

DATA PROTECTION LAW IN THE EU:
ROLES, RESPONSIBILITIES AND LIABILITY

DATA PROTECTION LAW IN THE EU: ROLES, RESPONSIBILITIES AND LIABILITY

Brendan VAN ALSENOY



intersentia

Cambridge – Antwerp – Chicago

KU LEUVEN

CiTiP

CENTRE FOR IT & IP LAW

Intersentia Ltd
Sheraton House | Castle Park
Cambridge | CB3 0AX | United Kingdom
Tel.: +44 1223 370 170 | Fax: +44 1223 370 169
Email: mail@intersentia.co.uk
www.intersentia.com | www.intersentia.co.uk

Distribution for the UK and Ireland:

NBN International
Airport Business Centre, 10 Thornbury Road
Plymouth, PL6 7 PP
United Kingdom
Tel.: +44 1752 202 301 | Fax: +44 1752 202 331
Email: orders@nbninternational.com

Distribution for Europe and all other countries:

Intersentia Publishing nv
Groenstraat 31
2640 Mortsel
Belgium
Tel.: +32 3 680 15 50 | Fax: +32 3 658 71 21
Email: mail@intersentia.be

Distribution for the USA and Canada:

Independent Publishers Group
Order Department
814 North Franklin Street
Chicago, IL60610
USA
Tel.: +1 800 888 4741 (toll free) | Fax: +1312 337 5985
Email: orders@ipgbook.com

Data Protection Law in the EU: Roles, Responsibilities and Liability

© Brendan Van Alsenoy 2019

The author has asserted the right under the Copyright, Designs and Patents Act 1988, to be identified as author of this work.

No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, without prior written permission from Intersentia, or as expressly permitted by law or under the terms agreed with the appropriate reprographic rights organisation. Enquiries concerning reproduction which may not be covered by the above should be addressed to Intersentia at the address above.

Cover image: Jorma Puranen, Icy Prospects 29

ISBN 978-1-78068-828-2 (paperback)
ISBN 978-1-78068-845-9 (PDF)
D/2019/7849/47
NUR 822

British Library Cataloguing in Publication Data. A catalogue record for this book is available from the British Library.

FOREWORD

Have you ever considered the discussion on responsibilities and liabilities in the field of the European data protection law as a journey? You should. Brendan Van Alsenoy is inviting you take a trip through the whole history of data protection law in Europe and around the world, as well as through current practice to better understand the roles of different actors in what is a fiendishly complicated environment. You will find him to be a guide who effortlessly offers fresh perspectives on the subject: a relatively young scholar leveraging a surprisingly *extensive* and *intensive* practical experience in a national data protection authority as well as playing a key role in the Working Party Article 29 / European Data Protection Board.

This is a guide to the places that you know and new ones you never thought exist. At times it may explain concepts that you heard about dozens of times before. But Van Alsenoy's explanations are slightly different to the others. He is able to filter his academic knowledge through the lens of the regulatory authorities and their current disputes with other institutional and business players around the world.

One of the first problems the author addresses is the binary concepts of controller and processor. Is this division as clear-cut as when it was first postulated decades ago in European law, or it is rather a case that control is now distributed and should be regulated and applied accordingly? Has the concept of controller evolved to the degree that the explanations proposed in '80s and '90s are no longer useful? How does this model work in practice?

One may say that these are the questions posed over and over again. Be that as it may, this book will nonetheless give you a valuable historical background. It offers use cases illustrating how to understand and interpret the system which the GDPR has inherited from previous European legislation. What will be the effect of different forms of joint controllership on the level of responsibility of each of the players?

It is sometimes surprisingly difficult to distinguish the joint controllership of the GDPR from the exchanges between individual controllers who co-operate with each other using shared resources for different purposes or using different means. I must admit I always thought I was able to discern between the two. But having read this book I can see a fresh methodology may be required. If you think it's enough to read the GDPR and the other legislative reforms in the EU over recent years and compare it with current practices in the market, Brendan

Van Alsenoy invites you to think again. Without the historical background and a rigorous methodology you are likely to repeat the same old mistakes of earlier scholars, regulators and jurisprudence.

Your journey will take in the issues, grammatical, teleological, systemic and historical, along with the same typology of solutions. Then the revised model of liability can be proposed.

