogations and exemptions to from the GDPR, such as the definition of public authority and public interest, the age of consent for children using information society services, a system for authorising certification providers, and safeguards for processing for archiving, research and statistical purposes. The derogations will be discussed in more detail below. Chapter 3 applies a broadly equivalent regime to

1 Unless a later withdrawal date is agreed during negotiations.
2 Data Protection Bill [HL] 2017-19, <https://services.parliament.uk/bills/2017-19/dataprotection.html>

3 See Data Protection Act 2018 c. 12 Sch.19 (1) para.44. Some provisions in the DPA 1998 were retained on a transitional basis.
4 Data protection is not a devolved matter in Scotland, Wales, or Northern Ireland.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

certain types of processing to which the GDPR does not apply including the processing of unstructured manual files by public authorities but excluding law enforcement and intelligence agency (e.g. GCHQ) processing; **Part 3** is divided into six Chapters. This part transposes the Law Enforcement Directive (LED) into UK law. It applies to all processing for law enforcement purposes by a defined list of "competent authorities" listed in Schedule 7 that includes organisations such as Government departments, Fraud Office, Police, Probation, Youth Offending Teams etc.; **Part 4** provides a code of personal data processing for the intelligence agencies in six chapters. It draws from the modernised Convention 108. The rules in this Part contain predictably wide exemptions for national security processing; **Part 5** contains provisions to continue the existence of the role of the ICO and its functions; **Part 6** deals with enforcement of the data protection legislation i.e. the ICO's powers to issue enforcement notices and penalties.

Part 7 of the Act contains miscellaneous provisions such as order-making powers. A considerable number of the exceptions to the GDPR e.g. for research, education, health data, and social work data are dealt with in the 22 Schedules of the Act.

Most provisions in the DPA 2018 came into force on 25 May 2018 to coordinate with the GDPR becoming directly applicable in EU member states.[5]

B-General Observations

The DPA 2018 is highly 'conservative' departing in approach and terminology from the previous Act as little as possible. This is understandable in light of the short timescale available for legislative debate before the GDPR came into effect and the LED had be transposed and the need to be mindful of 'adequacy' requirements as part of the Brexit process (discussed in Part II).

C-Uncontentious Aspects

Part 2, Chapter 2 (and Schedules 1-3) of the DPA 2018 sets out derogations permitted in the opening clauses of the GDPR. The UK Government has used these derogations to ensure close alignment with the approach adopted under the previous data protection act or other existing laws. A few of the more notable derogations and powers are set out below:

1) Public authority & public task: definitions and exemptions

The GDPR contains numerous references to public authorities e.g. when stipulating, in Art 37, that such bodies need to appoint a Data Protection Officer, and when stipulating in Art 6(1)(f) that public authorities processing personal data in the performance of their public tasks cannot rely on 'legitimate interests' as the lawful basis for processing. As the terms 'public authority' and 'public body' are not defined in the GDPR, the DPA 2018 adopts in section 7 the definitions in the Freedom of Information Act 2000 and its Scottish equivalent, the Freedom of Information (Scotland) Act 2002, as well as bodies specified by the Secretary of State, subject to two qualifications. First, public authorities are only to be treated as public authorities for the purposes of the GDPR when they are carrying out a task in the public interest or in the exercise of official authority vested in it. Second, parish councils, community councils, and similar bodies are specifically excluded in section 7(3) from the definition. The government's rationale for exempting these bodies is that they are very small in terms of personnel, budget, and the volume of personal data they process such that the additional safeguards that public authorities normally have to apply would represent a disproportionate burden.[6] Consequently, parish councils and other exempt bodies do not need to appoint a data protection officer and can rely on legitimate interests as their lawful basis for processing personal data.

2) Continued registration with and payment of fees to the ICO

The GDPR advises member states to 'abolish indiscriminate general notification obligations' and replace them with effective procedures and mechanisms that focus on processing operations 'likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes.'[7] The UK government has interpreted this as permitting it to retain an obligation to register (also known as notification) and pay an annual fee to the ICO based on the risks posed by controllers processing personal data. The Data Protection

5 Some provisions commenced on 23rd July 2018 by virtue of s 212 of the Data Protection Act 2018 and the Data Protection Act 2018 (Commencement No1 and Transitional and Savings Provisions) Regulations 2018 (SI 2018, No. 625).

6 Data Protection Act 2018, Explanatory Notes, <http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf>, para 23.
7 Recital 89.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

(Charges and Information) Regulations 2018 three-tier fee system of £40, £60, or £2900 per annum is levied depending on staff numbers and annual turnover, or whether the controller is a public authority, a charity or a small occupational pension scheme, unless it can avail of an exemption.[8] Controllers are exempt from the notification and fee requirements if they only process personal data for one (or more) of the following purposes: staff administration; advertising, marketing and public relations; accounts and records; not-for-profit purposes; personal, family or household affairs; maintaining a public register; judicial functions; and/or processing personal information without an automated system such as a computer.[9] The Government undertook a public consultation on whether these exemptions remained appropriate and fit for purpose. After detailed analysis of consultation responses the Government decided not to change any of the current exemptions and further decided to introduce a new exemption from payment of the data protection charge for: all processing relating solely to standing for or fulfilling the office of all categories of elected representatives[10] and members of the House of Lords.[11]

Failure to pay exposes a controller (who does not benefit from an exemption) to the risk of a civil monetary penalty, levied by the ICO, of up to £4,350.[12] A "notice of intent" must first be served by the ICO on a controller that is believed not to have paid the requisite fee.[13] Significantly, it appears that the ICO now effectively has an automatic notice of intent procedure in place: We will email you before your previous payment expires and your new payment is due.[14] The ICO was quick to exercise its enforcement powers, issuing its first notices of intent to issue monetary penalty notices to 34 controllers for failure to pay the notification fee in September 2018.[15] Evidently, the ICO will readily issue penalties to those who, despite reminders, negligently or wilfully fail to pay the annual notification fee.

3) Stronger ICO investigatory & enforcement powers

The Facebook-Cambridge Analytica data scandal, which involved the collection by Cambridge Analytica via the 'thisisyourdigitallife' app of the personal data of millions of Facebook users in an attempt to influence voter opinions,[16] confirmed that the ICO's powers under the DPA 1998 to investigate were inadequate. It required data controllers to be given seven days of notice in writing of an intended search, and for them to be given an opportunity to argue in court against the granting of a search warrant. Such delay could weaken the ICO's ability to collect relevant evidence in a timely manner, and give an errant data controller the opportunity to destroy incriminating evidence.

On a positive note, the DPA 2018 has enhanced the powers of the ICO through the introduction of an obligation for data controllers to respond to urgent information requests from the ICO within 24 hours,[17] and by empowering the ICO to obtain a court order to require disclosure when a data controller refuses to respond to such requests,[18] as well as the introduction of an offence for destroying, falsifying or concealing information.[19] The ICO quickly utilised its new enforcement powers when it served (on 6 July 2018) an Enforcement Notice on AggregateIQ Data Services Ltd (AIQ) requiring it to 'cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes.'[20] However, the ICO later served

8 The Data Protection (Charges and Information) Regulations 2018 were made under powers sections 137 and 138 of the DPA 2018. The DPA 2018 provisions replaced similar powers under ss. 108-110 of the Digital Economy Act 2017. Regulation 3 sets the level of fee. Specific provision is made for charities and small occupational pension schemes and the charge is reduced if a data controller pays the charge by direct debit.

9 Regulation 2.

10 As defined in paragraph 23(3) of Schedule 1 to the DPA 2018

11 DCMS, Review of exemptions from paying charges to the Information Commissioner's Office: Government response to the public consultation, November 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/754690/Government_response_to_the_ICO_Charge_Exemption_Consultation_L.pdf> 5.

12 A sum which the ICO is required to set in statutory guidance, issued under section 158 of the DPA 2018. <https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf>, p.14. (£4350 represents 150% of the top tier fee).

13 Schedule 16, paragraph 2.

14 ICO, The General Data Protection Regulation: The data protection fee: A guide for controllers, February 2018, <https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf> 15.

15 ICO, ICO takes action for failure to pay new data protection fee, 26th September 2018, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-takes-action-for-failure-to-pay-new-data-protection-fee/>

16 C. Cadwalladr and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (*The Guardian*, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

17 Section 142.

18 Section 145.

19 Section 148.

20 Section 149 <https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf>.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

a variation to the notice (under section 153(1) of the DPA 2018), which requires AIQ to: '*Erase any personal data of individuals in the UK, determined by reference to the domain name of the email addresses processed by AIQ, retained by AIQ on its servers as notified to the Information Commissioner by Borden Ladner Gervais LLP in letters of 10 and 31 May 2018.*'[21] AIQ is obliged to comply with this enforcement notice within 30 days once notified by the Office of the Information and Privacy Commissioner of British Columbia (OIPC) that it is no longer the subject of any investigation by the ICO (or informed by the OIPC to comply with the Notice). It is not known whether the variation was served as a result of representations by AIQ who had appealed the notice on the basis that the terms were overly broad and imprecise but it has been reported that that the appeal has been withdrawn following the issuance of the variation.[22] This complex investigation provides evidence of the ICO using all powers available to it to investigate and prosecute when appropriate.[23]

Also, whilst the maximum fine that the ICO can impose has been increased from £500,000 to €20m or 4% of worldwide annual turnover (with the penalty in sterling to be determined by applying the spot exchange rate set by the Bank of England on the date on which the penalty notice is issued,[24] it is important to note that the ICO views itself as a 'proportionate regulator' and has sought to reassure data controllers that maximum penalties will only be issued in respect of the most serious breaches. Nevertheless, the ICO has repeatedly stated that it has the power to prohibit data controllers and data processors from processing personal data, and will not hesitate to use those powers if the circumstances warrant it. In effect, it has issued a warning to 'big players' that a potential fine should not be viewed an 'affordable business cost.' Rather, the ICO's power to order controllers cease personal data processing activities should give them pause for thought and be an effective compliance 'stick' in situations where one is needed, particularly when it could be regarded as a failure to meet corporate governance requirements or trigger a report to a stock exchange, thereby impacting share valuation.

