Codes of (Mis)conduct? An Appraisal of Articles 40-41 GDPR in View of the 1995 Data Protection Directive and its Shortcomings

Carl Vander Maelen

Ghent University – Faculty of Law

Research group Law & Technology[1]

In its articles 40 and 41, the General Data Protection Regulation (GDPR) proposes the use of codes of conduct to help private actors demonstrate data protection accountability, as well as to aid with the implementation of the Regulation. However, the emphasis that the GDPR places on these soft law instruments is somewhat remarkable since both the EU and legal scholars concluded that article 27 of the 1995 Data Protection Directive, as the legislative predecessor to articles 40 and 41 GDPR, failed to make codes of conduct a key element of European data protection practices. This contribution seeks to investigate why the 1995 Directive was unsuccessful and, on the basis of those findings, attempts to formulate informed predictions on what any similarities and differences between article 27 DPD and articles 40-41 GDPR might tell us about the future course of codes of conduct under the GDPR.

I. Introduction

As our digital economy raises issues as complex and diverse as free speech in a networked information environment[2] and deceptive data collection practices,[3] (supra)national governments are ramping up

[1] The author is grateful for the comments received during the PLSC Europe 2019 conference in Amsterdam.

[2] Julie E Cohen, 'Law for the Platform Economy' (2017) 51 UC Davis Law Review 133, 161.

[3] Facebook was accused of deceptive data gathering through the 'Facebook Research' VPN app. See: Josh Constine, 'Facebook Pays Teens to Install VPN That Spies on Them' *TechCrunch* (29 January 2019) <http://social.techcrunch.com/2019/01/29/facebook-project-atlas/> accessed 6 February 2019. Google allegedly did so through the 'Screenwise Meter' app. See: Zack Whittaker, Josh Constine and Ingrid Lunden, 'Google Will Stop Peddling a Data Collector through Apple's Back Door' *TechCrunch* (30 January 2019) <http://social.techcrunch.com/2019/01/30/googles-also-peddling-a-data-collector-through-apples-back-door/> accessed 5 February 2019.

their efforts to regulate tech companies.[4] Yet, the rapidly-evolving and highly technical nature of the information and communication technology (ICT) sector strains the effectiveness of traditional legislation. Due to the ponderous and time-consuming nature of the legislative process, legislation has difficulty keeping pace with the rapid and unexpected evolutions of technological innovation (the pacing problem)[5] while regulators do not always possess the required knowledge to make informed decisions on complex technological matters, nor can they realistically be expected to have such knowledge (the knowledge problem).[6] Both issues also reinforce each other[7] and the legislation produced as a result may have a chilling effect on innovation (instrument failure),[8] causing high opportunity costs,[9] as well as compliance costs that potentially scare off existing actors and demoralise new market entrants.[10]

For quite some time now, regulators are influenced by the 'new governance' school of thought and the prospect of achieving 'smart regulation',[11] increasingly causing them to turn to alternative regulatory instruments (ARIs). These are methods of rulemaking that nuance the role of government institutions by involving private actors (such as NGOs, enterprises or industry associations) in all or a number of stages of the regulatory process.[12] Such multi-stakeholder involvement not only helps manage the

[4] Evelyn Douek, 'Two Calls for Tech Regulation: The French Government Report and the Christchurch Call' (*Lawfare*, 18 May 2019) <https://www.lawfareblog.com/two-calls-tech-regulation-french-government-report-and-christchurch-call> accessed 20 May 2019; Damien Cave, 'Australia Passes Law to Punish Social Media Companies for Violent Posts' *The New York Times* (4 April 2019) <https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html> accessed 20 May 2019; Karishma Vaswani, 'Concern over Singapore's Anti-Fake News Law' (4 April 2019) <https://www.bbc.com/news/business-47782470> accessed 20 May 2019.

[5] Jonathan Cave, Chris Marsden and Steve Simmons, 'Options for and Effectiveness of Internet Self- and Co-Regulation' (RAND Santa Monica 2008); Sofia Ranchordás, 'Does Sharing Mean Caring: Regulating Innovation in the Sharing Economy' (2015) 16 Minnesota Journal of Law Science & Technology 413.

[6] Julie E Cohen, 'The Regulatory State in the Information Age' (2016) 17 Theoretical Inquiries in Law 397; Daniel J Gervais, 'The Regulation of Inchoate Technologies' (2010) 47 Houston Law Review 665. See already in 1959 the article by Lindblom: Charles E Lindblom, 'The Science of "Muddling Through"' (1959) 19 Public Administration Review 79.

[7] See for example the admission by the US Department of Transportation that private actors are outpacing the department's technical knowledge: US Department of Transportation (DOT) – National Highway Traffic Safety Administration (NHTSA), 'Request for Comment on Federal Automated Vehicles Policy' (*Federal Register*, 23 September 2016) <https://www.federalregister.gov/documents/2016/09/23/2016-22993/request-for-comment-on-federal-automated-vehicles-policy> accessed 28 February 2019.

[8] Julia Black, 'Critical Reflections on Regulation (CARR Discussion Papers (DP 4))' (2002).

[9] Jerry Ellig and Patrick A McLaughlin, 'The Quality and Use of Regulatory Analysis in 2008' (2012) 32 Risk Analysis 855; Peter Huber, 'The Old-New Division in Risk Regulation' (1983) 69 Virginia Law Review 1025, 1027.

[10] Daniel Mândrescu, 'Applying EU Competition Law to Online Platforms: The Road Ahead - Part 2' (2017) 38 European Competition Law Review 410; Julie Brill, 'The Intersection of Consumer Protection and Competition in the New World of Privacy' (2011) 7 CPI Journal 18 <https://ideas.repec.org/a/cpi/cpijrn/7.1.2011i=5928.html> accessed 20 December 2019.