My suggestion for the reader of this book is this: before you open it, sit down with a piece of paper and try your best to answer the author's main questions:

1. What is the nature and role of the controller and processor concepts under European data protection law?
2. What is the origin of the controller-processor model and how has it evolved over time?
3. What are the types of issues that arise when applying the controller-processor model in practice?
4. Which solutions have been proposed to address the issues that arise in practice and to what extent are they capable of addressing the issues?

Then – when you finish reading the book – take another piece of paper and try to answer the same questions. Compare your answers. My two sets of answers were quite different.

This journey through almost 700 pages was a unique experience as well as a rewarding academic challenge. I now view certain concepts differently compared to when just a few weeks ago, I had this manuscript in my hands for the first time. There are some ideas which I have to re-think again.

So, now I can invite you to follow the same journey I did. It will be an experience to remember. This book will land on the shelf just next to my desk because I am going to go back to it over and over again in my practical work as a regulator.

Dr. Wojciech WIEWIORSKI
European Data Protection Assistant Supervisor

NOTE TO THE READERS

Most of the research for this book was completed on 25 July 2016. Subsequent developments in EU data protection law are only partially addressed. The main updates relate to the judgments of the Court of Justice of the European Union and Advocate General Opinions published until 15 January 2019. Other parts of the text have been revisited or extended in light of the entry into application of the General Data Protection Regulation (GDPR), subsequent regulatory guidance, as well as a selection of academic works.

The contents of this book are based on the contents of my doctoral thesis entitled “*Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing*”, defended at the Law Faculty of KU Leuven on 30 August 2016.

ACKNOWLEDGMENTS

Early in my academic career, a learned professor told me: “the only good PhD is a finished PhD”. What he didn’t tell me, at the time, was that it takes a village to actually finish it. Completing my thesis would not have been possible without the support of my colleagues, family and friends.

I would like to begin by thanking my supervisor, Prof. Dr. Peggy Valcke, for her guidance, encouragement and trust. She gave me time and space to develop my own research, yet she was there to provide practical direction whenever needed. Warm thanks are also due to my co-supervisor, Dr. Els Kindt, for her insightful comments and continuous support. I am indebted to the members of my advisory committee, Prof. Dr. Geertrui Van Overwalle and Prof. Dr. Serge Gutwirth, for the invaluable feedback and references they provided. I thank Prof. Dr. Giovanni Sartor not only for acting as a member of my examination committee, but also for the fresh and critical perspective one so often encounters in his writing. My gratitude goes out to Em. Prof. Dr. Marc Boes for kindly agreeing to chair the examination committee. Finally, I would like to thank Em. Prof. Dr. Jos Dumortier for his advice and support at the beginning of my PhD project.

Working at the Centre for IT & IP law (CiTiP) has been an honour and a privilege. It is an environment filled with bright minds, dedicated people and a passion for knowledge. I would like to thank every one of my colleagues – past and current – for all the stimulating conversations, comradery and memories. Special thanks go out to Fanny Coudert, Jef Ausloos, Bjorn Coene and Yung Shin Van der Sype for providing me with ideas and feedback throughout the writing process. I would also like to thank Kirsten Van Gossum, Griet Verhenneman, Niels Vandezande, Aleksandra Kuczerawy, Eva Lievens, Eleni Kosta, Valerie Verdoodt, Jessica Schroers, Lina Jasmontaite and Ellen Wauters for the great collaborations in the many projects along the way. Finally, I would like to express my sincere appreciation to Shuki Tang, Carmen Clara, Edith Appelmans and Linda Mees, for their unique combination of professionalism and warmth in supporting our research activities on a daily basis.

The findings in this book have benefited from the input of many people outside my university department. I would especially like to thank Prof. Dr. Spiros Simitis and the Hon. Michael Kirby for sharing valuable insights in relation to the 1970 Hesse Data Protection Act and the 1980 OECD Privacy Guidelines. I am extremely grateful to Michael Donohue for giving me the

opportunity to join the OECD Secretariat during the revision of the OECD Privacy Guidelines, as well as for his comments on my research. Dr. Lina Kestemont provided me with invaluable support on how to navigate issues of legal methodology, without which my hermitage perhaps would have been prolonged indefinitely. I thank Joseph Alhadeff for introducing me to the world of multi-stakeholder policy development and for our many lively discussions. I thank Danny De Cock, Günes Açar, Claudia Diaz and Seda Gürses for showing me how cool working with computer scientists can be. Finally, I would like to thank Joelle Jouret for reviewing and commenting on the sections concerning the General Data Protection Regulation.