4) Profiling and automated decision making

To the extent that controllers are permitted to make automated decisions based on profiling under Article 22 of the GDPR, the following safeguards must apply: the controller must notify the data subject, as soon as reasonably practicable that there has been a decision based solely on automated processing; the data subject has within one month from receipt of the notification to request the controller to either reconsider the decision or to not base it solely on automated processing; and from receipt of such a request, the controller must within one month, comply with the request and notify the data subject in writing of the steps taken to comply with the request and the outcome of complying.[25]

D-Contentious aspects

Not all provisions in the DPA 2018 have been welcomed; several were the subject of criticism during the legislative process and continue to be considered controversial for the reasons set out below

1) A declaratory section on personal data

Concerns were raised at the Second Reading and Committee stages that the UK government's refusal to retain the EU Charter of Fundamental Rights (specifically the Article 8 right to the protection or personal data) in UK law after withdrawal from the EU would jeopardise an adequacy decision from the European Commission after Brexit. For instance, Lord Stevenson of Balmacara said:

> "One of the key principles which underpinned earlier data protection legislation is Article 8 of the EU Charter of Fundamental Rights. It is indeed the basis of much of what is in the GDPR and applies to the whole of the EU, but when we try to find references in the Bill to the right to privacy and to the protection of personal data which Article 8 guarantees, they are not mentioned explicitly…It is the removal of the references to Article 8 that will provide a significant and totally unnecessary risk when the time comes for the EU to assess whether our regime is essentially equivalent to the rest of the EU, because that will be the test."[26]

21 ICO, Enforcement Notice, The Data Protection Act 2018, Part 6, Section 149, Annex 1, (24th October 2018), <https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf>
22 T Webb, ICO narrows first-ever GDPR enforcement notice, *Global Data Review*, (30th October 2018) <https://globaldatareview.com/article/1176139/ico-narrows-first-ever-gdpr-enforcement-notice>.
23 ICO, Investigation into the use of data analytics in political campaigns, A report to Parliament, 6 November 2018, <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>
24 Section 157 (7).
25 Section 14.
26 Public Bill Committee 30 October 2017 cc1162-3

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

In an effort to allay these concerns the Government published a memorandum setting out how each article of the Charter derives from a wide variety of sources, including the Treaties, EU legislation, the ECHR and case law from both courts.[27] The government contended that as the 'substantive rights, of which the charter is a reflection not the source, will already be protected in domestic law by the European Union (Withdrawal) Bill, it is not necessary to retain the charter in order to protect such substantive rights.'[28] On that basis, when introducing the Government amendment at Report stage, Lord Ashton of Hyde said that a declaratory section would be added. It would not confer new rights; rather the intention was to provide reassurance:

> The Government's Amendment ... should provide reassurance ... that the UK has not just implemented EU law to the extent necessary but has gone further in legislating for a complete and total legal framework that covers all personal data processing across every sector of our economy.[29]

The declaratory section on personal data in section 2 (1) states that the GDPR, applied GDPR, and DPA 2018 'protect individuals by *requiring personal data to be processed lawfully and fairly on the basis of consent or other specified basis, conferring a right of access and rectification to data, and giving the ICO responsibility for enforcing the law*' (emphasis added). The wording mirrors the text of Art 8 of the EU Charter. The government is of the view that this will satisfy the European Commission (EC) of the UK's commitment to providing equivalent data protection rights once the UK leaves the EU and the EU Charter ceases to be part of the UK's legal framework. Doubts remain whether the declaratory section will suffice when the UK seeks an adequacy decision.[30]

2) Child's consent in relation to information society services

The Government's proposal to set the age at which a child could consent to the processing of their personal data by an Information Society Service (ISS) at 13 was controversial - the Bill's explanatory note stated that this was in line with the minimum age set by Facebook, Whatsapp and Instagram - as some members of parliament were of the view that it implied the government was more mindful of the concerns of ISSs than children. It was criticized during the second reading[31] and committee stages[32] in the House of Lords. Objections included survey data indicating that 81% of parents thought the age should be set at either 16 or 18.[33] Relatedly, concerns were expressed that variations in capacity to consent were not considered (children mature at different rates): "Although there are arguments for setting the age limit higher—or indeed lower—there is surely a need both for proper evidence to be gathered and for a minimum requirement for companies to have robust age verification systems and other safeguards in place before any such legislation is passed."[34] However, as it would not be practical or feasible to require a court or independent regulator to assess a child's capacity each time a child subscribed to an ISS, the government persisted with its proposal of setting a threshold age of consent below which parental consent would be required. Section 9 sets the age at which a child can give consent to the processing of data for the purposes of the provision of ISSs at 13 years old in England & Wales and in Northern Ireland, and in Scotland the presumption that a person over 12 years of age or over is of sufficient age and maturity to understand and give consent is modified in relation to information society services so that the presumption applies to children aged 13.[35]

On a more positive note, the government heeded comments made by *inter alia* the Children's Society that 'if companies continue to rely on their current practices—whereby they allow only over-13s to have an account but have no age verification process to check that children who are consenting are the age they state themselves to be—then there will continue to be widespread breaches of both the companies' own rules and this new Data Protection Act.'[36] Consequently, at the Report stage the Government supported amendments in the form of a requirement for the ICO to produce a

27 Explanatory Notes to Data Protection Bill, Para 92. <https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/en/18153-EN.pdf>, pp. 25-26.
28 Charter of Fundamental Rights of the EU Right by Right Analysis, (5th December 2017), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/05122017_Charter_Analysis_FINAL_VERSION.pdf >
29 HL Deb 11 December 2017 c1379.
30 House of Commons: Home Affairs Committee, UK-EU security cooperation after Brexit, Fourth Report of Session 2017–19, HC 635, para 94. <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/635/635.pdf>
31 For example, Lord Stevenson of Balmacara at HL Deb 10 October 2017 cc130-1.
32 Public Bill Committee 30 October 2017 cc1264-70
33 House of Lords, Data Protection Bill, Second Reading, 10 October 2017, Volume 785, Column 139.
34 Ibid, Column 131.
35 Section 208.
36 Ibid.

code of practice on age-appropriate design of online services.[37] To this end, the ICO has exercised its powers to consult in respect of an Age Appropriate Design Code of Practice. The Code of Practice will provide guidance on the design standards that the ICO will expect providers of online services and apps used by children to meet when they process their data. Once it has been published, the Commissioner will be required to take account of any provisions of the Code she considers to be relevant when exercising her regulatory functions. Courts and tribunals will also be required to take account of any provisions in the Code that they consider to be relevant in proceedings brought before them. Although the focus on age verification and age appropriate design of ISSs is to be welcomed, it will pose a big practical challenge for ISSs as they will be obligated to set up parental consent systems when they are needed, and have means of demonstrating that they have implemented appropriate techniques to verify age, which is difficult when children are *au fait* with techniques for bypassing age verification mechanisms and obtaining parental consent.[38]

3) Journalism exemption

During the passage of the Bill, the Lords proposed a provision requiring the Secretary of State to establish a new inquiry into allegations of data protection breaches by news and other media organisations i.e. on commencing part 2 of the Leveson inquiry. Part 2 of the Leveson Inquiry had been intended to address '*the extent of unlawful or improper conduct within News International and other media organisations, and collusion between the police, press and politicians*.'[39] It was postponed in 2012, to avoid prejudicing the large-scale police investigations into phone hacking and corrupt payments, which were then ongoing, and the government had decided not to proceed with it in March 2018. However, this provision was not included in the DPA 2018. Instead, the Commons added a provision requiring the Secretary of State to review every three years the use of the section 179 alternative dispute resolution procedures in cases involving failures by a media organisation to comply with data protection legislation.[40] The ICO has also been granted powers and responsibility to encourage media compliance with data protection law, including periodic review and reporting on compliance,[41] an obligation to issue guidance to individuals on seeking redress against media organisations,[42] and creation of a code of practice for media organisations on data protection compliance.[43] In addition, the Secretary of State must report every three years on the effectiveness of the media dispute resolution procedures, including under the Editors' Code of Practice.[44]

Significantly, the journalism exemption available under the Data Protection Act 1998 has been reproduced and its scope widened, in order to comply with Art 85 of the GDPR. Under 32 of the Data Protection Act 1998, a data controller processing for two or more substantive purposes, including for journalism, was on the face of the legislation precluded from relying on the exemption. By contrast, Schedule 2, part 5, para 26(3) is wider as it stipulates that the disapplication of certain GDPR provisions for journalists will apply 'to the processing of personal data carried out for the special purposes, *whether or not the data are being processed for a second or ancillary purpose*.' In addition, sections 170 and 171 of the DPA 2018 add to the existing offence of unlawfully obtaining personal data a new offence of *re-identification of de-identified personal data. The DPA 2018 also introduces* explicit journalism public interest defences.[45] When forming a belief that publication is in the public interest, a data controller must have regard to relevant codes of practice, namely the BBC Editorial Guidelines, the Ofcom Broadcasting Code and the Editors' Code of Practice.[46]