[11] Neil Gunningham and Joseph Rees, 'Industry Self-Regulation: An Institutional Perspective' (1997) 19 Law & Policy 363.

[12] Depending on the position of a specific ARI on the regulatory continuum; see below.

complexity of multi-actor interactions in the regulatory process, but also takes advantage of the diversity in knowledge and resources that a plurality of stakeholders possess.[13] The terms 'self-regulation' and 'co-regulation' are often used to describe such alternative regulatory constructions, but the conceptual choice for the term ARIs is made due to the impossibility of objectively classifying the extremely broad range of tools that allow for the decentralisation of regulatory authority among public, private and public-private actors and institutions (i.e. a positive definition of the broad range of forms in which ARIs can manifest themselves)[14] while on the other hand it more clearly portrays the status of such tools as any instrument that offers an 'alternative' to traditional top-down command-and-control state-issued legislation (i.e. a negative definition of what ARIs are not).[15] In fact, ARIs can be situated along a fluid 'regulatory continuum' according to the involvement of each actor and their respective roles in the creation, implementation and enforcement of rules,[16] with only the two extremities ('law' and 'self-regulation') serving as fixed points.

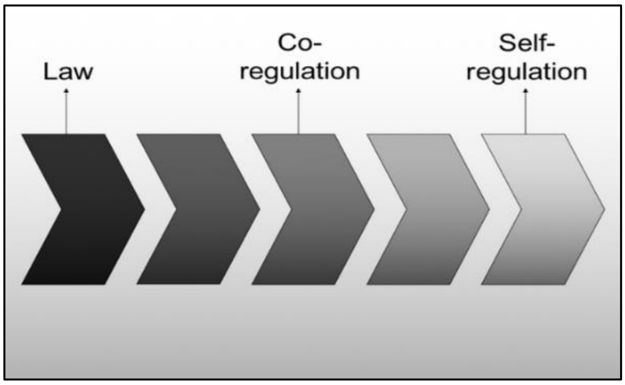

Fig. 1. The regulatory continuum.[17]

[13] Christopher Marsden and others, 'D4.1 Outline Overviews of Tasks R4.1-R4.4: Regulatory and Governance Methodologies' (European Commission 2013) 20.

[14] Eva Lievens, 'The Use of Alternative Regulatory Instruments to Protect Minors in the Digital Era: Applying Freedom of Expression Safeguards' (2011) 29 Netherlands Quarterly of Human Rights 164, 171; Kenneth W Abbott, 'Introduction: The Challenges of Oversight for Emerging Technologies', *Innovative Governance Models for Emerging Technologies* (2013) 6.

[15] See tool #18 in: European Commission, 'Better Regulation "Toolbox"'.

[16] Tony Prosser, 'Self-Regulation, Co-Regulation and the Audio-Visual Media Services Directive' (2008) 31 Journal of Consumer Policy 99, 101; Gunningham and Rees (n 11) 366; Darren Sinclair, 'Self-Regulation Versus Command and Control? Beyond False Dichotomies' (1997) 19 Law Policy 529, 532. See also the 'Beaufort scale of self-regulation': Jonathan Cave, Chris Marsden and Steve Simmons, 'Options for and Effectiveness of Internet Self- and Co-Regulation (Study for RAND Europe)' (RAND Europe 2008) TR-566-EC 27. See also the remark that soft law instruments are 'part of a continuum – from hard law through soft law, to political and social undertakings, and finally to the absence of any obligation' in: Kenneth W Abbott, Gary E Marchant and Elizabeth A Corley, 'Soft Law Oversight Mechanisms for Nanotechnology' (2012) 52 Jurimetrics 279.

[17] Eva Lievens, *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments* (Martinus Nijhoff Publishers 2010) 229.

Although the use of ARIs can result in a risk of 'regulatory bias' where industry actors only regulate those aspects that are advantageous to themselves[18] and attention must be paid to adequate oversight and enforcement to avoid free riders,[19] the decentralisation of authority that takes place when wielding ARIs allows more flexibility and speed in the adoption and revision of such instruments as compared to formal regulation and its strict government-based standardised procedures and structures.[20]

The use of ARIs also forms one of the pillars of the European Commission's policy to achieve a higher quality and lower quantity of regulation (the 'Better Regulation Agenda')[21] as can be seen from the acknowledgement of their benefits and recommendations on their use in a range of initiatives and documents, such as the Commission White Paper on Governance,[22] the 2003[23] and 2016 Interinstitutional agreements on better lawmaking,[24] the Better Regulation Guidelines[25] and its accompanying toolbox.[26] As a result, the EU increasingly integrates ARIs in legislation to allow for private stakeholder participation in the implementation and enforcement processes of those hard law instruments. A major example thereof is the General Data Protection Regulation (GDPR) which modernises the EU's previous personal data protection framework established in the 1995 Data Protection Directive (the 1995 Directive or DPD). The 1995 Directive already pioneered the use of ARIs by encouraging the use of codes of conduct in its article 27, but the GDPR further develops this by offering additional and more detailed provisions on codes in its articles 40 and 41.

[18] Benjamin P Edwards, 'The Dark Side of Self-Regulation' (2017) 85 University of Cincinnati Law Review 573, 608–610; Jilian Segal, 'Institutional Self-Regulation: What Should Be the Role of the Regulator? (Address to the National Institute for Governance Twilight Seminar, Canberra)'.

[19] Bert-Jaap Koops and others, 'Should Self-Regulation Be the Starting Point?', *Starting Points for ICT Regulation : Deconstructing Prevalent Policy One-liners* (2006) 125; Angela Campbell, 'Self-Regulation and the Media' (1999) 51 51 Federal Communications Law Journal 711 (1999).