Last but not least, I would like to thank my family, friends and loved ones. I thank my parents for their unwavering encouragement and support, both in research and in life. I thank my sister for being such an inspiration. I thank Dieter for keeping me grounded and for teaching me that long sentences do not make you seem smarter. I thank Paula for keeping me well-nourished and hydrated during the final stages of the writing process. Finally, I thank Aleksandra for her patience, indulgence and caring, and for giving me the motivation to keep going on.

Brendan VAN ALSENOY
July 2016

ABSTRACT

Practically every organisation in the world processes personal data. In fact, it is difficult to imagine a single organisation which does not regularly collect, store or access information about individuals. European data protection law imposes a series of requirements designed to protect individuals against the risks that result from the processing of their data. It also distinguishes among different types of actors involved in the processing and sets out different obligations for each type of actor. The most important distinction in this regard is the distinction between “controllers” and “processors”. Together these concepts provide the very basis upon which responsibility for compliance with EU data protection law is allocated. As a result, both concepts play a decisive role in determining the potential liability of an organisation under EU data protection law.

For almost 15 years, Directive 95/46 stood strong as the central instrument of EU data protection law. In 2010, however, the European Commission announced that the time for change had come. The Commission considered that while the objectives and principles of Directive 95/46 remained sound, revisions were necessary in order to meet the challenges of technological developments and globalisation. A public consultation conducted in 2009, had revealed concerns regarding the impact of new technologies, as well as a desire for a more comprehensive and coherent approach to data protection. During the consultation, several stakeholders also raised concerns regarding the concepts of controller and processor. Various solutions were put forward, ranging from minor revision to outright abolition of the concepts. In the end, the EU legislature opted to retain the existing concepts of controller and processor in the General Data Protection Regulation (GDPR). Notable changes were made, however, with regards to the allocation of responsibility and liability among the two types of actors.

Technological and societal developments have rendered it increasingly difficult to apply the concepts of “controller” and “processor” in practice. The complexity of today’s processing operations is such that a clear-cut distinction between “controllers” and “processors” is not always possible. Identifying “who’s who” can be particularly difficult when the processing involves a large number of actors, who each play their own distinct role in realising the goal(s) of the processing.

Against this background, this book seeks to determine whether EU data protection law should continue to maintain its current distinction between

controllers and processors as the basis for allocating responsibility and liability. Specifically, it seeks to determine whether it would be possible to modify the current approach in a manner which would increase legal certainty, without diminishing the legal protections enjoyed by data subjects. To realise these objectives, this book undertakes an analysis consisting of five parts.

After a brief introduction, a detailed analysis of the current state of the art is provided. The state of the art explores the nature and role of the controller and processor concepts, as well as the associated allocation of responsibility and liability. The third part of this book offers a historical-comparative analysis, which traces the origin and development of the controller-processor model over time. Having set out the origins and rationale of the controller-processor model, a number of real-life use cases are examined in part four. The aim of this exercise is to document the issues that arise when applying the controller-processor model in practice. Once the issues have been analysed, an evaluation is made of potential solutions. Finally, the approach adopted by the European legislature in the context of the GDPR is compared with the outcome of the preceding evaluation.

The book concludes that the GDPR has introduced considerable improvements, which are likely to be adequate for the time being. In the long run, however, it may become necessary to introduce further changes. Having this in mind, a number of avenues for possible improvements are presented. First, the possibility of abolishing the distinction between controllers and processors should receive further consideration. It is possible to implement the same policy choices without retaining these problematic concepts. Alternatively, the definitions of each concept could be revised to include less ambiguous or mutually exclusive criteria. Second, the EU legislature should consider the use of standards (as opposed to rules) to mitigate risks of overinclusion in certain situations. Third, the obligation to implement data protection by design should also be made directly applicable to the providers of processing services, given their important role in determining the means of the processing. Fourth, the legal framework should allow for greater contractual flexibility in the relationship between “controllers” and “processors”, leaving room for greater specificity in the form of regulatory guidance. Finally, the scope of the personal use exemption should be expanded to apply to all activities which may reasonably be construed as taking place in the course of an individual’s private or family life.