4) Profiling by political parties

Despite the Facebook - Cambridge Analytica data scandal (a whistle-blower, ex employee revealed that it

37 HL Deb 11 December 2017 cc1426-42.
38 K Mc Cullagh, (2016) The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?, in *Data Protection, Privacy and European Regulation in the Digital Age*., Bräutigam, T. & Miettinen, S. (eds.), Forum Iuris, ISBN 978-951-51-2530-9.
39 Leveson Inquiry, Terms of Reference, Part 2, <http://webarchive.nationalarchives.gov.uk/20140122144942/http://www.levesoninquiry.org.uk/about/terms-of-reference/>
40 A significant amount of time was also spent debating bringing section 40 of the Crime and Courts Act 2013 into force. Section 40 of the Crime and Courts Act 2013 would have made news publishers who were not subject to a Government-approved regulator, liable for the costs of defamation, privacy, and harassment claims, regardless of whether they won or lost. The proposed amendments were ultimately defeated and s 40 of the 2013 Act will now be repealed at the earliest opportunity. Matt Hancock, Oral statement to Parliament: Leveson Consultation Response, (1st March 2018), https://www.gov.uk/government/speeches/leveson-consultation-response; It has not been repealed at as of 14th January 2019.
41 Section 178.
42 Section 177
43 Section 124.
44 Section 179.
45 Sections 170-171.
46 Schedule 2, part 5, para 26(5).

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

had illicitly harvested the personal data of millions of people's Facebook profiles without their consent and used it to profile individual US voters, in order to target them with personalised political advertisements),[47] the DPA 2018 contains a provision that permits political parties to process personal data 'revealing political opinions' (without the individual's consent), for the purposes of their political activities,[48] with "democratic engagement" listed as an example of processing activities that can be undertaken lawfully in the public interest.[49] Privacy International, a campaign group, have expressed dismay that 'There is nothing in the provision to prohibit delegation of such activities to a third party specialising in profiling.'[50] They are particularly concerned as 'modern technologies make it possible to infer political inclinations of people from a wide variety of sources of information.'[51] They contend that the provision is open to abuse and will facilitate targeted and exploitative political advertising.[52] It remains to be seen whether two recommendations by the ICO in the course of evidence to the Inquiry, namely (1) that inferred data should be as protected under the law as personal information, and (2) that a Cope of Practice which highlights the use of personal information in political campaigning be underpinned by primary legislation, are implemented by the government.[53]

5) Henry VIII clause – sensitive data

The Act gives wide powers to the Secretary of State in the form of Henry VIII clauses[54] to alter the application of GDPR, including conditions for processing sensitive personal data without a data subject's consent. The government has justified this approach (which bypasses effective parliamentary scrutiny) on the basis that it will provide necessary 'flexibility to manage unforeseeable circumstances (citing the decision by the Home Secretary to establish the Hillsborough Independent Panel to investigate the circumstances in which multiple fatalities occurred at a football stadium, as an example in which it was appropriate to use such powers).[55]

6) No Collective redress without authority mechanism

This issue of collective redress without authority was the subject of significant debate during the legislative process. Campaigners emphasised *inter alia* the difficulties of seeking a positive "opt-in" to proceedings from affected individuals, and highlighted that those affected by data breaches and other illegal data-related activities are often unaware of what has happened.[56] Controversially, unlike most other member states,[57] the UK government decided not (at this stage) to allow representative bodies to take independent action when they consider that there has been a failure to comply with the DPA 2018. There is some room for optimism, however, in relation to this provision though as the Government made a small concession in the form of an agreement to review this provision within 30 months of 25 May 2018.[58]

7) Immigration exemption

The Data Protection Act 2018 introduces an exemption based on Articles 6(3) and 23(1) of the GDPR which restricts the application of certain GDPR provisions to personal data processed for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control, to the extent that the application of those provisions would be likely to prejudice those purposes.[59] The exemption removes most of a data subject's rights, including notification and subject access rights,[60] right to erasure,[61] right to restrict processing,[62] right to object

47 House of Commons, Digital, Culture, Media and Sport Committee, Evidence from Christopher Wylie, Cambridge Analytica whistle-blower, 28 March 2018, <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-evidence-wylie-correspondence-17-19/>
48 Schedule 1, para 22.
49 Section 8 (e).
50 Privacy International, UK Data Protection Act 2018 – 339 pages still falls short on human rights protection, (13 June 2018), <https://privacyinternational.org/blog/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection>
51 Ibid.
52 Ibid.
53 House of Commons Digital, Culture, Media & Sport Committee, Disinformation and 'fake news': Final Report, Eighth Report of Session 2017-19, HC 1791, 18 February 2019, paras 48 and 216.
54 'Henry VIII clauses' are clauses in a bill that enable ministers to amend or repeal provisions in an Act of Parliament using secondary legislation, which is subject to varying (that is, lower) degrees of parliamentary scrutiny.
55 Data Protection Act 2018, Explanatory Notes, para 27.
56 House Of Commons Official Report General Committees, Public Bill Committee, Data Protection Bill [Lords], Third Sitting, Thursday 15 March 2018 (Morning), <https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/PBC153_Combined_1-8_22_03_2018_REV.pdf>
57 See the contribution by Alexia Pato on p.94
58 Ss. 187 & 189.
59 Data Protection Act 2018, Schedule 2, part 1, paragraph 4
60 Articles 13-15, GDPR.
61 Article 17(1) and (2), GDPR.
62 Article 21(1), GDPR.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

to processing;[63] and all the principles in Article 5 of the GDPR (which require that processing must be lawful, fair and transparent, accurate, adequate, for explicit and legitimate purposes, processed in a manner that is secure, and limited to the specific original processing purpose). Notably, the right to rectification,[64] the notification obligation regarding rectification, erasure or restriction,[65] and the data portability right,[66] are not exempt. A narrower set of exemptions applies where a new controller obtains the personal data from the original controller for the purpose of discharging statutory functions.[67] This exemption is most likely to be used by immigration and border authorities, for example, to withhold information from data subjects.

The exemption was introduced despite strong criticism from the ICO who observed that, "If the exemption is applied, individuals will not be able to access their personal data to identify any factual inaccuracies and it will mean that the system lacks transparency and is fundamentally unfair."[68] Similarly, the Deputy Counsel to the Joint Committee on Human Rights (JCHR) queried "why immigration control requires exemptions from fundamental principles such as lawfulness, fairness and accuracy in order to maintain its effectiveness", and further contended that "it is arguably disproportionate to extend such restrictions to immigration control, particularly so in relation to lawful immigration."[69]

Observers were surprised that the government did not withdraw or amend the exemption in response to these and other objections,[70] not least because the Government was already 'under fire' for the way it had 'mishandled' immigration data relating to the Windrush Generation (a term used to refer to individuals who moved from the West Indies to the UK between 1948 and 1971 at the express invitation of the UK Government who offered them indefinite leave to remain status for helping to rebuild the UK's economy post-WWII). The Home Office had disposed of their disembarkation records (known as 'landing cards') that were often a key piece of documentary evidence proving their right to remain. As there are clear parallels between the position of the Windrush Generation and EU citizens currently resident in the UK whose status may be questioned when the UK withdraws from the EU, the *Open Rights Group* and *the3million*, a campaign group representing EU citizens living in the UK, have instigated judicial review proceedings in the High Court on the basis that the exemption is incompatible with the GDPR as well as the European Convention on Human Rights.[71] The exemption also has a strong potential to negatively impact any post-Brexit finding of adequacy that that UK may seek from the EU Commission in respect of EU-UK personal data transfers.

8) Data Subject access to confidential references

Under the DPA 1998, confidential references given by a data controller for the purposes of education, training, employment, placement, appointment, provision of a service, or corresponding prospective opportunities of a data subject were exempt from the data subject access right.[72] However, the exemption did not apply to references received by a prospective employer so a data subject could make a subject access request to a prospective employer to access information written about them by a current or previous employer. In addition, the exemption did not exclude the fairness requirements of the first data protection principle so a prospective employee was able to find out that personal data containing an employment reference had been provided when an employer sought a reference from a referee unknown to the prospective employee. By contrast, the DPA 2018 extends the exemption to include confidential references received by a prospective employer.[73] It also gives an exemption from the right to be informed under Article 13 and 14 of GDPR i.e. the need to mention it in a privacy notice. This change was introduced without any debate, and has been criticised as potentially weakening the position of employees (whether paid or voluntary), no longer have any means of accessing confidential

63 Article 18(1), GDPR.
64 Article 16, GDPR.
65 Article 19, GDPR.
66 Article 20, GDPR.
67 Schedule 2, Part 1, paragraph 4(3) and (4).
68 ICO Briefing (2017), 'Data Protection Bill, House of Lords Report Stage –Information Commissioner's briefing – Annex II,' <https://ico.org.uk/media/about-the-ico/documents/2172865/dp-bill-lords-ico-briefing-report-stage-annex-ii-20171207.pdf>.
69 Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017, <https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf>.
70 Both the Law Society of England and Wales and the Bar Council warned that the immigration exemption clause in the Bill could give rise to serious miscarriages of justice, <https://www.lawsociety.org.uk/news/press-releases/home-office-not-to-be-trusted-with-data-protection-exemptions/>
71 Leigh Day, 'Campaign groups granted permission for judicial review of immigration exemption,' 17 January 2019, <https://www.leighday.co.uk/News/2019/January-2019/Campaign-groups-granted-permission-for-judicial-re>
72 Schedule 7, paragraph 1.
73 Schedule 2, paragraph 24.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

references.

