

## 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 Associate 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



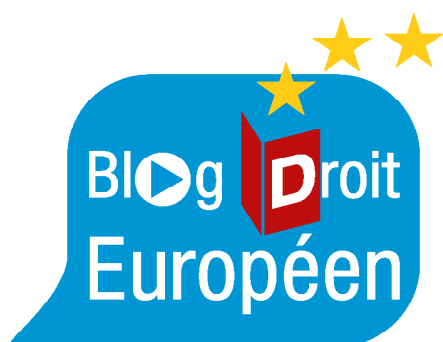
9 782919 956302

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



### **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/p60BGR-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/p60BGR-2QK>

Disponible sur Internet : <https://wp.me/p60BGR-2QK>

ISBN 978-2-9199563-0-2



Attribution-NonCommercial-NoDerivs 2.0 Generic (CC BY-NC-ND 2.0)



# 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

---

<b>List of Abbreviations</b>	<b>14</b>
<b>Introduction to the Editors</b>	<b>18</b>
<b>Introduction to the Contributors</b>	<b>19</b>
<b>Acknowledgements</b>	<b>23</b>
<b>Opening Remarks</b>	<b>24</b>
by <a href="#">Dr. Olivia Tambou</a>	
<b>I - The visibility of the European Model of Data protection proposed by the GDPR</b>	
<b>II- The current lack of readability of this European Model</b>	
A-The General Nature of the GDPR	
B- The Complicated Nature of the National Adaptations of the GDPR	

---

<b>Part 1: Illustrations of the Diversity of the National Adaptations of the GDPR</b>	<b>28</b>
---	-----------

---

<b>The New Federal Data Protection Act – Implementation of the GDPR in Germany</b>	<b>29</b>
by <a href="#">Dr. jur. Christian L. Geminn</a>	
<b>I-Introduction</b>	
<b>II-Data Protection Law in Germany</b>	
<b>III-The New Federal Data Protection Act</b>	
A-Structure	
B-Scope of the Act	
C-Opening clauses and regulatory mandates of the GDPR	
D-Areas of particular interest	
1) Data processing for employment-related purposes	
2) Video surveillance	
3) Supervisory authorities	
4) Restrictions on the rights of the data subject	
5) Data protection officers	
6) Representation of data subjects	
7) Processing of special categories of personal data	
8) Scoring	
9) Penal provisions and fines	
<b>IV-Conclusion</b>	
<b>V-Outlook</b>	



---

**TABLE OF CONTENTS**
**Austrian Adaptation of the GDPR** 35  
 by Dr. Günther Leissler LL.M., Mag. Patrizia Reisinger, Mag. Janos Böszörményi

- I- The origins of data protection in Austria
- II- National culture of data protection in Austria
- III- Adoption of national law to supplement the GDPR
- IV- Main Provisions at national level in Austria

**The Swedish measures accompanying the GDPR** 42  
 by Dr. Patricia Jonason

- I-Introduction
- II-The scheme of the Swedish data protection act
  - A-The content of the Data Protection Act (2018:218)
  - B-The scope of the new Act
  - C-The relationship to the GDPR
- III-The impact of the new European data protection legislation on Swedish law
  - A-The relationship between the GDPR and the freedom of opinion
    - 1) The relationship between the right of access to official documents and the data protection legislation
    - 2) The relationship between the freedom of expression and the data protection rules
  - B-An increase of formalism
    - 1) The GDPR leads to fewer preliminary procedures
    - 2) The GDPR confirms the regulatory model
  - C-The improvement of the data subject's rights in regard to the Data Protection Authority
    - 1) The Right of the data subject to lodge a complaint and the obligation of the supervisory authority to examine the complaint
    - 2) The rights of the data subjects to judicial remedies against the supervisory authority
- IV-Conclusion

**The French Adaptation of the GDPR** 52  
 by Dr. Olivia Tambou

- I-Introduction
- II-The accelerated adoption of the New Data Protection Act
- III-The French approach of the national adaptation of the GDPR
- IV-The respect of the rationale of the GDPR reform
  - A-Strengthening the CNIL
  - B-Moderate uses of Margin of Manoeuvre
    - 1) Limitation of the Prior Formalities
    - 2) Provision on the Law Applicable in Cross-Border Cases
    - 3) A derogation for the Communication of Personal Data Breach
- V-Most disputed topics regarding the adoption of the New Data Protection Act
  - A-The Uses of the Openings Clauses in the Context of the Algorithmic Decisions