For the immediate future, however, practitioners of EU data protection law will have to continue to work with the controller-processor model as it exists today. This book hopes to provide its readers with the right analytical framework to help navigate the intricate relationship among roles, responsibility and liability under EU data protection law.

CONTENTS

Foreword v

Note to the Readers. vii

Acknowledgments. ix

Abstract xi

PART I.

INTRODUCTION 1

Chapter 1.

Background 3

Chapter 2.

Problem Statement 7

1. A broken “binary” 7

2. The threshold for (joint) control 9

3. The implications of “granular” control. 10

Chapter 3.

Research Questions. 13

Chapter 4.

Structure and Methodology 17

1. State of the art. 17

2. Historical-comparative analysis 18

3. Use cases 19

4. Recommendations. 19

PART II.

STATE OF THE ART 21

Chapter 1.

Introduction. 23

Chapter 2.

Scope of EU Data Protection Law 25

1. Material scope 25
2. Territorial scope 28

Chapter 3.

Basic Protections 33

1. Key principles 33
2. Transparency and data subject rights 37
3. Confidentiality and security 40
4. Supervisory authorities 42
5. Accountability 43

Chapter 4.

Allocation of Responsibility 47

1. Key elements of the “controller” and “processor” concepts 47
 - 1.1. Controller 48
 - 1.2. Processor 52
2. The relationship between controllers and processors 53
 - 2.1. Due diligence 53
 - 2.2. Bound by instructions 55
 - 2.3. Legal binding 57
 - 2.4. Distinguishing between controllers and processors 62
 - A. Circumstances giving rise to “control” 63
 - B. “Purpose” over “means” 65
 - C. Additional criteria 67
 - D. Dynamic perspective 68
 - 2.5. Importance of the distinction 70
3. The relationship between (joint) controllers 72
 - 3.1. “Joint control” vs. “separate control” 72
 - A. Joint control 72
 - B. Separate control 74
 - C. Decisive factor 75
 - 3.2. The typology of Olsen and Mahler 76
 - A. Single controller 77
 - B. Collaborating single controllers 77
 - C. Partly joint controllers 78
 - D. Full scope joint controllers 79
 - 3.3. The arrangement between joint controllers 79

Chapter 5.**Liability Exposure of Controllers and Processors 83**

1.	Directive 95/46: “strict” liability for controllers	83
1.1.	Controller liability	84
A.	The nature of controller obligations	84
B.	A non-delegable duty of care	85
C.	Burden of proof.	88
D.	Defences.	90
E.	Eligible damages.	94
1.2.	Processor liability.	95
A.	Failure to implement controller instructions.	96
B.	Acting outside of processing mandate	97
1.3.	Multiple controllers	97
A.	Separate controllers	98
B.	Joint controllers	100
2.	The GDPR: “cumulative” liability for controllers and processors	103
2.1.	Controller liability	103
A.	The nature of controller obligations	103
B.	Non-delegable duty of care	104
C.	Burden of proof.	104
D.	Defences.	105
E.	Eligible damages.	107
2.2.	Processor liability.	108
A.	The nature of processor obligations.	108
B.	Proportional liability	109
C.	Burden of proof.	111
D.	Defences.	112
E.	Sub-processing	112
F.	Eligible damages.	113
2.3.	Multiple controllers	113
A.	Separate controllers	113
B.	Joint controllers	113
C.	Apportioning liability	114
3.	Conclusion	114

Chapter 6.**Specific Issues. 117**

1.	Individuals within organisations	117
2.	Branches, departments and subsidiaries	121
A.	An (over)emphasis on legal personality?	122
B.	Corporate concerns	126
C.	Governmental bodies.	128

3.	The role of “third parties” and “recipients”	129
A.	Third party.....	129
B.	Recipient	132
C.	Importance of the distinction	134
D.	A “third group” among those processing personal data?.....	135
4.	Sub-processing	136
A.	Directive 95/46	136
B.	GDPR	138

Chapter 7.