III-THE DATA PROTECTION IMPLICATIONS OF BREXIT

The GDPR was also introduced against the backdrop of the UK's decision to leave the EU. The UK is on course to become a 'third country' for data protection purposes. Accordingly, this section sets out the data protection implications of the UK leaving the EU with transitional withdrawal arrangements in place or on a 'no deal' basis, and further explains why the UK may struggle to obtain a finding of adequacy from the European Commission.

A- Leaving the EU but retaining the GDPR

The UK Government intends to incorporate the GDPR into domestic law when it ceases to be a member of the EU despite not being legally obliged to do so when it becomes a third country. The motivation for doing so is the economic value of EEA-UK personal data transfers. The UK economy is largely service based (service industries account for approximately 78% of the UK's Gross Domestic Product (GDP), and personal data processing underpins these service industries. [74] The EU is forecast to remain the UK's largest trading partner for many years after Brexit, so frictionless transfer of personal data will be imperative to ensure continued economic growth in the UK after Brexit. As the GDPR has extra-territorial application it would continue to apply to UK established data controllers and processors when processing personal data relating to the offering of goods or services to individuals in the EEA, or when monitoring the behaviour of individuals in the EEA countries, for example, through cookies after the UK leaves the EU.[75] Relatedly, as the European Commission will not make an adequacy decision to facilitate EEA-UK personal data transfers unless the UK satisfies the EU that UK law provides an 'essentially equivalent' level of protection to the GDPR, the easiest way to ensure compliance is to retain the GDPR in UK law when the UK leaves the EU. In essence, "We are leaving the EU and businesses need a single standard under which they can operate"[76] so that data flows "*remain uninterrupted after the UK's exit from the EU [and EEA]*".[77]

74 ONS, Statistical Bulletin: Index of Services, April 2016.
75 Art 3 GDPR.
76 DCMS, A New Data Protection Bill: Our Planned Reforms, A Statement of Intent, (7 August 2017), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf> 14.
77 Ibid, 24.

B- Potential transitional arrangements

After the UK served notice of its intention to withdraw from the EU,[78] the UK and EU negotiated the terms of a Withdrawal agreement[79] and Political Declaration.[80] The Withdrawal Agreement sets out arrangements for the UK's withdrawal from the EU on 29 March 2019 and includes a transition period (which the UK refers to as an "implementation period") which will last until 31 December 2020 (or possibly until 2022 at the latest by joint agreement),[81] during which EU data protection law will continue to apply in and to the UK.[82] The Political Declaration sets out a vision for the future, including a commitment to a high level of data protection and ensuring the free flow of personal data between the EU and UK, accompanies the Withdrawal Agreement. It indicates willingness on the part of the European Commission to commence an adequacy assessment during the transition period with the aim of securing an adequacy finding by the end of 2020 i.e. by the end of the anticipated transition period. It also states that the UK will put in place a mechanism to ensure a free flow of data from the UK to the EU and further mentions an intention to have "appropriate cooperation between regulators". Taken together, these texts confirm a commitment by the UK to maintaining GDPR standards during the transition period, which is welcome news for international businesses seeking certainty, consistency and continuity in the measures

78 Prime Minister's Office, Prime Minister's letter to Donald Tusk triggering Article 50, 29 March 2017, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604079/Prime_Ministers_letter_to_European_Council_President_Donald_Tusk.pdf>
79 Department for Exiting the European Union, Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as endorsed by leaders at a special meeting of the European Council on 25 November 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759019/25_November_Agreement_on_the_withdrawal_of_the_United_Kingdom_of_Great_Britain_and_Northern_Ireland_from_the_European_Union_and_the_European_Atomic_Energy_Community.pdf>.
80 Department for Exiting the European Union, Political Declaration Setting Out The Framework For The Future Relationship Between The European Union And The United Kingdom, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759021/25_November_Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom__.pdf>.
81 Article 132 of the Withdrawal Agreement provides that the Joint Committee (i.e. UK and EU representatives deciding jointly) can agree to extend the transition period at any time before 1 July 2020 (i.e. 6 months before the end of the transition period).
82 Art 127.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

they have to take to protect personal data. It also offers reassurance to individuals that data protection measures will remain robust immediately after the UK leaves the EU.

The Withdrawal Agreement and Political Declaration were approved by EU member states at a special European Council meeting on 25th November 2018.[83] The UK government subsequently laid the final version of the Withdrawal Agreement before Parliament, as it needs implementation in domestic law through primary legislation to be given legal effect. This outcome is by no means assured, however, as it remains to be seen whether it will survive debate and votes in the UK parliament (it has already been the subject of a historically large government defeat and it remains to be seen whether contested provisions regarding the UK-EU border in Ireland will be resolved). If the UK government eventually approves the Withdrawal agreement and Political Declaration, then the transitional data protection arrangements set out below will take effect.

C- Personal data transfers during a transition period

The Withdrawal Agreement states that GDPR will continue to apply in and to the UK in relation to personal data processed during the transition period thereby ensuring that there will be no restrictions on personal data transfers between the EU and UK during the transition period.[84] The Withdrawal agreement further provides that EU member states will not treat data received from the UK during the transition period differently to data received from EU member states solely on the basis that the UK has left the EU.[85] The CJEU will continue to have jurisdiction to settle questions of interpretation raised by the UK courts regarding data protection law and the UK will abide by CJEU decisions during the transition period.[86]

Significantly, the Withdrawal Agreement provides that:

> "Union law on the protection of personal data shall apply in the United Kingdom in respect of the processing of personal data of data subjects outside the United Kingdom, provided that the personal data (a) were processed in accordance with Union law in the Union Kingdom before the end of the transition period; or (b) are processed in the United Kingdom after the end of the transition period on the basis of this Agreement." [87]

When read in conjunction with comments in a speech by Emma Bate, General Counsel for the Information Commissioner's Office (ICO):

> "... you may be interested to hear the current [ICO] thinking regarding transfers. We have moved away from pure geographical considerations. A transfer of data outside the EEA is not restricted by Chapter V of the GDPR if the data, when held by the non-EEA recipient, is still protected by the extra-territorial scope provisions of the GDPR. The rationale being that no additional protection is needed as the GDPR still applies, so this is not a transfer outside of the protection of the GDPR."[88]

It is apparent that the ICO is of the view that data transfer restrictions under the GDPR do not apply where the recipient of personal data is directly bound by the GDPR, i.e. covered by a "GDPR-envelope". This approach could have positive implications for international transfers of data from the UK during the transition period because the general counsel of the ICO has seemingly suggested that data transfers to non-EEA countries that haven't been granted an adequacy decision will be unrestricted if the recipient (UK based business) is already subject to the EU rules. Significantly, the "GDPR-envelope" would apply only to personal data processed in the UK during the transition period,[89] or personal data which continue to be processed in the UK in reliance on these arrangements after the transition period ends[90] because it is anticipated that the "GDPR-envelope" will be superseded by an adequacy decision, which should be in place by the end

83 Council of the European Union, Special meeting of the European Council (Art. 50), 25/11/2018, <https://www.consilium.europa.eu/en/meetings/european-council/2018/11/25/>
84 Department for Exiting the European Union, Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as endorsed by leaders at a special meeting of the European Council on 25 November 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759019/25_November_Agreement_on_the_withdrawal_of_the_United_Kingdom_of_Great_Britain_and_Northern_Ireland_from_the_European_Union_and_the_European_Atomic_Energy_Community.pdf>, Art 71.
85 Ibid, Art 73.
86 Ibid, Art 129.
87 Ibid, Art 71(1).
88 Emma Bate (Counsel, ICO) Speech: Conference 5RB, (26 September 2018) <https://www.whatdotheyknow.com/request/523197/response/1257274/attach/2/Emma%20Bate%20speech%20PDF.pdf>
89 Art 71 (a).
90 Art 71 (b).

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

of the transition period.[91] In effect, it ensures that EU residents' personal data does not lose GDPR protection once the transition period ends if an adequacy decision is not in place by then. Relatedly, Article 71(3) creates a backstop during the transition period, as in the event of a finding of adequacy being withdrawn or revoked it commits the UK to ensuring a level of protection of personal data "essentially equivalent" to that under in the GDPR in respect of EEA residents' personal data.