[20] Ryan Hagemann, Jennifer Skees and Adam D Thierer, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (2019) 17 Colorado Technology Law Journal 37, 41; Abbott (n 14). This is not per se meant as a critique aimed at traditional legislation; in fact, this rigid, deliberate and predictable process is essential to their legitimacy and arguably their greatest strength.

[21] Inge Govaere and Sasha Garben, 'The Multi-Faceted Nature of Better Egulation', *The EU better regulation agenda : a critical assessment* (Hart Publishing 2018); European Commission, 'European Governance: Better Law-Making COM(2002)275 Final'; Adrienne Héritier, 'New Modes of Governance in Europe: Policy-Making Without Legislating?', *Common Goods: Reinventing European and International Governance* (2002).

[22] European Commission, 'European Governance: A White Paper'.

[23] European Parliament, Council of the European Union and Commission of the European Communities, '2003 Interinstitutional Agreement on Better Law-Making'.

[24] European Parliament, Council of the European Union and Commission of the European Communities, '2016 Interinstitutional Agreement on Better Law-Making'.

[25] European Commission, 'Better Regulation Guidelines'.

[26] European Commission, 'Better Regulation Toolbox'.

Although there is no universally accepted definition of what codes of conduct are – which is the case for most ARIs due to their fluidity[27] – we can construct a working definition based upon several elements common to scholarly work on the topic: codes of conduct aim to stipulate the desirability of a certain conduct by States, international or non-governmental organisations or private associations and persons,[28] with codes aimed at corporations specifically seeking to enhance the accountability of such corporate actors in the (international) marketplace[29] by defining voluntary standards and principles to steer the behaviour of similar types of enterprises (i.e. a certain sector).[30]

Articles 40-41 GDPR are aimed at associations and other bodies representing categories of controllers or processors (article 40 paragraph 2) and state that codes are 'intended to contribute to the proper application [of the GDPR]' by specifying the concrete application of the GDPR's data protection principles, rights and obligations. Such codes are subjected to the approval of a supervisory authority (namely the national supervisory authority or the European Data Protection Board; this division will be elucidated later) and must also be accompanied by monitoring mechanisms. The European legislator thus clearly considers codes important tools to help implement the main provisions of the GDPR,[31] while also emphasising the value for enterprises by stating that codes can help demonstrate GDPR compliance and thereby lead to the mitigation or avoidance of fines,[32] while also raising the trust of data subjects and resulting in more legal certainty for sectorial processing practices.[33]

However, the emphasis that the GDPR places anew on codes of conduct is somewhat remarkable since several sources concluded that article 27 of the 1995 Directive as the legislative predecessor to

[27] See the European Commission's remark that "it is often hard to define the exact nature of a given soft regulatory approach": European Commission, 'Better Regulation "Toolbox"' (n 15) 88. See also how the Article 29 Working Party equates 'recommended practices' to codes of conduct in Article 29 Working Party, 'Working Document on IATA Recommended Practice 1774 Protection for Privacy and Transborder Data Flows of Personal Data Used in International Air Transport of Passengers and of Cargo' 3. The terms 'codes of conduct' and 'codes of ethics' are used interchangeably by consultancy behemoth Deloitte: Deloitte, 'Suggested Guidelines for Writing a Code of Ethics/Conduct'.

[28] Jürgen Friedrich, 'Codes of Conduct', *Max Planck Encyclopedias of International Law* (2010).

[29] Helen Keller, 'Corporate Codes of Conduct and Their Implementation: The Question of Legitimacy', *Legitimacy in International Law* (Springer 2008) 4.

[30] Neil Robinson and others, 'Review of EU Data Protection Directive: Summary' (Information Commissioner's Office 2009); Organisation for Economic Co-operation and Development, 'Codes of Corporate Conduct: An Inventory, Working Party on the Trade Committee, TD/TC/WP(98)74/Final'.

[31] European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679'.

[32] Article 83, 2 (j) GDPR.

[33] UK Information Commissioner's Office, 'Codes of Conduct'.

articles 40 and 41 GDPR failed to make self-regulatory and co-regulatory mechanisms key elements of European data protection practices,[34] begging the question as to which elements of the 1995 Directive's approach to codes were (un)successful and why (section 2). On the basis thereof, we can make informed predictions on what any similarities and differences between article 27 DPD and articles 40-41 GDPR might tell us about how codes will be employed under the GDPR and whether this charts a different course from the DPD (section 3).

This research was conducted using a desk research method. However, a lack of scholarly legal work on the topic of codes of conduct under both the 1995 Directive and the GDPR was quickly encountered. As a result, this research instead consulted and analysed reports on the implementation of the DPD, policy documents by the EU and the text of the DPD and the GDPR. For that reason, this paper should not be considered, nor does it aim to be, a definitive evaluation of DPD-based and GDPR-based codes. For the GDPR in particular, more codes must first come to fruition, which can only happen once stakeholders become fully comfortable with the new processes created by the GDPR. Additionally, reports on the implementation of the DPD by Korff[35] and Robinson et al.[36] show that a vital part of the approval procedure that a code must undergo consists of informal contact between the regulatory authorities and bodies representing categories of controllers or processors, both on the national level and that of the EU. My doctoral research will attempt to capture such processes through an empirical analysis of corporate documents and semi-structured interviews with stakeholders such as data protection authorities (DPAs), the European Data Protection Board (the EDPB) and corporate policy advisors to come to a more holistic view of the *ex ante* procedures and *ex post* effects tied to GDPR-based codes of conduct.

II. Codes of conduct under the 1995 Directive: a regulatory success story?

An investigation into the approach that the 1995 Directive took regarding codes of conduct in its article 27 can help us gain valuable insights as to how ARIs in the context of the EU's personal data protection

[34] Neil Robinson and others, 'Review of the European Data Protection Directive' (RAND Europe 2009) 9–10; LRDP Kantor Ltd., 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments - Final Report' (European Commission 2010) 52–53. See also Korff, who notes that 'Codes do get adopted and (positively) "assessed" … but the process is often tortuous and the number of codes issued in this way is only limited' in: Douwe Korff, 'EC Study on the Implementation of Data Protection Directive - Report on the Findings of the Study' (European Commission 2002) 187.