Additional Functions of the Controller and Processor Concepts.	141
---	-----

1.	Territorial scope	141
2.	Compliance with substantive provisions	143
2.1.	Transparency of processing	143
2.2.	Data subject rights	143
2.3.	Balance of interests	144
2.4.	Legal binding	144

Chapter 8.

Conclusion	145
-------------------------	-----

PART III.

HISTORICAL-COMPARATIVE ANALYSIS	149
--	-----

Chapter 1.

Introduction.	151
----------------------------	-----

Chapter 2.

The Emergence of Data Protection Law	155
---	-----

1.	Historical context	155
2.	Rationale	156
3.	Goals of data protection regulation	157
4.	National and international development	160

Chapter 3.

National Data Protection Laws before 1980	163
--	-----

1.	The Hesse Data Protection Act (1970)	163
1.1.	Origin and development	163
1.2.	Scope	165
1.3.	Basic Protections	166
A.	Protection of data	166

B. Rights for individuals	167
C. Access to information by legislature	167
D. Data Protection Commissioner	168
1.4. Allocation of responsibility and liability	168
1.5. Conclusion	173
2. The Swedish Data Act (1973)	174
2.1. Origin and development	174
2.2. Scope	177
2.3. Basic Protections	178
A. Prior authorization	178
B. Duties of a “responsible keeper”	180
C. Data Inspection Board	182
2.4. Allocation of responsibility and liability	183
2.5. Conclusion	186
3. The French Law on Informatics, Files and Liberties (1978)	188
3.1. Origin and development	188
3.2. Scope	190
3.3. Basic protections	191
A. Prior consultation or declaration	192
B. Data processing requirements	194
C. Data subject rights	198
D. National Committee on Informatics and Liberties (CNIL) ..	199
3.4. Allocation of responsibility and liability	200
3.5. Conclusion	206

Chapter 4.

International Instruments	207
1. Introduction	207
2. The OECD Guidelines (1980)	208
2.1. Origin and development	208
2.2. Scope	209
2.3. Basic protections	210
A. Basic principles of national application	210
B. Basic principles of international application	213
C. National implementation	213
D. International co-operation	214
2.4. Allocation of responsibility and liability	214
2.5. Conclusion	219
3. Convention 108 (1981)	220
3.1. Origin and development	220
3.2. Scope	222
3.3. Basic protections	223

A. Basic principles for data protection	223
B. Transborder data flows	225
C. Mutual assistance	226
3.4. Allocation of responsibility and liability	226
3.5. Conclusion	229

Chapter 5.

National Data Protection Laws after 1981 231

1. United Kingdom (1984)	231
1.1. Origin and development	231
1.2. Allocation of responsibility and liability	234
A. The Younger Committee	234
B. The Lindop Committee	236
C. The 1984 Data Protection Act.	240
i. Data user	240
ii. Computer bureau.	243
iii. Distinguishing “users” from “bureaux”	244
iv. Allocation of responsibility and liability	247
1.3. Conclusion	251
2. Belgium (1992)	252
2.1. Origin and development	252
2.2. Allocation of responsibility and liability	254
A. “Controller of the file”	254
B. “Processor”	258
C. Civil and criminal liability	259
2.3. Conclusion	260

Chapter 6.

Directive 95/46/EC 261

1. Origin and development	261
2. Allocation of responsibility and liability	263
2.1. Legislative development	263
A. Commission proposal	263
B. First reading European Parliament	266
C. Amended EC proposal.	269
D. Council position	272
E. Second reading and final text	275
2.2. Conclusion	276

Chapter 7.**General Data Protection Regulation. 279**

1.	Origin and development	279
2.	Allocation of responsibility and liability	282
2.1.	Legislative development	282
A.	Commission proposal	282
i.	Definitions	283
ii.	Obligations	283
iii.	Liability and sanctions	287
iv.	Assessment	288
B.	First Reading European Parliament	292
i.	Definitions	293
ii.	Obligations	296
iii.	Liability and sanctions	300
iv.	Assessment	301
C.	General approach of the Council.	302
i.	Definitions	303
ii.	Obligations	303
iii.	Liability and sanctions	305
iv.	Assessment	307
D.	Trilogue and final text	310
i.	Definitions	311
ii.	Obligations	311
iii.	Liability and sanctions	314
iv.	Assessment	316
2.2.	Conclusion	317
A.	Controller accountability	317
B.	Enhanced obligations for processors.	319
C.	Relationship between joint controllers	321
D.	Cumulative liability	321