It remains to be seen whether this "GDPR envelope" will be reflected in the EDPB's guidance on territorial scope and data transfers. The prospect of UK based data controllers being able to continue to receive personal data from EEA countries during the transition period without needing to put in place Chapter V transfer mechanisms (e.g. model clauses or binding corporate rules, or rely one of the derogations), has been welcomed by some data protection experts because "it could only have the effect of making transfers easier."[92] However, other data protection experts have reacted with concern to the "GDPR-envelope" interpretation on the basis that it would allow the UK to temporarily avoid compliance with the *Schrems* criteria i.e. fundamental rights compliant limits on surveillance.[93] These experts have noted that although the "GDPR-envelope" in the withdrawal agreement would be justiciable by the CJEU, the transition period would likely have concluded by the time a complaint was heard.[94] Although it would be better to insist that UK data controllers rely on Chapter V GDPR mechanisms such as contracts and derogations during the transition phase, the reality is that drafting and implementation of such measures e.g. contractual arrangements would be a costly, time consuming (they might not be in place for most of the transition period) and onerous exercise. It would unfairly penalise small and medium sized enterprises, causing harm to both the EU and UK economies, which both parties are keen to avoid, particularly as an adequacy decision could well be in place before the other mechanisms are finalised. Whilst not ideal, the pragmatic 'fudge' minimises economic harm by ensuring that EU-UK personal data transfers continue unimpeded during the transition period, and is acceptable because it will be a temporary arrangement as the UK will still be obliged to *inter alia* amend provisions in the Investigatory Powers Act 2016 in order to secure finding of adequacy by the European Commission by the end of the transition period.

D- Data protection implications of 'No deal'

Of course, if the UK Parliament fails to approve the Withdrawal agreement then the UK is scheduled leave the EU on 29 March 2019 on a 'no-deal' basis with no agreement in place regarding future arrangements for data protection. There would, however, be no immediate change in the UK's data protection standards because the Data Protection Act 2018 would remain in place and the European Union Withdrawal Act 2018 would incorporate the GDPR into UK law.[95] In such circumstances, the UK government would also bring a statutory instrument, namely, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations, 2019 into effect.[96] It would transitionally recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for UK personal data.[97] It would also preserve the effect of existing EU adequacy decisions on a transitional basis so that transfers from UK organisations to adequate countries, territories, or international organisations could continue uninterrupted.[98] It would maintain the extra-territorial scope of the Data Protection Act 2018[99] and oblige non-UK controllers processing UK data on a large scale to

91 Art 71(2).
92 S. Clark, No SCCs needed for data controllers governed by GDPR, ICO lawyer suggests, quoted Jon Baines, Mischon de Reya, in Global Data Review Blog, (12 October 2018), <https://globaldatareview.com/article/1175590/no-sccs-needed-for-data-controllers-governed-by-gdpr-ico-lawyer-suggests>
93 C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650
94 Cybermatron, Data protection in the EU-UK Withdrawal Agreement - Are we being framed? Cybermatron Blog, (15 November 2018), <http://cybermatron.blogspot.com/2018/11/data-protection-in-eu-uk-withdrawal.html>
95 European Union (Withdrawal Act) 2018, <http://www.legislation.gov.uk/ukpga/2018/16/contents/enacted>
96 A draft Statutory Instrument, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, has been prepared in readiness. <http://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf>
97 Department for Digital, Culture, Media & Sport, Guidance: Amendments to UK data protection law in the event the UK leaves the EU without a deal on 29 March 2019, (13 December 2018), <https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019>, para 2.2.
98 Ibid, para 2.3; Adequacy decisions are currently in place for: Andorra, Argentina, Canada (commercial organisations, PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to Privacy Shield, white-listed organisations).
99 Ibid, para 2.6; The Data Protection Act 2018 would apply to controllers or processors who are based outside of the UK where they are processing personal data about individuals in the UK in connection with offering them goods and services, or monitoring their behaviour, including controllers and processors based in EEA states.

UK: GDPR ADAPTIONS by, *Dr. Karen Mc Cullagh*

it to appoint a UK representative.[100] Furthermore, the UK would continue to recognise European Commission approved Standard Contractual Clauses (SCCs),[101] and Binding Corporate Rules (BCRs) authorised before the exit date,[102] and the ICO the Information Commissioner would have the power to issue new SCCs after Exit day under the proposed regulations.[103]

Whilst these laws would enable data to flow from the UK to EEA countries without additional measures, transfers of personal data from the EEA to the UK would be affected as EEA data exporters would need to put appropriate safeguards such as SCCs and BCRs in place for transfers of personal data into the UK, until such times as the UK secures an adequacy decision (which can only be applied for when the UK becomes a 'third' country).[104]

E- Prospects of a obtaining an adequacy decision

Irrespective of whether the UK leaves the EU with Withdrawal Agreement transitional arrangements in place or on a no deal basis, securing an adequacy decision will be vital to ensuring the unimpeded personal data between the EU and the UK in the longer term. There is, however, no guarantee that the UK will obtain an adequacy decision from the European Commission because provisions in the Data Protection Act 2018, that is, the inclusion of a declaratory section on personal data instead of incorporating Art 8 of the EU Charter into UK law, and the inclusion of the Immigration exemption (subject to the outcome of the judicial review action instigated by action groups: ORG and the 3million). Furthermore, provisions in the Investigatory Powers Act 2016 concerning the bulk collection and retention of communications data powers of the UK surveillance services are likely to be an obstacle to an adequacy finding. Until such time as these provisions are amended, a finding of adequacy is not likely to be forthcoming.[105]

F- Impact on the ICO

Another consequence of Brexit is that the UK national supervisory authority, the ICO, involvement and influence in regulatory co-operation mechanisms will be significantly reduced when the UK leaves the EU and becomes a 'third country' for data protection purposes. If the UK secures an adequacy decision the ICO could potentially be granted observer status (as opposed to full membership status) at European Data Protection Board meetings. However, as an 'observer' the ICO would not have a right to vote in such meetings, so would lose its ability to directly influence the development of data protection in the EU. Also, the ICO would not be able to participate in the One Stop Shop dispute resolution mechanism, nor would it be permitted to act as the lead authority for Binding Corporate Rules applications.

IV-CONCLUDING REMARKS

The UK Government is to be commended for taking the opportunity to maintain alignment with the GDPR before and after Brexit as the EU promotes it as the global 'gold standard' data protection law.[106] It signals to businesses and individuals that the UK intends to maintain high standards of protection in respect of personal data processing – a vitally important message given that personal data processing underpins the UK economy. However, incorporating the GDPR into UK law upon withdrawal from the EU will not in and of itself be enough to satisfy the EC that a finding of adequacy should be made in respect of the UK. As outlined above, to secure an adequacy decision the UK will have to revise both the DPA 2018 and national surveillance laws, but these changes are worth making to ensure regulatory alignment and frictionless EEA-UK trade in personal data.

100 Ibid para 2.7; The requirement does not apply to public authorities or if the controller/processor's processing is only occasional, low risk, and does not involve special category or criminal offence data on a large scale. This obligation mirrors GDPR Article 27.
101 Ibid, para 2.4
102 Ibid, para 2.5
103 Ibid paras 2.4 & 2.5
104 Ibid, para 2.2.
105 It is beyond the scope of this chapter to discuss provisions in the Investigatory Powers Act 2016 that may preclude a finding of adequacy. However, an analysis can be found in Mc Cullagh, K. Post-Brexit Data Protection in the UK, *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, eds. R. Van Brakel, & P. De Hert, (Edward Elgar).

106 Butarelli, G. 'The EU GDPR as a clarion call for a new global digital gold standard,' *International Data Privacy Law*, Volume 6, Issue 2, 1 May 2016, Pages 77–78.

DATA PROTECTION IN SWITZERLAND: A PREVIEW

By François Charlet
DPO and Lawyer specialising in IT Law

The Federal Act on Data Protection (FADP) was first enacted in 1993 and is currently subject to a complete revision. It applies only to the processing of data pertaining to natural persons and legal persons by private persons and federal bodies. Cantons and communes have their own data protection acts regarding the processing of data by their authorities. Other sectoral laws contain provisions that apply to specific sectors (e.g. employment law and social security law).

Switzerland is not part of the European Union but signed many agreements with the European Commission in various fields (e.g. free trade, insurance, customs facilitation, security, free movement of persons, research). Switzerland achieved adequacy status under the 1995 Data Protection Directive.

I-GDPR EFFECTS FOR SWITZERLAND

Swiss organisations fear that Switzerland may lose its adequacy status between the 25 May 2018 and the entry into force of its revised FADP, which may not happen before mid 2019. At the moment nobody knows when the European Commission will revaluate the adequacy decisions and there is no evidence the European Commission intends to imminently change its mind regarding Switzerland's status. It is clear, however, that the result of the revaluation will depend on the choices made by the Swiss Parliament regarding the FADP's overhaul. Should the European Commission refuse to maintain the Switzerland's status, the effects on the Swiss market and especially the SMEs would be problematic. Swiss companies could have to commit to respecting GDPR provisions (e.g. through Binding corporate rules or model clauses).

The GDPR applies to the processing of personal data by a controller or processor outside the European Union, if the data subjects are in the Union, and if the controller or processor is offering goods and services to those in the Union, or monitoring the behaviour of those within the EU (§ 3.2 GDPR). There is no doubt that Swiss organisations are subject to GDPR if one of these two conditions is fulfilled, even though they do not have an establishment in the EU.

However, GDPR creates uncertainties and impracticalities regarding Swiss organisations and their relationship to European authorities and supervisory authorities. Here is a selection.

- Some Swiss companies are required by law to process personal data in order to fulfil their mandate (e.g. social security). There could be a conflict of laws between the GDPR and the sectoral laws regarding the legal framework that must be applied to European residents. The abovementioned agreements between the EU and Switzerland would possibly need to be revised in order to take this problem into account.

- Numerous recitals and provisions of the GDPR refer to the law of the Member States (e.g. regarding the processing of special categories of personal data, § 9.2 GDPR). Switzerland is not a Member State, which means Swiss national laws have no effect regarding the GDPR recitals and provisions referring to Member States law, even though GDPR applies to Swiss organisations according to § 3.2 GDPR. Were the Swiss adequacy status maintained or not, it would have no impact on this issue.