[35] Korff (n 34).

[36] Robinson and others (n 34).

policy have been applied in the past. This, in turn, can allow us to make informed predictions about the course of the GDPR and codes adopted under its auspices, including whether they can make a valuable contribution to the proper application of the hard law instrument in which they are encapsulated – certainly since the European Commission noted itself in its 2010 'Communication on a comprehensive approach on personal data protection in the European Union' that 'current provisions on self-regulation in the Data Protection Directive, namely the scope for drawing up Codes of Conduct, have rarely been used so far and are not considered satisfactory by private stakeholders'.[37] Where did the DPD go 'wrong' and can the GDPR offer meaningful improvements? For the sake of reader convenience, the brief content of article 27 DPD is displayed in its entirety here:

> 1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
>
> 2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
>
> Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
>
> 3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

[37] European Commission, 'Communication on a Comprehensive Approach on Personal Data Protection in the European Union' 12.

This section will follow the abovementioned distinction made by the DPD itself regarding the territorial application of codes of conduct: those adopted at the national level, within Member States, will be called 'national codes'; codes applicable in the entire EU are called 'Community codes'.

II.A. National codes of conduct: severe fragmentation

As noted by Robinson et al. in their review of the DPD, codes of conduct were marked by a low uptake. The authors offer the explanation that this 'is possibly due to a perception that [self-regulation and co-regulation] are 'an enhancement rather than a substitute means of making data protection legislative requirements more effective and legitimate'.'[38] Consulting the Directive seems to reinforce this point since codes of conduct are only mentioned in the DPD in very limited ways: recital 61 merely paraphrases article 27, and recital 26 gives a very constricted example of how codes can be used, stating that codes 'may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible'.

Additionally, as article 27 paragraph 1 DPD states, national codes are 'intended to *contribute* to the *proper implementation of the national provisions* adopted by the Member States pursuant to this Directive' (*emphasis added*). They thus act as *supporting* instruments to national provisions that are in turn *adapted* from supranational norms. Recital 61 also highlights the rather awkward position that national codes find themselves in: they are meant to 'facilitate the operation' of the Directive, but must also respect the national provisions adopted for the Directive's implementation. Although this is a logical consequence of EU law principles, such a twice-removed link from the original provisions of the Directive might offer an explanation as to Korff's finding in his comprehensive comparison of the implementation of the DPD that national legislations took wildly divergent viewpoints on how codes should be drawn up, assessed, what their effects should be, and what their legal status was.[39] This resulted in a cooperative processes in drafting codes in Denmark; the possibility of imposing codes and a subsequent legislative approval that gives them binding legal effect in Ireland; and the near-default practice of Greek authorities issuing sectoral rules themselves.[40]

[38] Robinson and others (n 34) 9.
[39] Korff (n 34) 202.
[40] ibid 186–187.

Such different practices were also accompanied by tensions between national authorities and industry. In two separate reviews of the DPD, similar sentiments were found in interviews whereby enterprises accused the national DPAs of not taking their needs into account and instead attempting to unilaterally impose their preferred rules,[41] while authorities considered that corporations sometimes attempted to 'use codes as a means to evade certain strict rules in the law'[42] – codes of misconduct, if you will.

It is of particular interest to note in this regard that article 27 paragraph 2 stipulates that 'Member States shall make provision for trade associations and other bodies representing other categories of controllers … to be able to submit [codes] to the opinion of the national authority. Member States shall make provision *for this authority to ascertain*, among other things, *whether the drafts submitted to it are in accordance* with the national provisions' (*emphasis added*). Authors such as Lloyd interpret this to mean that draft national codes were to be submitted to the national supervisory authority mandatorily,[43] which also seemed to have been the practical reality – granting the national authorities significant power in determining the content of national codes as a result. Such a mandatory process stands in stark contrast to the voluntary submission for Community codes in article 27 paragraph 3 (see below).

In spite of this hands-on role for national authorities, the actual effects of national codes on compliance have been disputed and authors furthermore remark that the development of codes only occurred at a slow pace,[44] raising the question of whether it is truly beneficial for national DPAs to exercise such a large influence on the process.

II.B. Community codes: meagre results

'Community codes' are the DPD's term to indicate codes of conduct whose territorial scope encompasses the entire EU. Similar to national codes, Robinson et al. note that Community codes were

[41] Robinson and others (n 34) 37. A notable example under the DPD thereof was Italy's stipulation that, if press organisations did not draw up a code of conduct, the national authorities would impose one upon them: see Korff (n 34) 186. This is similar to the most recent version of the updated Audio-Visual Media Services Directive wherein it is stated that the European Commission may impose codes. See: European Parliament and European Council, *supra* note 34, articles article 4a para. 2, article 9 para. 5 and article 28b para. 10.
[42] Korff (n 34) 187.
[43] Ian J Lloyd, *Information Technology Law* (Oxford University Press 2011) 121.
[44] Korff (n 34) 240.

not widely used.[45] Here too, the aforementioned perception of codes as 'an enhancement rather than a substitute' for hard law is a possible explanation. Codes were not defined in the 1995 Directive and scholars did not seem to undertake conceptualisation efforts either, instead simply referring to them as codes '[a]t the European level'.[46] This lack of elucidation within the 1995 Directive led to conceptual conflation, as evidenced by the statement by former European Data Protection Supervisor (EDPS) Peter Hustinx that 'adequate protection [of data flows] is increasingly frequently delivered in 'binding corporate rules', codes of conduct endorsed by enterprises that meet specific requirements and which competent supervisory bodies accept as sufficiently effective'.[47] Although it would lead us too far to fully discuss the difference between binding corporate rules (BCRs) and codes of conduct, it is important to note that the 1995 Directive already distinguished between codes and BCRs – although they were not explicitly named so – by devoting articles 25 and 26 to them (see in particular the latter's second paragraph). The GDPR has made the distinction between both even more explicit and places a specific emphasis on the use of BCRs for the purpose of data transfers to third countries.[48]