Chapter 8.**Conclusion 325**

1.	Introduction	325
2.	Development of the controller concept	325
2.1.	The meaning of “control”	325
2.2.	National laws before 1980.	326
2.3.	International instruments	328
2.4.	National laws after 1981	330
2.5.	Directive 95/46 and the GDPR.	331

3.	Development of the processor concept.	334
3.1.	National laws before 1980.	334
3.2.	International instruments	336
3.3.	National laws after 1981	337
3.4.	Directive 95/46 and the GDPR.	338
A.	Directive 95/46	338
B.	GDPR	339

PART IV.

USE CASES.	341
-----------------	-----

Chapter 1.

Introduction.	343
--------------------	-----

Chapter 2.

E-Government Identity Management.	347
--	-----

1.	Introduction	347
2.	Actors.	350
2.1.	Citizen	352
2.2.	Authoritative source	353
2.3.	Credential Service Provider	355
2.4.	Integrator.	356
2.5.	Verifier.	358
2.6.	Relying party	359
3.	Roles.	359
3.1.	Citizen	360
3.2.	Authoritative source	361
3.3.	Credential Service Provider	362
3.4.	Integrator.	364
3.5.	Verifier.	366
3.6.	Relying party	366
4.	Allocation of responsibility and liability	367
5.	Practical examples.	368
5.1.	Internal Market Information System (IMI).	368
A.	Introduction	368
B.	Functionalities	370
C.	IMI actors	371
D.	Roles	372
E.	Responsibilities.	375
i.	Confidentiality and security	375
ii.	Data quality	377
iii.	Retention of data	378

iv. Transparency	379
v. Data subject rights	381
5.2. Cross-border identification and authentication (Stork and eIDAS)	382
A. Introduction	382
B. Functionalities	385
C. Actors	386
D. Roles	388
E. Responsibilities	389
6. Evaluation	391

Chapter 3.

Online Social Networks

1. Introduction	395
2. Actors	395
2.1. OSN user	397
2.2. OSN Provider	398
2.3. Page administrator	400
2.4. (Third-party) application provider	401
2.5. (Third-party) tracker	402
2.6. (Third-party) data broker	405
2.7. (Third-party) website operator	406
2.8. Other observers	408
2.9. Infrastructure (service) provider	409
3. Roles	409
3.1. OSN provider	409
3.2. OSN users	413
3.3. Page administrators	417
A. Questions referred	417
B. Opinion of the Advocate General	419
C. Holding of the CJEU	422
3.4. Application providers	426
3.5. Third-party website operators	429
A. Questions referred	429
B. Opinion of Advocate General Bot	431
C. Opinion of Advocate General Bobek	432
3.6. Other actors	438
4. Allocation of responsibility and liability	439
4.1. Transparency	439
4.2. Legitimacy	441
A. OSN provider	441
B. Application provider	443

C. OSN user	444
D. Assessment	444
4.3. Data accuracy	445
4.4. Confidentiality and security	446
A. OSN provider	446
i. Privacy-friendly default settings	446
ii. Access by third-party apps	448
B. Application provider	449
C. OSN user	449
4.5. Data subject rights	450
A. OSN Provider	450
B. Application provider	451
C. User	452
5. Evaluation	452
5.1. Scope of the personal use exemption	452
5.2. Control over user-generated content	455
5.3. Responsibilities of platform providers	458
5.4. Joint control, joint responsibilities?	460
Chapter 4.	
Cloud Computing	467
1. Introduction	467
2. Actors	472
2.1. Cloud customer and end-user	474
2.2. Cloud provider	474
A. Application provider (SaaS)	474
B. Platform provider (PaaS)	476
C. Infrastructure provider (IaaS)	478
3. Roles	479
3.1. Cloud customers and end-user	479
3.2. Cloud provider	482
A. Application providers (SaaS)	484
B. Platform provider (PaaS)	486
C. Infrastructure provider (IaaS)	488
4. Allocation of responsibility and liability	490
4.1. Transparency	490
4.2. Data quality	491
A. Purpose specification and use limitation	491
B. Retention of data	492
4.3. Confidentiality and security	493
4.4. Data subject rights	497
4.5. International transfers	497