## TABLE OF CONTENTS

- 1) General Legal Framework for the Implementation of the Individual Decisions Solely Based on Automated Processing
- 2) A Legal Basis for a Systematic Use of Administrative Individual Decisions Solely Based on Automated Processing
- B-The Impact of the GDPR on Specific Situations**
  - 1) The Need to Consider the Protection of the Child
  - 2) The Local and Regional Entities Concerns
- C-The “Qwant” Amendment**
- D-The Introduction of a Collective Action for Damage**
- E-The processing of personal data relating to criminal convictions and offences**
- VI-Conclusion**

### **The Danish Adaptation of the GDPR**

61

by [Tenna Overby](#)

- I-Introduction**
- II-The legal framework before the GDPR**
- III-The Data protection act project and the main content**
- IV-The material scope and geographical scope**
- V-The use of opening clauses**
  - A-Extension of public authorities’ right to access personal data
  - B-Restrictions of data subject rights
  - C-Processing for scientific research purposes
  - D-Minors’ consent in relation to information society services
- VI-Other key provisions**
  - A-Data Protection Officer
  - B-Independent Supervisory Authorities
  - C-Penalties
- VII-After the 25 May**

### **The GDPR Implementation in the Netherlands**

66

by [Paul Breibarth](#)

- I-Introduction**
- II-A new law, the same rules**
  - A-The legislative Process
  - B-Public Consultation
  - C-The House of Representatives
  - D-The Senate
- III-The National implementation of GDPR in the Netherlands**
  - A-The age of Consent
  - B-The Role and Independence of the Dutch Data Protection Authority
- IV-Next Steps**

---

**TABLE OF CONTENTS**

<b>The Irish Adaptation of the GDPR: The Irish Data Protection Act 2018</b>	<b>72</b>
by <a href="#">Dr. Maria Murphy</a>	

- I- Data protection Enforcement under Irish law
- II- Fines and Public Body exemption
- III- Children and the Irish Data Protection Act
- IV- Freedom of Expression Exemption
- V- Politics and Data Protection
- VI-Conclusion

<b>The Adaptation of the GDPR in Spain: The New Draft of the Data Protection Act</b>	<b>80</b>
by <a href="#">Dr. Cristina Pauner and Jorge Viguri</a>	

- I-Introduction.
- II-Legislative process. Key dates.
- III-Noteworthy aspects.
- IV-Digital Rights Charter.
- V-Critical aspects.
- VI-Conclusions

<b>Report on the harmonization of Italian Law with the enforcement of The GDPR</b>	<b>89</b>
by <a href="#">Monica A. Senor and Dr. Massimo Durante</a>	

- I-Introduction
- II-General provisions
  - A-The definition of “communication” and “dissemination”
- III-Principles
  - A-The lawful basis for the processing
  - B-Conditions applicable to child’s consent in relation to information society services
  - C-Processing of particular categories of personal data necessary for reasons of significant public interest
  - D-Safeguards measure for the processing of genetic data, biometric data or data concerning health
- IV-Rights of the data subject
- V-Data controller and data processor
  - A-Attribution of roles and tasks to designed subjects
  - B-Processing presenting specific risks for the performance of a task carried out in the public interest
- VI-Remedies, liability and penalties
- VII-Opening Clauses: a General Overview

<b>The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Rights</b>	<b>98</b>
by <a href="#">Dr. Alexia Pato</a>	

- I-Introduction
- II-Article 80 GDPR: An Interpretative Guide
- III-Country Breakdown
  - A-France

## TABLE OF CONTENTS

B-Belgium  
C-Spain  
D-Germany  
E-Austria  
F-The United Kingdom  
G-Dealing with National Adaptation Issues

**IV-Article 80 in Practice**

**V-Concluding Remarks**

---

## **Part 2: Illustrations of the international influence of the GDPR** **107**

---

### **UK: GDPR adaptations and preparations for withdrawal from the EU** **108**

by [Dr. Karen Mc Cullagh](#)

**I-Introduction**

**II-Rationale for enacting the Data Protection Act 2018**

A-Scope & Structure of the Data Protection Act 2018

B-General Observations

C-Uncontentious Aspects

- 1) Public authority & public task: definitions and exemptions
- 2) Continued registration with and payment of fees to the ICO
- 3) Stronger ICO investigatory & enforcement powers
- 4) Profiling and automated decision making

D-Contentious Aspects

- 1) A declaratory section on personal data
- 2) Child's consent in relation to information society services
- 3) Journalism exemption
- 4) Profiling by political parties
- 5) Henry VIII clause – sensitive data
- 6) No Collective redress without authority mechanism
- 7) Immigration exemption
- 8) Data Subject access to confidential references

**III-The data protection implications of Brexit**

A- Leaving the EU but retaining the GDPR

B- Potential transitional arrangements

C- Personal data transfers during a transition period

D- Data protection implications of 'No deal'