- For example, organisations in the EU must communicate the details of their data protection officer to the supervisory authority (§ 37.7 GDPR). Who is the European supervisory authority for a Swiss organisation that has no establishment in the EU? It cannot be a Swiss authority because the supervisory authority must be established in a Member State. Can a Swiss organisation therefore 'choose' its

DATA PROTECTION IN SWITZERLAND: A PREVIEW by, *François Charlet*

supervisory authority amongst Member States when it has no establishment within the EU? As Switzerland's main languages are German, French and Italian, it is likely that Swiss organisations will communicate with authorities that speak their language, or 'choose' the supervisory authority of the Member State in which they have more customers.

- Switzerland's economic actors are mainly SMEs, and these have generally no establishment abroad. Without an establishment in the EU to investigate, European and Member States' supervisory authorities will be tasked with investigating data protection suspected violations directly in Switzerland. However, Swiss sovereignty prevents this from happening without an agreement between Switzerland and the European Commission (and possibly the Member States).

- This raises the question about whether Swiss authorities will collaborate with European supervisory authorities when the latter need to investigate Swiss organisation's processing activities in Switzerland. There is no doubt the Swiss federal supervisory authority, the Federal Data Protection and Information Commissioner (FDPIC), will want to collaborate with European supervisory authorities regarding their investigations will create an official collaboration between the European Data Protection Board (EDPB) and European Free Trade Association (EFTA) DPAs or integrate EFPA DPAs into the EDPB as observer/consultative parties.

- Another question is whether the FDPIC will have the resources to do it. In 2017, its budget amounted to about 5.7 million Swiss Francs, with 5.1 million only for salaries and other staff-related expenses. In March 2018 the FDPIC had an equivalent of 27 full-time employees.

- How will administrative fines and other corrective measures be enforced if they are imposed on Swiss organisations that have no establishment in the EU? In order to protect the Swiss sovereignty, agreements will need to be signed (if they are not already) with the European Commission and the Member States. It needs to be specified clearly that the FDPIC will not enforce the GDPR against Swiss organisations. The FDPIC will certainly collaborate to Europeans investigations but will not take measures against Swiss companies based on the GDPR. (So, will this render the GDPR toothless/ineffective? How can Swiss organisations be 'persuaded' to comply – is it the threat of not renewing an adequacy decision?)

- As mentioned by the Swiss Government in a response to a Member of the Federal Parliament's question, another issue is the concept of double jeopardy (i.e. the same misconduct cannot be prosecuted more than once; *ne bis in idem* principle). The current FADP does not lay down any administrative penalty for failures to comply with data protection laws. However, it is proposed (though Parliament has not yet finally agreed that) the revised FADP should introduce fines up to 250,000 Swiss Francs (currently approximately 200,000 euros). This maximal amount is nothing in comparison to the fines introduced by the GDPR (§ 83). If the same data protection violation by the same Swiss organisation is prosecuted by an European administrative authority (e.g. a supervisory authority) and a Swiss criminal authority, the latter could take into account the European authority sanction only if it qualifies as a criminal sanction according to the European Court of Human Rights (*Engel and others v. The Netherlands* [GC], no 5100/71, § 50, ECHR 1976), which could be the case.

II-CONCLUSION

The wording of GDPR is often not clear and brings confusion to European companies and supervisory authorities. The situation is worse and rather more complex for non-Member States like Switzerland and their organisations that face numerous specific questions, a selection of which was highlighted above. Regardless of these specific uncertainties, Swiss organisations have the same problems as European organisations regarding GDPR implementation.

THE IMPACT OF GDPR IN JAPAN

By Hiroshi Miyashita
Associate Professor, LL.D., Chuo University, Tokyo, Japan

I-GDPR IN JAPAN

It is not an exaggeration to say that the European Union's (EU) General Data Protection regulation (hereafter 'GDPR') has become a new Japanese word, and particularly so for the global business in 2018. The GDPR was translated into Japanese by the Personal Information Protection Commission in 2018[1]. Further, the GDPR was a topic of debate in 2018 in the Diet (Japanese Parliament)[2]. A report published in Nikkei newspaper stated that the GDPR was ranked in the first place in the oversea cases based on the survey by the lawyers in 2018[3]. Several GDPR commentaries in Japanese were published in 2018[4]. This short article examines the impact of the GDPR in Japan, a non-EU country.

Countries such as Japan that are not a part of the EU should be mindful of at least two important articles. First, GDPR provides the extraterritorial scope (Art.3)- that is, if a Japanese company has an establishment in the EU for processing personal data, GDPR will undoubtedly apply. Even without an establishment within the EU, if a Japanese company offers goods or services or monitors the behaviour of individuals in the EU, this company is required to comply with the GDPR. Second, GDPR will apply when a Japanese company transfers personal data from the European Economic Area (EEA). Thus, the Japanese companies had to utilise other mechanisms such as standard contractual clauses, binding corporate rules, or certification (Art.46 & 47) until the European Commission officially makes an adequacy decision in respect of Japan (Art 45). This short article thus aims at clarifying the impact of the GDPR, in particular in the context of data transfer from the EU to Japan and its related process for mutual adequacy[5].

II-AMENDMENTS TO DATA PROTECTION LEGISLATION IN 2015

Japan has its own data protection laws in addition to the personality right interpreted from the Constitution and the civil law. For instance, the Supreme Court of Japan held, in the case of providing personal information of the students without consent from the university to the police for the Chinese parliamentarian Jintao's lecture, that the university infringed privacy of the students by betraying the reasonable expectation of proper management of information relating to privacy voluntarily provided by the students[6]. A remedy for this tort could be sought under the Civil Code[7]. The Court has also held in the case of residential network (the so-called Juki-Net) that every individual has the liberty of protecting his or her own personal information from being disclosed to a third party or being made public without good reason as a part of private life liberty of an individual under the Constitution Art.13[8], but concluded that the residential network system does not violate such liberty[9].

1 Personal Information Protection Commission homepage (https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/).
2 For instance, House of Representatives, Committee on Economy, Trade and Industry, 196th Diet, 16 May 2018.
3 Nikkei newspaper, Corporate legal affairs and lawyers' survey in 2018, 17 December 2018 p. 11.
4 For instance, Hiroshi Miyashita, EU General Data Protection Regulation, Keisoshobo, 2018.
5 The details of the Japanese legal systems on data protection cannot be described in this article. See Hiroshi Miyashita, Japan amends its DP Act in light of big data and data transfers, *Privacy Laws & Business International Report*, vol.137 (2015) p.8: Graham Greenleaf, Japan: Toward international standards except for 'Big Data', *Privacy Laws & Business International Report*, Vol.135 (2015) p.12.
6 Judgment of the Supreme Court on 12 September 2003, Minshu vol.57 no. 8 p.973.
7 A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence. (Art.709)
8 All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs. (Art.13)
9 Judgment of the Supreme Court on 6 March 2008, Minshu vol.

THE IMPACT OF GDPR IN JAPAN by, *Hiroshi Miyashita*

In May 2003, the Act on the Protection of Personal Information (hereafter 'APPI') was promulgated, and it fully entered into effect in April 2005. Along with the comprehensive basic idea, APPI provides the obligations of the business operators in handling personal information in the private sectors. For the public sector, the two separate laws were introduced in 2003: the Act on the Protection of Personal Information Held by Administrative Organs (hereafter 'APPIHAO') and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (hereafter 'APPI-IAA'). In addition, the Cabinet Order and the Guidelines supplements these laws.

The Japanese data protection laws are rooted in the eight principles set by the OECD (Organisation for Economic Co-operation and Development) Privacy Guidelines in 1980. In Japan, before the 2015 amendments (discussed below), there was no independent supervisory authority in Japan responsible for data protection; instead, each competent ministry used to have supervisory powers over supervision for its own business sector under co-ordination of the Cabinet Office and, later, that of the Consumer Affairs Agency. In the public sector, the Ministry of Internal Affairs and Communications was given the power to supervise both the APPIHAO and the APPI-IAA.

With the rise of big data business in 2013, there were controversies with regard to the scope of personal information in Japan. For instance, it was revealed in 2013 that 43 million personal data including the public transportation IC cards were permitted to be sold to a data analytics company following removal of a certain information such as name, date of birthdate, telephone number, sales information etc[10]. In 2014, the National Institute of Information and Communications Technology planned to conduct an experiment at the Osaka station using the automatic facial recognition CCTVs to capture the people's images and to trace their gaits, and automatically and immediately convert these into a unique ID[11]. Under APPI, personal information is defined as information relating to the living individual by which a specific individual can be identified including those which can be 'readily collated' with other information and thereby identify a specific individual. Here, 'readily collated' may mean 'easily collated' with other information, but the information which may not be 'easily collated' with other information is out of the scope of the obligation provided by the APPI. Following these cases, there was much discussion regarding 'identifiability' in the context of the definition of personal information between the pseudonymous data and anonymous data.

With a clear awareness of the EU data protection reform, the APPI was amended in September 2015 and it entered into force on 30 May 2017. The public sector laws of the APPIHAO and the APPI-IAA were also amended in 2016 to include the de-identification processing of information. The amended APPI, which will be discussed later in this article, can be summarised as follows.