5.	Evaluation	499
5.1.	Threshold for control	499
5.2.	Design of cloud services	503
5.3.	Networked data processes	506
5.4.	Hosting services	507
 Chapter 5.		
	Internet Search Engines.	511
1.	Introduction	511
2.	Actors	513
2.1.	Search engine provider	515
2.2.	Website publishers and content providers	518
2.3.	End-users	519
2.4.	Infrastructure (service) providers	520
3.	Roles	521
3.1.	Search engine provider	521
A.	Question referred in Google Spain	521
B.	Oral arguments	521
C.	Opinion of the Article 29 Working Party	523
D.	Opinion of the Advocate-General	524
E.	Holding of the CJEU	527
3.2.	Website publishers and content providers	528
3.3.	End-user	529
3.4.	Infrastructure (service) providers	530
4.	Allocation of responsibility and liability	530
4.1.	Lawfulness	531
4.2.	Principles relating to the processing of personal data	532
A.	Purpose specification and use limitation	532
B.	Data minimisation	533
C.	Accuracy	535
4.3.	Transparency	536
4.4.	Confidentiality and security	537
4.5.	Right to object and to erasure	538
5.	Evaluation	539
5.1.	True to both letter and spirit	539
5.2.	Absence of knowledge or intent	542
5.3.	Shooting the messenger?	544
5.4.	Scope of obligations of search engine providers	546
5.5.	Impact on freedom of expression	552

PART V.	
RECOMMENDATIONS	553

Chapter 1.

Introduction.....	555
-------------------	-----

Chapter 2.

Typology of Issues.....	557
-------------------------	-----

1. Introduction	557
2. Grammatical.....	558
2.1. “Determines”	558
2.2. “Purpose”	560
2.3. “And”	561
2.4. “Means”	563
2.5. “Alone or jointly with others”	566
2.6. “The processing”	567
2.7. “Of personal data”	569
2.8. “On behalf of”	570
3. Teleological.....	572
3.1. Continuous level of protection	573
3.2. Legal certainty	576
3.3. Effective and complete protection.....	577
4. Systemic.....	578
4.1. Transparency and data subject rights.....	579
4.2. Scope of obligations.....	580
4.3. Implications of joint control.....	581
4.4. Legal binding	582
5. Historical.....	584
5.1. The democratisation of “control”	585
5.2. Control over user-generated content	588

Chapter 3.

Typology of Solutions.....	589
----------------------------	-----

1. Introduction	589
2. Grammatical.....	590
2.1. Deletion of “means”.....	590
2.2. Adding “conditions”	592
2.3. “Benefit-based” approach	593
2.4. Assessment	594
3. Teleological.....	597
3.1. Abolition of the distinction	597

3.2. Obligations for processors	600
3.3. Assessment	603
A. Abolition of the distinction	603
i. Equal distribution (joint and several liability)	604
ii. Role-based accountability (proportional liability)	606
iii. Combined approach (general and proportional liability)	607
iv. Interdependencies	609
B. Obligations for processors	609
C. Internal comparison	610
i. Standards vs. rules	611
ii. Optimal specificity of legal rules	612
iii. Implications for data protection law	615
iv. Implications for the controller-processor model	616
D. Final text GDPR	619
4. Systemic	622
4.1. Partial assimilation	622
4.2. Greater recognition of joint control	624
4.3. “No wrong door” and “Single point of contact”	625
4.4. Tailoring obligations	626
4.5. Contractual flexibility	629
4.6. Assessment	630
5. Historical	632
5.1. Personal use exemption	632
5.2. Liability exemptions of the E-Commerce Directive	635
5.3. Assessment	636
 Chapter 4.	
Recommendations	639
1. Abolish the concepts or revise the definitions	639
1.1. Abolishing the concepts	640
1.2. Revising the definitions	641
2. Use of standards and exemptions	642
3. Require data protection by design from “processors”	642
4. Enhance contractual flexibility	644
5. Expand the scope of the personal use exemption	647
 Chapter 5.	
Conclusion	651
 <i>Bibliography</i>	<i>655</i>