Article 27 paragraph 3 is also marked by inconsistency. Submitting codes to the expert opinion of the Working Party (WP) is optional ('Draft Community codes, and amendments or extensions … *may* be submitted to the Working Party' (*emphasis added*)) yet good faith actors who take the trouble to do so then risk the WP disapproving of the code ('This Working Party shall determine … whether the drafts submitted to it are in accordance with the national provisions').[49] Moreover, there existed little to no incentive for private actors under the DPD to undergo this evaluative process in the first place, since neither the DPD nor the Article 29 Working Party (A29WP) in its post-legislative guidance document[50] offer any advantages for approved codes. Although the stipulation that '[t]he Commission may ensure appropriate publicity for the codes which have been approved' hints at the fact that national data protection authorities (DPAs) could have taken such approval into account when investigating an

[45] Robinson and others (n 34) 9.
[46] ibid.
[47] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' 11–12.
[48] Article 4, 20 GDPR.
[49] Article 16, 1(b) of the 2000 e-Commerce Directive is similarly non-binding, explicitly mentioning the 'voluntary transmission of draft codes of conduct at national or Community level to the Commission'.
[50] Article 29 Working Party, 'Working Document on the Procedure for the Consideration by the Working Party of Community Codes of Conduct'.

enterprise that adheres to a code, this is never stated explicitly. As a result, paragraph 3 created a free rider-esque scenario whereby actors who made the effort to submit their codes potentially suffered drawbacks compared to actors who do not.

Additionally, the fact that Community codes needed to be in accordance with Member States' fragmented national provisions created a complicated puzzle for any one instrument to address.[51] Although the earlier-cited 1998 guidance document would introduce the important nuance that it shall be determined whether codes are in 'accordance with the data protection directives and, *where relevant*, the national provisions adopted pursuant to these directives'[52] (*emphasis added*), industry actors ultimately criticised the lengthy and exhaustive nature of the process employed by the A29WP and the Commission as the main obstacle in developing codes of conduct.[53]

Ultimately, only two Community codes were ever approved: the 'European Code of conduct for the use of personal data in direct marketing' by FEDMA (Federation of European Direct and Interactive Marketing) in 2003[54] and its long-gestating 2010 Annex,[55] and 'Recommended Practice 1774 – Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo' by IATA (International Air Transport Association) – with the important caveat added by the A29WP itself that the latter does not strictly qualify as a Community code of conduct in the sense of Article 27 (3)[56] since it is rather

> a suggested framework that individual members adapt to comply with their national requirements and according to their own individual commercial practices. … [E]ach airline will remain free to create its own code of conduct vis-à-vis its own customers, and in accordance

[51] Robinson and others (n 34) 37.

[52] Article 29 Working Party, 'Working Document on the Procedure for the Consideration by the Working Party of Community Codes of Conduct' (n 50) 4.

[53] LRDP Kantor Ltd. (n 34) 52–53.

[54] Federation of European Direct Marketing, 'European Code of Conduct for the Use of Personal Data in Direct Marketing'; Article 29 Working Party, 'Opinion 3/2003 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing'.

[55] Article 29 Working Party, 'Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing'.

[56] Article 29 Working Party, 'Working Document on IATA Recommended Practice 1774 Protection for Privacy and Transborder Data Flows of Personal Data Used in International Air Transport of Passengers and of Cargo' (n 27) 7.

> with national legal and regulatory requirements. Also for evident antitrust immunity reasons IATA must avoid imposing any commercial behaviour on its members.[57]

Finally, it is notable that the World Anti-Doping Agency's (WADA) attempt to gain the A29WP's approval for its International Standard for the Protection of Privacy and Personal Information ended in failure in 2009 after the Working Party rejected the standard in its second opinion.[58] At the end of the Data Protection Directive's lifespan in May 2018, the total tally of approved Community codes stood at two; a meagre result for a 23-year-long regulatory regime.

III. Does the GDPR chart a different course?

Based on the findings in the previous section, we can compare the approaches of the DPD and the GDPR to offer thoughts on whether articles 40 and 41 GDPR employ a different strategy and whether they might achieve different results than article 27 DPD. The text of the GDPR itself is clear in the objectives it wishes codes to achieve: they are 'intended to contribute to the proper application of this Regulation' (article 40 paragraph 1) and are tools to take into account 'the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises … [and they] could calibrate the obligations of controllers and processors' (recital 98). Is it possible for the GDPR to achieve those goals?

One of the most important obstacles to overcome in this regard is the prevailing negative perception under the DPD that ARIs are 'add-ons' to legislation, rather than valid and autonomous instruments. In that regard, the EU has gone to great lengths to legitimise the role of self-regulation and co-regulation within the Union, emphasising the potential benefits in many instruments (see above). Nonetheless, the GDPR, at least at first glance, treats codes subservient to itself as a hard law instrument, with both the text of the regulation and background documents considering codes of conduct (and certification mechanisms) as compliance tools.[59] Thus, by adhering to a code, actors can show their compliance – or at least their willingness to comply – with the main provisions of the GDPR, which can in turn influence

[57] ibid 3.

[58] Article 29 Working Party, 'Second Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on Related Provisions of the WADA Code and on Other Privacy Issues in the Context of the Fight against Doping in Sport by WADA and (National) Anti-Doping Organizations'.

[59] European Commission, 'Communication: Stronger Protection, New Opportunities - Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018' 12.

the amount of a fine or even their very imposition as a result of a violation of one of the GDPR's main provisions: as stated by article 83, 2 (j) GDPR, '[w]hen deciding whether to impose an administrative fine and deciding on the amount … due regard shall be given to … adherence to approved codes of conduct'. The A29WP's guidelines on the application and setting of administrative fines elaborate by explaining that 'adherence … might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority' and that the authority in question might also be satisfied by letting the code's monitoring and enforcement schemes deal with the violation.[60] Hence, codes of conduct under the GDPR largely act as 'liability reduction mechanisms', with non-participating data controllers exposing themselves to a higher risk of fines *or* a risk of higher fines, offering a much clearer incentive for corporate actors to participate in codes compared to the DPD. As stated before, such a function for codes *does* denote their subservience vis-á-vis the GDPR's other provisions, but Korff predicts that the mechanism will ultimately result in 'industry practice to only award processor contracts and only allow further sub-contracting to processors and sub-processors who … are subject to an approved code',[61] creating an autonomous system that achieves the objectives of data protection.[62]

The parties standing to gain most from a wider acceptance of codes might be small-to-medium enterprises (SMEs). Their mention alongside codes of conduct in recital 98 GDPR (and throughout the rest of the regulation)[63] is an important innovation as compared to the DPD. This can be attributed to two reasons: the EU's general policy goal to use the GDPR-induced data reform to stimulate 'economic growth by cutting costs and red tape … especially for small and medium enterprises',[64] as well as fears that high GDPR compliance costs potentially demotivate new market entrants or cause existing actors

[60] Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679' 15.

[61] Douwe Korff, 'The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service' [2019] Unpublished manuscript 25–26 <https://papers.ssrn.com/abstract=3439293> accessed 6 September 2019.

[62] Robinson and others (n 34) 9.

[63] See recitals 13, 98, 132, 167 and articles 40 and 42 of the GDPR.

[64] European Commission, 'Fact Sheet: Stronger Data Protection Rules for Europe' <https://europa.eu/rapid/press-release_MEMO-15-5170_en.htm>.

to retreat.[65] Although some claim that codes could actually 'impose particular additional requirements',[66] most commentators believe that the tailor-made nature of codes allows them to translate the abstract concepts of the GDPR into practical guidelines in very cost-effective manners,[67] greatly aiding the capacity of smaller enterprises to adhere with the accountability requirement set out by the GDPR.[68]

The submission procedure that was optional under the text of the DPD has also seen a significant change under the GDPR. Article 40 now obliges the submission of any draft codes to the relevant national authority in the case of national codes (paragraph 5) or to the European Data Protection Board for codes relating to processing activities in several Member States (paragraph 7). This has the unquestionably positive side effect of removing the free rider-esque scenario under article 27 paragraph 3 DPD where actors who went through the trouble of submitting their code were possibly met with a rejection while those who did not submit a code could proceed unhindered.

Another interesting change between the DPD and the GDPR is due to the difference in legislative nature between both instruments. Whereas the DPD as a directive still required national provisions to incorporate its ruleset, the GDPR as a regulation creates a harmonised set of principles and rights across the EU.[69] This also changes the classifications that both instruments make regarding codes: the DPD used to make a two-fold distinction between national codes and Community codes, but the GDPR now has a three-fold classification according to the territorial reach of codes. First, there are the national codes applicable within Member States, which remain as they were in the DPD. Second, however, a new category is created in article 40 paragraph 7, namely codes 'relat[ing] to processing activities in several Member States' or 'transnational codes'.[70] Such an extra classification is understandable to guarantee the harmonised regime that the GDPR aims for; after all, when a draft code relating to

[65] Jennifer Huddleston, 'What GDPR's First Year Says about Data Privacy Regulation' *The Hill* (10 May 2019) <https://thehill.com/opinion/technology/443103-what-gdprs-first-year-says-about-data-privacy-regulation> accessed 16 May 2019.

[66] Ruth Boardman, James Mullock and Ariane Mole, 'Guide to the General Data Protection Regulation' (Bird & Bird 2019).

[67] European Data Protection Board (n 31) 8; Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 73; Robinson and others (n 34) 52.

[68] Eric Lachaud, 'Adhering to GDPR Codes of Conduct: A Possible Option for SMEs to GDPR Certification' (2019) 3 Journal of Data Protection & Privacy 1.

[69] With some specific exceptions; going into further detail would go beyond the scope of this paper, however. See also recital 13 GDPR for the emphasis on 'ensuring a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data'.

[70] The term 'transnational codes' is introduced in the EDPB's guidelines on codes of conduct and monitoring bodies. See: European Data Protection Board (n 31) 7.

processing activities in several Member States is submitted to a national authority of the code owner's choice (the 'competent supervisory authority' or CompSA), it triggers the obligation for the CompSA to elect two co-reviewing supervisory authorities (SAs). If the draft is approved, the CompSA must first await the EDPB's opinion as the central EU-level authority (the so-called 'consistency opinion')[71] before finally deciding whether or not to grant the ultimate approval. An important point is that the code owner is free in choosing a CompSA of its liking; although appendix II to the EDPB's guidelines on codes of conduct set out factors that *could* be taken into account when choosing a CompSA, there are no binding rules.[72] The possibility therefore exists that a situation of 'regulatory arbitrage'[73] emerges whereby code owners deliberately seek out more accommodating national authorities.[74] The GDPR does have mechanisms in place to counter such a lopsided situation: besides the obligation of having two co-reviewing SAs as well as the mandatory submission to the Board, articles 64 and 65 set out the authoritative status of the Board's opinion, the need for CompSAs to explain why they would diverge from the Board's opinion, and a dispute resolution procedure by the Board. The chances of widespread abuse are thereby mitigated to some degree.

[71] European Data Protection Board, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities'.

[72] European Data Protection Board (n 31) 28.

[73] Elizabeth Pollman, 'Tech, Regulatory Arbitrage, and Limits' (2019) 20 European Business Organization Law Review 567.

[74] Indeed, this very phenomenon seems to be occurring, as investigative journalistic effects have uncovered that close ties exist between certain national data protection authorities and the tech industry, due to the massive economic impact the presence of large tech companies can have on small economies. See: Nicholas Vinocur, '"We Have a Huge Problem": European Tech Regulator Despairs over Lack of Enforcement' (*POLITICO*, 27 December 2019) <https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605> accessed 27 December 2019; Nicholas Vinocur, 'How One Country Blocks the World on Data Privacy' *POLITICO* (24 April 2019) <https://politi.co/2PqFc42> accessed 15 May 2019.

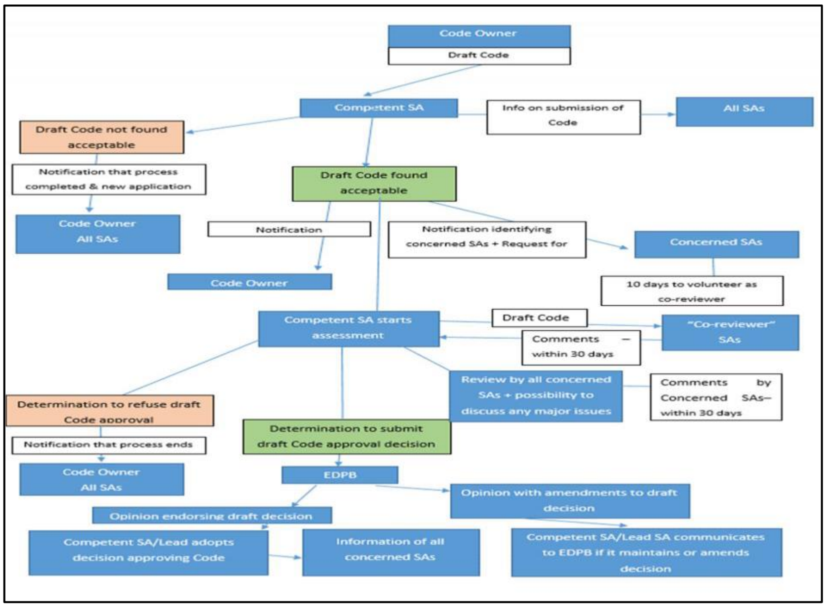
Code Owner
Draft Code
Competent SA
Info on submission of Code
All SAs
Draft Code not found acceptable
Notification that process completed & new application
Code Owner All SAs
Draft Code found acceptable
Notification
Notification identifying concerned SAs + Request for
Concerned SAs
Code Owner
10 days to volunteer as co-reviewer
Competent SA starts assessment
Draft Code
"Co-reviewer" SAs
Comments – within 30 days
Review by all concerned SAs + possibility to discuss any major issues
Comments by Concerned SAs– within 30 days
Determination to refuse draft Code approval
Determination to submit draft Code approval decision
Notification that process ends
Code Owner All SAs
EDPB
Opinion with amendments to draft decision
Opinion endorsing draft decision
Competent SA/Lead adopts decision approving Code
Information of all concerned SAs
Competent SA/Lead SA communicates to EDPB if it maintains or amends decision

Fig. 2. The EDPB's flow chart for transnational codes.[75]

Finally, a third GDPR category of codes exists entitled 'codes having general validity' in article 40 paragraph 9 GDPR. Although the meaning of 'general validity' is not explained in the GDPR itself, it is interpreted as meaning that 'actors in a given sector from any of the 28 Member States may sign up to the code'.[76] Additionally, the EDPB's guidelines set out that controllers and processors not subject to the GDPR can make binding and enforceable commitments where a validated code is concerned.[77] Importantly, the GDPR's article 40 paragraphs 7 through 9 determine that 'codes having general validity' flow out of transnational codes:

> Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority … shall … submit it … to the Board which shall provide an opinion; [w]here the opinion … confirms that the draft code, amendment or extension … provides appropriate safeguards, the Board shall submit its opinion to the Commission; [t]he Commission may … decide that the approved code of conduct, amendment or extension submitted to it … have general validity within the Union

This process in phases forms a positive step, since it can more quickly lead to the establishment of a code that is then incrementally expanded. For example, as suggested by the EDPB itself, a successfully

[75] European Data Protection Board (n 31) 30.
[76] Steptoe & Johnson, 'The GDPR from an Insurance and Financial Intermediation Perspective' (BIPAR 2016) 42.
[77] European Data Protection Board, *supra* note 33 at 21 and footnote 72.

approved and applied national code can be extended in scope to start the approval procedure for a transnational code.[78] This could then grow into a code 'having general validity', with the text of these paragraphs implying that transnational codes can enter into effect while awaiting the Commission's decision whether or not a code in the meaning of paragraph 7 is bequeathed general validity – thus somewhat addressing the industry's frustration with the DPD that the approval process was too drawn out. To further improve the pace of processing codes, a 2010 review of the DPD suggests adopting 'the system used in the European Privacy Seal … [I]n that system, approved independent experts do the preparatory work (paid for by the private parties concerned, …), subject to a close review and (if positive) certification by an official body, involving national data protection authorities'.[79]

The GDPR's nature as a regulation should theoretically also remedy the divergent national practices regarding the drawing up, assessment, effects and the legal status of codes that were the result of transposing the Directive's provisions to national legislation. However, two creases are introduced to this theory.

First, the GDPR does provide 'a margin of manoeuvre for Member States to specify its [sic] rules' (recital 10) in certain instances, such as the conditions for a child's consent under article 8 or the personal data of deceased persons as mentioned in recital 27. The EDPB nonetheless believes that codes can 'help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law … particularly … where a code relates to processing activities in several Member States'.[80] Yet this raises the specter of why Community codes failed to become a widespread practice under the DPD: the obligation to be in accordance with a fragmented collection of national provisions. It will be interesting to see if any sector representatives are willing to tackle topics that diverge widely between Member States through a code.

Second, article 40 paragraph 5 still foresees a highly influential role for national supervisory authorities in the same vein of the DPD. After all, the competent national DPA '*shall provide an opinion* on whether the draft code, amendment or extension complies with this Regulation *and shall approve* that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards' (*emphasis added*).

[78] ibid 27.
[79] LRDP Kantor Ltd. (n 34) 53.
[80] European Data Protection Board, *supra* note 33 at 5 and footnote 5.

As noted by Korff, the possibility for a DPA to assess a code's compatibility with the law and issue an opinion thereon, introduces an important element of ambiguity regarding the legal status of national codes and national DPAs.[81] Here too, the EDPB seeks to counter such a risk for new varying national practices by emphasising that its 2019 guidelines on codes are meant to ensure consistency for both the transnational and national processes.[82]

IV. Conclusion

As was already noted in the introduction, this paper does not seek to comprehensively evaluate GDPR-based codes of conduct; after all, it is simply too early in the instrument's lifespan and additional research (being: more scholarly literature on codes of conduct in the EU's personal data protection policy) and research methods (such as an empirical analysis of corporate documents and semi-structured interviews with stakeholders such as DPAs, the EDPB and corporate policy advisors) are necessary to achieve a satisfactory evaluation. Instead, the goal was to make tentative assessments on the GDPR's approach vis-á-vis the DPD; where did the 1995 Directive go wrong and does the GDPR learn from those failures?

The first signs are positive. By explicitly designating codes of conduct as liability reduction mechanisms, industry actors are offered a clear incentive to participate in codes. Additionally, it creates the potential for an evolution toward a meaningful and autonomous system that raises data protection standards (cfr. Korff's prediction). The GDPR's innovation of emphasising the usefulness of codes for small-to-medium enterprises also appears successful due to the focus that codes inherently put on the practical implementation of abstract standards and subsequently their potential in offering cost-effective compliance. Finally, the move from an optional submission procedure to a mandatory one removes the potential for a free rider-esque scenario á la article 27 paragraph 3. Nonetheless, it remains to be seen whether other significant changes will achieve positive effects. The three-fold classification between codes that is introduced in article 40 GDPR is a necessary consequence of the GDPR's status as a regulation and the need for consistency across the Union. While it displays thoughtful measures to combat abuses of the system, many individual procedural steps and deadlines remain, and several different governmental authorities stay involved (at least in the case of transnational codes). This does

[81] Korff (n 34) 185–186.

[82] European Data Protection Board (n 31) 6.

not directly address the industry's complaint under the DPD that the approval process of codes was too lengthy and exhaustive.[83] It also remains to be seen whether the practical implementation of codes dealing with Member States' regulatory margin for specific provisions of the GPDR will align with the EDPB's optimistic outlook that codes could function as bridges that paper over national regulatory differences.[84]

In turning toward the future, we can notice an encouraging amount of activity regarding codes of conduct under the GDPR. According to reports, the French supervisory authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), has announced preparatory work on national codes for the medical research sector and cloud infrastructure.[85] Furthermore, work on two high-profile transnational codes of conduct is underway: the EU Data Protection Code of Conduct for Cloud Service Providers is undergoing review of its version 2.1,[86] while the Privacy Code of Conduct on mobile health (mHealth) apps is being revised after a negative advice by the Article 29 Working Party in 2018.[87]

It is also worth noting the effort that the EDPB has made to increase legal certainty for stakeholders[88] by issuing guidance on the principles and procedures regarding the approval process for codes early on in the life cycle of the GDPR. Additionally, it demonstrated its willingness to take the feedback of the parties involved into account by making meaningful changes to the finalised guidelines published in July 2019 compared to the draft version for public consultation of February 2019. Nonetheless, important questions remain on both the theoretical side (such as the fine line between using codes in a co-regulatory or a top-down manner and the legal repercussions thereof, as well as the impact that GDPR-based codes can have on global data protection standards)[89] and regarding practical matters (such as

[83] LRDP Kantor Ltd. (n 34) 52–53.

[84] See, for example, an extensive Politico report that notes a 'lack of transparency and cooperation between European data protection authorities' and diverging regulatory interpretations that result in regulatory patchwork: Vinocur, '"We Have a Huge Problem"' (n 74).

[85] Boardman, Mullock and Mole (n 66) 48.

[86] SCOPE Europe, 'Press Release: Ready for Submission: EU Cloud Code of Conduct Finalized' (25 April 2019) <https://scope-europe.eu/en/projects/eu-cloud-code-of-conduct/> accessed 20 September 2019.

[87] Article 29 Working Party, 'Subject: Your Letter of 7th December 2017 and a New Draft Code of Conduct with the Request of a Positive Opinion from the WP29 under the Data Protection Directive'.

[88] Cynthia O'Donoghue and Eleanor Brooks, 'EDPB Completes Guidelines on Codes of Conduct, Certification and Accreditation of Certification Bodies' (*Technology Law Dispatch*, 20 June 2019) <https://www.technologylawdispatch.com/2019/06/privacy-data-protection/edpb-completes-guidelines-on-codes-of-conduct-certification-and-accreditation-of-certification-bodies/> accessed 25 September 2019.

[89] See for example the reference by the EDPB to the 'wider international community' in its guidelines: European Data Protection Board (n 31) 10.

doubts whether there will be much appetite to develop codes that must deal with topics that touch on Member States' 'margin to manoeuvre' such as under article 8). Further research into this underexplored topic must be carried out as more codes are drawn up, approved and implemented.