First, the amended APPI establishes Personal Information Protection Commission (hereafter 'PPC'), a new independent supervisory authority, to overcome the enforcement regime. The scope of power for the PPC lies under the APPI, so that the public sector laws of the APPIHAO and the APPI-IAA are supervised, except for the de-identification processing, by the Ministry of Internal Affairs and Communications.

Second, the scope of personal information was clarified by adding new categories of personal information that required special care such as race, creed, social status and medical history. Additionally, the amended APPI included individual identification code in its protective scope such as driving licence number, individual identification number (referred to as so-called My number), fingerprints and vein.

Third, the amended APPI aims to promote the big data businesses that process anonymised information. The PPC issued Guidelines on anonymously processing information to share some good practices this aspect[12].

Fourth, as a counter-measure to incidents such as the data broker scandal by an education company[13], it is mandatory for the business operators to ensure

62 no. 3 p.665.

10 See JR sells commuters' data, Japan Times, 3 August 2013. https://www.japantimes.co.jp/opinion/2013/08/03/editorials/jr-sells-commuters-data/ See also Shigeru Kawasaki, The challenges of transportation/traffic statistics in Japan and directions for the future, IATSS Research, vol.39 issue 1, p.1.

11 See Osaka train station set for large face-recognition study, PCWorld, 5 February 2014. https://www.pcworld.com/article/2094660/osaka-train-station-set-for-large-facerecognition-study.html

12 PPC, Guidelines on the Act of Protection of Personal Information (Anonymously processing information edition) https://www.ppc.go.jp/files/pdf/guidelines04.pdf (in Japanese).

13 Benesse Holdings, Inc., Investigation report by the data breach incident investigation committee, 25 September 2014 p.5 (in Japanese). According to this investigation report, a total of 35.04 million items (some cases of a single item including several personal data) were leaked.

THE IMPACT OF GDPR IN JAPAN by, *Hiroshi Miyashita*

the traceability of personal data, in principle, for three years.

Fifth, to promote international harmonization and cooperation, the APPI incorporates the articles pertaining to data transfer restriction and international cooperation. Data transfers to a third country are restricted unless the third country ensures an equivalent level of protection as Japan or the controller in the third country takes appropriate measures to protect of personal information. During the parliamentary debate in the Japanese Diet, the Minister of the Cabinet Office announced that the Japanese government after government, insert: intended to obtain an EC adequacy decision in order to improve the data transfer practices for Japanese companies established in the EU [or monitoring the behaviour of individuals in the EU][14].

III-EU-JAPAN MUTUAL ADEQUACY STRATEGY

The EU and Japan initiated the mutual adequacy strategy, quite possibly motivated by the EU-Japan negotiations regarding Economic Partnership Agreement and Strategic Partnership Agreement[15]. In January 2017, the European Commission published the Communication on 'Exchanging and Protecting Personal Data in a Globalised World', which clearly mentions prioritising adequacy discussions with Japan[16]. On 4 July 2017, the two Commissioners from EU DG Justice and PPC stated that 'the recent reforms of their respective privacy legislation have further increased the convergence between their two systems'[17]. Following this Communication and the statement, both political leaders in the EU and Japan issued a joint declaration on 6 July 2017, stating that 'new opportunities to facilitate data exchanges, including through a simultaneous finding of an adequate level of protection by both sides'[18]. Later on, a series of statements from the two Commissioners followed to reach the mutual adequacy discussions until July 2018[19].

It is well known that the EU had data transfer restrictions in the 1995 EU Data Protection Directive. The EU 'white-listed' 11 countries in addition to the EU-US Privacy Shield, as providing an adequate level of protection before the GDPR entered into effect. During the parliamentary debate on amending the APPI in Japan, the Japanese government consciously identified the several factors that needed to be changed before seeking an adequacy decision from the European Commission. For instance, the government mentioned the following five issues (now addressed through the APPI amendments) should be solved to obtain adequacy with, namely: independent authority, sensitive data, small business enterprise exemptions, data transfer restriction and clarification of the right to request management[20]. These five issues were all amended in APPI during this process.

On the other hand, there were no specific data transfer restrictions under APPI before the 2015 amendments. The amended APPI introduced the EU-style data export restrictions. The third country must ensure an equivalent level of protection to the Japanese system, or the third party of receiving personal data from Japan must establish a system conforming to the standards provided by the PPC rules (Art.24)[21]. The PPC rules clarify the standards of the third country through Art. 24 of the APPI. According to the PPC rules (Art.11(1)), the third country may be found as having an equivalent level of protection if, as can be summarised,

14 House of Representatives, plenary session, Minister Shunichi Yamaguchi's statement, 189th Diet, 23 April 2015.
15 EU-Japan EPA & SPA negotiations was initiated in March 2013 and concluded with the exchange of diplomatic notes in December 2018. https://www.mofa.go.jp/region/page5e_000023.html https://www.mofa.go.jp/press/release/press1e_000110.html
16 European Commission, Communication on exchanging and protecting personal data in a globalised world, 10 January 2017, p.8 & p.10. The Communication also indicates the adequacy talk with South Korea.
17 Press statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 4 July 2017. https://www.ppc.go.jp/files/pdf/290704_pressstatement.pdf
18 Joint declaration by Mr. Shinzo Abe, Prime Minister of Japan and Mr. Jean-Claude Juncker, President of the European Commission, 6 July 2017. https://www.mofa.go.jp/mofaj/files/000270696.pdf
19 Joint statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 14 December 2017; Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 31 May 2018; Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, 17 July 2018. https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf; https://www.ppc.go.jp/files/pdf/300531_pressstatement.pdf; https://www.ppc.go.jp/files/pdf/300717_pressstatement2.pdf See Yumi Watanabe, Japan EU Data Transfers - Mutual adequacy findings under APPI and GDPR, Global Compliance News, 9 April 2018. https://globalcompliancenews.com/japan-eu-data-transfers-20180409/
20 House of Councilors, Cabinet Committee, Councilor, Cabinet Secretariat, statement, 189th Diet, 26 May 2015.
21 PPC issued Guidelines on transfer to the third party in the foreign country edition in November 2016 (in Japanese) https://www.ppc.go.jp/files/pdf/guidelines02.pdf

THE IMPACT OF GDPR IN JAPAN by, *Hiroshi Miyashita*

it (i) has equivalent legislation, (ii) has an independent authority equivalent to the PPC with its necessary and proper supervision, (iii) enables cooperation with Japan based on the mutual understanding of utilising proper and effective personal information and protection of the rights and interest of an individual, (iv) is capable of transferring personal data mutually and smoothly without hindering international data transfer beyond the necessary scope, and (v) will promote creation of new industry, vigorous economic society and wealthy citizens' life. On the basis of these rules, the PPC tabled a proposal recognising the EU member states as providing an equivalent level of protection by ensuring (i) (stated in the previous sentence) in July 2018[22].

IV-THE PPC'S SUPPLEMENTARY RULES

The amended APPI may still have gaps if one compares it with provisions in the GDPR. Therefore, the PPC published Guidelines on the handling of personal data transferred from the EU based on an adequacy decision in April 2018. According to the PPC, these Guidelines were changed into 'Supplementary Rules' in September 2018 in order to satisfy the minimum compliance requirements[23]. Therefore, the Supplementary Rules state that they are 'binding on a personal information handling business operator that receives personal data transferred from the EU based on an adequacy decision'.

The Supplementary Rules have the following five elements to supplement the APPI and the existing Guidelines: (i) Special care-required personal information now also includes data concerning a natural person's sex life or sexual orientation or trade-union membership, which are not explicitly written in the APPI. (ii) Retained personal data is protected irrespective of the period which it is set to be deleted, though the Cabinet Order excludes personal data retained for less than six months. (iii) The business operator must confirm and record the purpose for which personal data is received from the EU, in addition to the items to be confirmed and recorded under the APPI. (iv) As to the restriction on data transfers to a third party in a foreign country, a third party must obtain consent from data subjects in advance, or the third party's country must meet the level of protection equivalent to that in Japan, and the third party then implements appropriate and reasonable measures such as contract or binding arrangements within a company group. (v) Anonymously processed information should make the de-identification of the individual irreversible for anyone, though there are only requirements of non-identifiable and non-restorable information under the APPI. Among these five elements, data transfer restrictions are notably stricter than the Guidelines originally issued by PPC, which allows the company to use the APEC (Asia-Pacific Economic Cooperation) Cross-Border Privacy Rules to fit the e-commerce scheme in this region[24].

It remains unclear whether these Supplementary Rules developed without input from the Diet will be found binding and enforceable by Japanese courts; they could be challenged in the courts because the normal legislative process has not been followed in their creation[25]. It is also questionable whether a Japanese company can discriminate between personal data transferred from the EU and the non-EU personal data (eg., personal data on LGBT status from the EU may be treated as sensitive data, but LGBT data processed in Japan are not treated as such). Yet, it is likely that these Supplementary Rules will become an integral part of the APPI during the process of future amendments.

In addition to these five major issued to be bridged by the Supplementary Rules, one may still identify the several elements missing from the APPI, namely, definition of consent and withdraw of consent, data portability right, profiling, data breach notification, data protection officer, the amount and enforcement of fines (maximum one year imprisonment or 500,000 yen (approximately 4,000 euros)).