E- Prospects of a obtaining an adequacy decision

F- Impact on the ICO

**IV-Concluding remarks**

### **Data Protection in Switzerland: A Preview** **120**

by [François Charlet](#)

**I-The GDPR effects for Switzerland**

**II-Conclusion**

---

### TABLE OF CONTENTS

<b>The impact of the GDPR in Japan</b>	<b>122</b>
by <a href="#">Hiroshi Miyashita</a>	

I-GDPR in Japan

II-Amendments to Data protection legislations in 2015

III-EU- Japan Mutual Adequacy Strategy

IV-The PPC's supplementary rules

V-The fate of mutual adequacy

---

<b>Annex: List of the studied national laws for the adaptation of the GDPR</b>	<b>128</b>
--	------------

---

## LIST OF ABBREVIATIONS

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Agency)
AIQ	AggregatelQ 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
BGBI	Bundesgesetzblatt
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BNDG	Bundesnachrichtendienstgesetz
BR	Bundesrat
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
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

# 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](mailto:pauner@uji.es)



### By Jorge Viguri

PhD researcher in Constitutional Law at the Universitat Jaume I of Castellón (UJI). For correspondence [jviguri@uji.es](mailto: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<sup>1</sup>. The Organic Law 5/1992, of 29<sup>th</sup> 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<sup>2</sup>. 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.<sup>3</sup>

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

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.

<sup>3</sup>The Royal Decree-Law 5/2018, of July 27<sup>th</sup> 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.

<sup>1</sup> VVAA, *20 años de Protección de Datos en España*, AEPD, 2015.

<sup>2</sup> 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

## 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.<sup>4</sup> 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<sup>5</sup>, 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<sup>6</sup>. 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)<sup>7</sup> at the behest of the Ministry of Justice. The APLOPD was followed by the mandatory impact reports<sup>8</sup> and the consequent opinion of the

4 In the words of the Court of Justice, the principle of legal certainty obliges 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 LOPD-GDD, 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](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](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-Disposi->

Council of State<sup>9</sup>. On 24 November 2017, the new draft LOPD was presented for the corresponding parliamentary procedure<sup>10</sup>.

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<sup>11</sup> 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<sup>12</sup> 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 LOPD-GDD was published in the Official State Gazette on 6 December and entered into force on 7 December 2018.

[tion&blobheadervalue1=attachment%3B+filename%3DMAIN.PDF](http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/3.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](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#\(P%3%A1gina1\)](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%3%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=%28D-SCD-12-PL-104.CODI.%29#\(P%3%A1gina28\)](http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28D-SCD-12-PL-104.CODI.%29#(P%3%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](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<sup>13</sup>.

**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 6<sup>th</sup> Additional Provision. It sets a minimum financial limit for the inclusion

<sup>13</sup> 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*”<sup>14</sup> (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<sup>15</sup>. 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

<sup>14</sup> 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/>

<sup>15</sup> 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.

of October 7, 2016, for a Digital Republic<sup>16</sup>, the “Right to Disconnect” recognised in the French Labour Code<sup>17</sup> or the Declaration of Internet Rights in Italy.<sup>18</sup>

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.<sup>19</sup> 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

<sup>16</sup> *Loi n° 2016-1321, du 7 octobre 2016, pour une République numérique* (<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORF-TEXT000033202746&dateTexte=&categorieLien=id>).

<sup>17</sup> 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”.

<sup>18</sup> [http://www.camera.it/application/xmanager/projects/leg17/commissione\\_internet/testo\\_definitivo\\_inglese.pdf](http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf)

<sup>19</sup> 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 providers or 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 news 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**.<sup>20</sup> 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<sup>21</sup>. This legal uncertainty could undermine their effective implementation as it is not fully regulated in the GDPR nor in the current LOPD<sup>22</sup>.

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<sup>23</sup>.

<sup>21</sup> 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/esque-ma-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.

<sup>22</sup> 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?\\_pir ef73\\_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](http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_pir ef73_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, Parliamentarian 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](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))

<sup>23</sup> 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*

<sup>20</sup> 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.



### 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) subparagraphs 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).<sup>24</sup> 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*.<sup>25</sup> 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 through 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.

<sup>24</sup> 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.

<sup>25</sup> ECHR, 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 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 an 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 LODPGDD 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”.<sup>26</sup>

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”.<sup>27</sup> 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<sup>28</sup>, which mark a very important step for extra legal certainty in a key sector for the consistent implementation of the data protection legislation.

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

<sup>27</sup> *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>

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

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



### By Monica A Senior

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](mailto: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”<sup>1</sup>.

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<sup>2</sup>. 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

<sup>1</sup> 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.

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