V-FATE OF MUTUAL ADEQUACY

On 5 September 2018, the European Commission issued a draft adequacy decision on Japan under Art. 45 of GDPR[26]. The draft adequacy decision has a comprehensive and detailed explanation of the Japanese

22 PPC, On the designation of EU based on the Art. 24 of the Act on the Protection of Personal Information, 70th Meeting,17 July 2018 (in Japanese). https://www.ppc.go.jp/files/pdf/180717_shiryou2-1.pdf
23 PPC, Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, September 2018. https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf English translation is available at the Commission's adequacy draft Annex I.

24 The analysis of APEC CBPR scheme which may be used for onward transfer from the EU to other APEC regions is Marija Bartl & Kristina Irion, The Japan EU Economic Partnership Agreement: flows of personal data to the land of the rising sun, 25 October 2017. https://www.ivir.nl/publicaties/download/Transfer-of-personal-data-to-the-land-of-the-rising-sun-FINAL.pdf
25 Graham Greenleaf, Japan's proposed EU adequacy assessment: substantive issues and procedural hurdles, *Privacy Laws & Business International Report*, vol.154 (2018) p. 5.
26 European Commission, Commission implementing decision of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan, 5 September 2018.

THE IMPACT OF GDPR IN JAPAN by, *Hiroshi Miyashita*

data protection laws, including government access to data held by private companies. In the conclusion of the draft adequacy decision, the Commission considered that the APPI, together with the Supplementary Rules and the commitments by the official representations, ensures that Japan provides an essentially equivalent level of protection to that guaranteed by the GDPR (para 171 & Art.1(1) of the draft adequacy decision).

Most importantly, the scope of adequacy is limited to 'personal data transferred from the European Union to personal information handling business operators in Japan' under the APPI and the Supplementary Rules in Annex I with English translation. In other words, the adequacy scope is limited to the private sector in the context of data transfer from the EU. As for the government access to data held by the private companies in Japan, the details are explained by each Ministry in the Annex II which is subject to a repeal, amendment, or suspension of the adequacy decision if in the case of noncompliance.

In December 2018, the European Data Protection Board (EDPB) issued an opinion with admiration of the convergence between the two systems but also recorded several concerns[27]. The concerns include: (i) the Commission should monitor onward transfers from EU via Japan to another third country; (ii) the notions of consent and transparency are not clearly defined including withdrawal of consent and the obligation to genuinely inform data subjects; and (iii) there is a risk that EU individuals may face difficulties in accessing administrative and judicial redress. Some clarifications and monitoring demands made to the Commission are pronounced, such as the difference between the 'handling personal data' under the APPI and 'processing personal data' under GDPR, the status of 'trustee', the restrictions to the rights of individuals, the cases regarding direct-marketing and profiling, the effectiveness of sanctions and relevant remedies, the scope of voluntary disclosure procedure in the cases of government access to private data and the whole life cycle of the effective protection of personal data. In light of these concerns and the other clarifications sought by the Commission, the EDPB called for the Commission to conduct a review of the Japanese adequacy finding (at least) every two years instead of the existing once-in-four-years cycle.

Alongside the EDPB's opinion, the European Parliament also issued a resolution stipulating some concerns[28]. These concerns are summarised as follows: (i) The definition of personal data might not meet the standard of being essentially equivalent to the GDPR since the Japanese harm-based approach in defining of personal data is not compatible with the EU approach and its scope is not likely to include information to 'single out' a person. (ii) There are no legal provisions regarding automated decision-making, profiling, and direct-marketing. (iii) There should be further evidence and explanation of demonstrating the existence of appropriate safeguards throughout their whole life cycle of protection of personal data. (iv) A clear explanation is necessary in the case of an onward transfer by prior consent, which has no definition in the APPI. (v) The level of possible fines that would be imposed by the penal authorities is insufficient to ensure effective compliance with the APPI. (vi) The European Commission being encouraged to assess government access of private data on a 'voluntary basis' would be compliant with the GDPR[29]. (vii) The European Commission should provide more information about Japanese mass surveillance.

Some of the concerns were already identified during the amendment process in 2015 in Japan. For instance, some of the important issues such as profiling and the dispute resolution for appropriate remedies were discussed during the amendment process but eventually were passed over as a future task and were not tabled in the amendments[30]. The scope of personal information such as IP address and terminal ID, in particular in the context of it being 'readily collated' with other information, was also intensively debated in the Diet[31]. In this sense, most of the concerns expressed by the EDPB and the European Parliament are expected to be addressed in the next amendments process.

27 European Data Protection Board, Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, 5 December 2018.

28 European Parliament, Resolution of 13 December 2018 on the adequacy of the protection of personal data afforded by Japan, 13 December 2018.

29 The recent newspaper article notes that the Prosecutor's Office has a list of approximately 290 companies that give customers' data to the Office on a voluntary basis. See Prosecutor listed how to obtain customers' data and holds it from the 290 companies, 3 January 2019, Tokyo newspaper (in Japanese). http://www.tokyo-np.co.jp/s/article/2019010301000873.html

30 IT Strategic Headquarters, Policy Outline of the Institutional Revision for Utilization of Personal Data, 24 June 2014 p.23. http://japan.kantei.go.jp/policy/it/20140715_2.pdf

31 House of Representatives, Budget Committee, first subcommittee, 189th Diet, 10 March 2015. Councilor of Cabinet Secretariat testified that both terminal ID and IP address are basically out of the scope of personal information since they are automatically assigned.

THE IMPACT OF GDPR IN JAPAN by, *Hiroshi Miyashita*

It may be possible to bridge the two systems, in order to overcome the expressed concerns by the EDPB and the European Parliament, with amendments of APPI, and might be supplemented by the additional guidelines or supplementary rules or further assurances or commitments. The EU-Japan bridge needs to be robust enough to foresee and endure the digital tsunami in the coming new technologies such as artificial intelligence and robotics[32].

At the same time, it is not just academically but practically important to carefully observe the consequences of protection of personal data in the context of trade based on the EU-Japan Economic Partnership Agreement (hereafter 'EPA'), entering into force in February 2019. Since the EU had only adopted the adequate decisions with four countries out of 20 largest trading partners so far, the EU-Japan EPA will open the door of digital trade[33]. On the other hands, the EPA, in spite of the mutual adequacy strategy, includes a disclaimer which provides that each Party may 'define or regulate *its own levels of protection* in pursuit of or furtherance of its public policy objectives in areas' [emphasis added] of 'personal data' (Art.18.1(2)(h) in Chapter 18 good regulatory practices and regulatory cooperation)[34]. The EPA should not lower the level of protection of personal data between the two partners guaranteed by the EU-Japan adequacy decision.

The impact of the GDPR was much bigger than expected after the EU-Japan mutual adequacy negotiations. It is never an easy task to find the 'identical' laws and practices in the different legal history, tradition and culture. At least, the European Commission, EDPB, and the European Parliament recognise that the adequacy assessment does not require Japan to have a legal regime that is 'identical' to that of the EU. Adequacy review does not mean a carbon copy of the data protection text. Instead, the adequacy process needs to reflect the 'essence' of the EU data protection philosophy enshrined in the Charter of Fundamental Rights of the European Union, and provide an 'essentially equivalent' level of protection of fundamental rights[35]. The adequacy scheme should not be viewed for merely a convenient mechanism for facilitating data transfers, rather it should be viewed as a process that allows the EU and the third country to recognise convergence of their data protection philosophies.

- On 23 January 2019, both the European Commission and the Japanese PPC issued the mutual adequacy decision[36]. The joint statement from both Commissioners states 'with this mutual adequacy arrangement, Japan and the EU reaffirm their commitment to shared values in the field of privacy, and to strengthen their cooperation in shaping global standards based on a high level of protection of personal data'. The Japanese Official Gazette lists the 31 countries of the European Economic Area as of 23 January 2019 as ensuring the equivalent level of protection under the PPC rules Art. 11 (1).

32 EU-Japan ICT Dialogue counted 24th in December 2018. https://ec.europa.eu/digital-single-market/en/blogposts/eu-japan-digital-week-2018-vienna

33 European Parliament, Resolution of 12 December 2017 on 'Towards a digital trade strategy', 12 December 2017.

34 The EU-Japan EPA text is available at https://www.mofa.go.jp/files/000382106.pdf

35 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para73 & 96, ECLI:EU:2015:650.

36 European Commission, Press Release: European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, 23 January 2019. http://europa.eu/rapid/press-release_IP-19-421_en.htm: Japanese PPC, The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force, 23 January 2019. https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/

ANNEX : LIST OF THE STUDIED NATIONAL ADAPTATIONS OF THE GDPR

MEMBER STATES	ORIGINAL VERSION
Austria	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG) https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf (With an English version)
Denmark	Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven https://www.retsinformation.dk/Forms/R0710.aspx?id=201319 https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf (English Version)
France	LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel https://www.legifrance.gouv.fr/eli/ordonnance/2018/12/12/JUSC1829503R/jo/texte
Germany	Bundesdatenschutzgesetz https://www.gesetze-im-internet.de/bdsg_2018/index.html https://www.gesetze-im-internet.de/englisch_bdsg/index.html (English version)
Ireland	Data protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
Italy	Decree n°101 of 10 August 2018 http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg
Japan	Japanese 'Act on the Protection of Personal Information' https://www.ppc.go.jp/personal/legal/ (in Japanese) https://www.ppc.go.jp/en/legal/ (in English).
Netherlands	Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) https://www.officielebekendmakingen.nl/stb-2018-144.html
Spain	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf
Sweden	Lag med kompletterande bestämmelser till EU:s dataskyddsförordningen (2018:218) https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218
United Kingdom	Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted