INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications

Rotem Medzini *The Hebrew University of Jerusalem*

DOI: https://doi.org/10.14763/2021.3.1577

Published: 30 September 2021
Received: 11 November 2020 **Accepted:** 12 March 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Medzini, R. (2021). Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1577

Keywords: Data protection, Regulatory intermediares, Certification, Accreditation, Codes of conduct, Internet governance

Abstract: This paper addresses how European policymakers have delegated the responsibility of protecting European values inside transnational data flows to private bodies acting as regulatory intermediaries. The paper uses a process-tracing methodology to argue that by accrediting private bodies to monitor codes of conduct and to assess conformity with certification schemes, policymakers have allowed enhanced self-regulation to exist in the shadow of European and national hierarchies. The paper process-traces how the two sub-regimes have evolved and then asks what the similarities and differences between the two sub-regimes are. The paper thereafter draws conclusions about how regulators can impact self-regulation that exists in their shadow through regulating via intermediaries instead of using direct modes of regulation.

This paper is part of **Governing "European values" inside data flows**, a special issue of *Internet Policy Review* guest-edited by Kristina Irion, Mira Burri, Ans Kolk, Stefania Milan.

1. Introduction

The governance of European values around issues of data protection is continually on global political, regulatory, academic, and business agendas. The policies that European policymakers and national regulators adopt address the concern that information technology (IT) companies and political actors use private information to track, misinform, and affect individuals' political and commercial preferences. Data protection policies also increasingly influence business practices: they shape organisational structures and policies, assign tasks to corporate actors, and require the appointment of compliance officers. For multinational organisations, data protection policies can impact business decisions on information flow, information processing, and the location of data centres. New modes of governance and self-regulation emerge from these policies to include regulatory intermediaries, i.e., actors who work in conjunction with policymakers and regulators to influence the behaviour of regulated organisations: controllers and processors alike (together: rule-takers). In the emerging modes of governance, both these groups of actors—the regulatory intermediaries and the rule-takers—can self-regulate in the shadow of European and national hierarchies.

Political and social scientists have long been suggesting that self-regulation can exist in the shadow of coercive hierarchies (Black, 1996, p. 27; Héritier & Lehmkuhl, 2008). This occurs when policymakers initiate steps to legislate, for instance where there are no preexisting laws, or where regulators threaten executive decisions, for instance by reregulating towards tighter regulation as a precondition for creating an industry more willing to engage in self-regulation (Héritier & Eckert, 2008, p. 114). Therefore, political scientists and legal scholars explain that self-regulation in the shadow of hierarchy involves both the delegation of tasks and responsibilities from policymakers to private actors to formulate and impose regulations (Black, 1996, p. 27), as well as involving the mechanisms to continuously threaten or induce compliance (Héritier & Lehnkuhl, 2008, p. 2). Such relationships, especially when they constrain or incentivise self-regulation in the shadow of hierarchy, raise questions of politics and policies about whether the threat or incentive will materialise, and questions about the mode of governance that would ensure the long-term commitment of all involved stakeholders. This paper process-traces the adoption of two such (sub-)regimes that exist in the shadow of

European and national hierarchies: the requirement under the General Data Protection Regulation (GDPR) to rely on private monitoring and certification bodies to adopt data protection codes of conduct or certifications. [1]

The adoption of the GDPR in 2016, and consequently the emergence of a new European data protection regime, offers an interesting case study for the new modes of governance in the shadow of hierarchy. Until 2016, the old data protection regime and its core legislation—the European Data Protection Directive (EDPD)—assigned *sole* regulatory competence to the national data protection supervisory authorities (DPAs) to monitor and to enforce data protection rules (Newman, 2008). Under this regime, controllers needed to notify DPAs of their self-regulatory practices, and DPAs in turn ratified and then registered the controllers' processing operations in public registries. Conversely, while the GDPR maintains the leading regulatory position of DPAs in monitoring and enforcing data protection rules (see Article 57), it also adopts a regime of enhanced self-regulation via regulatory intermediation that permits private bodies to interpret, monitor, and sometimes even enforce data protection rules (see Articles 41(1) and 43(1)). These data protection rules must first be defined, either in codes of conduct or certification (see Articles 40 and 42), and then the private bodies must receive accreditation from a public authority (see Articles 41(2) and 43(2)). [2] Only after the standardisation and accreditation phases can the private bodies monitor and assess conformity with the codes and certifications. Once accredited and certified, monitoring bodies, certification bodies, and the rule-takers that they monitor or certify, can all act in the shadow of the hierarchical decisions of European policymakers and national regulators.

Two preliminary clarifications are needed regarding the role of DPAs in creating a shadow of hierarchy. First, while a threat by European policymakers to amend the GDPR in order to nudge regulatory intermediaries and rule-takers towards self-regulation is possible, the more immediate 'threat' can originate from the DPAs. The GDPR clarifies that the existence of codes and certifications, as well as the delega-

1. To date, the European Data Protection Board (EDPB) has registered three codes of conduct: two with named monitoring bodies and one conditional on naming a monitoring body. Additionally, in May 2019, the EDPB issued two opinions on draft decisions regarding European codes of conduct for cloud service providers (EDPB, 2021a) and cloud infrastructure service providers (EDPB, 2021b). No certifications have yet been registered.
2. According to Colin Bennett and Charles Raab (2006, pp. 153–155), codes of conduct or practice are a set of rules that provide guidance about correct procedures and behavior. Meanwhile, according to Loconto (2017, pp. 117–118) certification occurs when independent third-party actors both attest to the target's compliance and determine conformity with a standard. An accreditation offers another level of determination, wherein accreditors determine conformity of the certifiers with another set of standards.

tion of responsibilities to monitoring and certification bodies, are without prejudice to the tasks and powers of the DPAs (see Articles 41(1), 41(4), 43(1), and 43(7)). As regulators, the DPAs have the final word about which decisions are subject to possible effective judicial remedies (Article 78). Second, Articles 40(1) and 42(3) of the GDPR specify that the purposes of the codes and certifications are, respectively, to *contribute* to the proper application of the GDPR, and to permit rule-takers to *demonstrate* compliance. Even though the codes and certification are enhanced by the empowerment of private monitoring and certification bodies, a demonstration of compliance does not ensure compliance with the GDPR (Leenes, 2020). Although DPAs can require higher compliance standards than demonstrated, given the continuous debate on whether DPAs have sufficient resources to successfully regulate data protection (European Commission, 2020), monitoring and certification bodies can assist the DPAs to regulate from a distance and can free up the DPAs' time and resources.

I therefore ask, how have European policymakers established the two regulatory arrangements that permit private bodies to act as regulatory intermediaries in order to monitor codes and assess conformity with certifications in the shadow of hierarchy? The paper thereafter asks what the similarities and differences in the design of the two sub-regimes are, and concludes by addressing how hierarchical decisions can impact the self-regulation that exists in the sub-regimes' shadows. To answer these questions, I chose to use the process-tracing methodology as it has previously been used to empirically and theoretically study European integration (Pierson, 1996). To apply the methodology, I first examined the European regimes for codes of conduct and certification prior to the adoption of the EDPD and the GDPR. I started with these initial decisions in order to understand whether they created path dependencies for policymakers and regulators. From there, I obtained documents for the process-tracing through formal freedom of information (FOIA) requests and from European Council documents leaked by civil activists (n=466). Additional documents included formal and online publications by European institutions such as the European Commission, the European Data Protection Board (EDPB), and the DPAs. Materials on the specification of the codes and certification schemes were retrieved from websites of the European institutions and of the owners of the relevant codes and certifications. I also participated in a workshop hosted by the European Commission on *Data protection certification mechanisms and standards: industry needs and views on the new GDPR certification*.

Based on the documents I gathered, the second step of the analysis involved tracing how the policy outcomes regarding codes of conduct and certification in gen-

eral, and the reliance on monitoring and certification bodies in particular, came about. This step involved answering why the precise policy outcome became dominant over other policy alternatives, which policymakers were involved in the decision-making process, and how power was distributed amongst them and other parties (Van Den Bulck, 2012, p. 18). I searched the documents for behind-the-scenes political bargaining, decisions and arguments made by policymakers in the European Council, the European Parliament, and the European Commission both in favour and against the decisions to adopt codes and certifications into the regime and to enhance them by relying on monitoring and certification bodies. During the process tracing and document analysis I also looked for policy and regulatory decisions that lay the groundwork for the decision to include the certifications and codes of conduct as part of the proposal for the GDPR. At the next stage, I adopted an inductive qualitative approach aimed at comparing the similarities and differences between data protection codes of conduct and certification. Due to the length of the criteria that the GDPR provides and the additional specification by the EDPB, I separated the comparison into three parts, one part for each phase of the standardisation process: standardisation, accreditation, and certification. The final stage of the research included drawing conclusions about how regulators can impact self-regulation that exists in their shadow through regulating via intermediaries instead of using direct modes of regulation.

The next section addresses the theoretical framework of self-regulation: how regulatory regimes incorporate self-regulatory components, and how regulatory intermediation can also be used to create regimes of self-regulation. Section 3 then describes how the two self-regulatory sub-regimes in the shadow of European hierarchies have emerged, and Section 4 compares the two sub-regimes. Thereafter, I draw conclusions about how regulators can impact self-regulation that exists in their shadow by regulating via the intermediaries instead of using direct modes of regulation.

2. Theoretical framework

Self-regulation means the process through which individual organisations or the regulated industry design formal or informal rules and procedures and thereafter enforce the rules and procedures on themselves (Porter & Ronit, 2006). Self-regulation regimes usually benefit from a greater degree of experience and efficiency, yet they tend to suffer from a lack of accountability and legitimacy (Ogus, 1995). And while self-regulation can be voluntary (Black, 1996), policymakers and regulators can overcome deficiencies in its accountability and legitimacy by introducing

self-regulatory components into public regulatory regimes. They can mix and match different policy mechanisms and constraints to mandate rule-takers to self-regulate (enforced self-regulation; Ayres & Braithwaite, 1992). Policymakers can also decide to share responsibilities between government actors and private bodies in order to overcome regulatory shortfalls (co-regulation; Levi-Faur, 2011) or regulate the manner in which private actors self-regulate (meta-regulation; Gilad, 2010). Policymakers and regulators can additionally coerce rule-takers to self-regulate by threatening to adopt constraining rules (Black, 1996, p. 27; Héritier & Lehmkuhl, 2008) or by inducing them to consider social values or environmental concerns (Schneider & Scherer, 2019). Hence, policymakers and regulators make the self-regulatory regimes more public, they offer to introduce democratic accountability, and they suggest that the new forms of regulation better consider long-term policy goals.

However, these mechanisms and constraints that mandate rule-takers to self-regulate tend to focus on the direct and hierarchical relationships between regulators and regulated organisations. Conversely, another method of influencing self-regulation is to introduce an intermediary to indirectly regulate and affect the self-regulatory practices of rule-takers. When actors in a self-regulatory regime move beyond self-regulation mechanisms and rely on independent regulatory intermediaries to constrain their conduct and improve policy implementation, I call such a form of self-regulation via regulatory intermediation 'enhanced self-regulation' (Medzini, 2021b). The term 'enhanced' indicates that actors can delegate responsibilities to regulatory intermediaries in order to improve the credibility of self-regulation, for example towards accountability in data protection (Medzini, 2021a).

The literature on regulatory governance defines regulatory intermediaries broadly as any actor that affects the behaviour of rule-takers and makes some aspect of the regulation of regulated organisations indirect (Abbott et al., 2017, p. 19). Regulatory intermediaries can enter the regulatory regime for either functional or political reasons. Policymakers, regulators, and regulated organisations might decide to rely on intermediaries due to the capacities they possess that other actors lack, or due to their legitimacy to regulate. At the same time, the same actors might decide to rely on regulatory intermediaries for political reasons. Regulatory actors, including the intermediaries, might consider the mechanism of regulatory intermediation as a way to capture the regulatory regime, to gain regulatory rents, or to direct decisions away from the public interest and towards special interests (Marques, 2019).

The literature on regulatory intermediation explains that regulatory regimes can

also include more than one group of intermediaries. In such regimes, one group of regulatory intermediaries (I_1) can regulate another group of regulatory intermediaries (I_2), although they might have different and unrelated functions. A leading example of regulatory intermediation regimes in which intermediaries have interrelated functions are tripartite standard regimes (TSR; Loconto & Busch, 2010). TSRs are defined by three separate phases: standardisation, accreditation, and certification. For example, policymakers and regulators first need to approve the criteria for accreditation and certification (the standardisation phase). They would then allow one group of intermediaries (I_1) to accredit another group of intermediaries (I_2) (the accreditation phase) in order for the accredited bodies to certify (the certification phase). [3] Such an approach creates multiple levels of oversight and consequently an indirect relationship between policymakers and regulated organisations. The literature further explains that European policymakers previously adopted such a TSR approach as part of the European 'New Approach' to standardisation; an approach which seeks to open the European market to products without threatening the safety of European consumers (Galland, 2017).

At the same time, one consequence of having several phases of intermediation is the introduction of increased complexity. Besides having more intermediaries to capture, more intermediaries mean there are more actors who can hold, or more critically fail to hold, regulated organisations to account. For example, intermediaries can fail to conduct proper oversight or to rectify noncompliance (accountability forum drift; Schillemans & Busuioc, 2014, pp. 201–205). To provide an explanation of how European policymakers have adopted the two sub-regimes of enhanced self-regulation, the next section traces the process by which European policymakers introduce certification and monitoring bodies into the European data protection regime.

3. The origins of the European codes of conduct and certification

3.1. Codes of conduct before and during the old regime

The use of codes of conduct as policy instruments in the European data protection regime can be traced to national legislation adopted during the 1970s and 1980s

3. Certification and accreditation provide a statement of conformity following a process of attestation and determination. The mechanism that differentiates certification and accreditation from first-party conformity (self-reporting) or second-party verification is regulatory intermediation. Certification and accreditation occur when one or more third parties conducts the attestation and then determines conformity with the criteria.

in response to the introduction of electronic data processing (Mayer-Schönberger, 1997). According to Francesca Bignami (2011), codes of conduct were popular in Britain, Germany, and the Netherlands, but not in France and Italy. While the codes existed at the national level, their adoption at the supranational level did not happen so easily. To begin with, European policymakers did not always see eye to eye on the urgency to have European data protection rules nor to have mechanisms of self-regulation. [4] Primarily, the European Commission disagreed with the resolutions passed by the European Parliament due to the potential cost of the resolutions to the private sector. According to Abraham Newman (2008, pp. 112–16), the actions taken by transgovernmental policy entrepreneurs against the emergence of data havens resulted in a much-needed policy shift. They nudged European policymakers to propose the adoption of a European-wide data-protection framework—the EDPD.

During the deliberations on the EDPD, the European Commission and the European Council did not agree on the purpose of using codes of conduct. The Commission envisioned that sectoral codes could enable the free flow of personal information throughout the European Community. The codes would contribute to the Commission's objectives of establishing an adequate level of protection throughout the Community and preventing barriers to information flows. The Commission also sought to use codes of conduct as a source for establishing additional initiatives (European Council, 1991a) which could be considered while it proposed new sector-specific legislation and measures. While the Commission did not prevent the use of *national* codes of conduct (European Council, 1991b, pp. 17–18), it wanted member states to encourage their business circles to participate in drawing up *European* codes (European Council, 1990). In contrast, while the Council agreed with the Commission on the need to achieve harmonisation, delegations strived to have sufficient discretion for implementation, while considering their special national and sectoral characteristics. For instance, delegations proposed using the codes to exempt a large majority of cases from the broad notification requirement that was embedded early on into the draft EDPD (European Council, 1992a). The Council later also adopted the Dutch position that the purpose of codes was to supplement or to interpret data protection laws, and not to introduce derogations or new limitations (European Council, 1992b).

Following additional consultation with the European Parliament, the Commission

4. While the Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981*, the Convention lacked mechanisms for self-enforcement, and it was unable to create harmonisation among the European member states (Newman, 2008, pp. 109–10).

amended its proposal for the EDPD. The new draft included provisions on *national* codes. In return for more authority and certainty, the new draft tasked DPAs with ensuring that trade associations that submit their codes are in fact representative, and that the codes are well thought through. As the codes would not bind third parties and the courts, *national* codes would hence only improve implementation (European Commission, 1992, pp. 36–7). The new draft EDPD also shifted decision-making about the codes from the Commission to regulators: DPAs would decide on *national* codes, and the Article 29 Working Party (WP29) would decide on *Community* codes. Consequently, instead of adopting the Commission's position regarding *Community* codes, codes became a mechanism for contributing to the proper application of national legislation (European Council, 1993, p. 5). A later version of the EDPD joined the two articles that separately addressed national and Community codes into one article: Article 27 of the EDPD (European Council, 1994).

The practice of adopting codes of conduct under the EDPD was a direct continuation of the events that occurred during the deliberations among European policy-makers. Researchers have observed that codes of conduct were mostly adopted at the national level, though with great variance between countries (Robinson et al., 2009). While in some countries, such as Denmark, the DPAs and industry collaborated on the process of drafting codes, in other countries, such as Ireland and Greece, codes tended to have a more binding effect (Vander Maelen, 2020, p. 236). Meanwhile, at the European Community level, WP29 formally issued a decision on three codes of conduct (Vander Maelen, 2020, p. 235). WP29 approved a code by the Federation of European Direct and Interactive Marketing (FEDMA) which addressed the use of personal data in direct marketing (Article 29 Working Party, 2003, 2010). It issued an opinion that a code by the International Air Transport Association (IATA) to address transborder data flows of personal data used in international air transport of passengers and of cargo should be read as a 'suggested framework' (Article 29 Working Party, 2001), but it rejected a standard by the World Anti-Doping Agency (WADA; Vander Maelen, 2020, p. 235). Unsurprisingly, the Commission made public its disappointment that only a few organisations had applied for Community codes (European Commission, 2003).

3.2. Certification during the old data protection regime

Unlike codes of conduct, certification schemes had no formal provisions under the EDPD. They existed either as private or as regulatory solutions (Kamara et al., 2019). Whereas most certification schemes are private, two schemes were managed by, or received the approval of, either the European Commission or national regulators who were members of the WP29. [5] The first scheme was the US–EU

Safe Harbor Agreement (SHA). The SHA was signed by the European Commission and the US Department of Commerce (DoC) in order to allow American companies—whose federal legal system provides no comprehensive data protection regime—to process personal data of Europeans. Companies needed to self-certify, annually and in front of the DoC, that they would adhere to the seven principles embedded in the SHA. As organisations made public commitments, their misrepresentation would have been enforced by the Federal Trade Commission as an 'unfair and deceptive' trade practice (Bennett & Raab, 2006, pp. 167–69). [6] An adequacy decision by the European Commission bound the European member states and their regulators—until the European Court of Justice (ECJ) invalidated the Commission's adequacy decision in 2015—as it found that the SHA failed to provide adequate safeguards for the personal information of Europeans. [7] The Privacy Shield Frameworks that replaced the SHA and which offered stronger obligations with more effective protections for individuals was invalidated by the ECJ in 2020. [8]

The second European-wide certification scheme was the European Privacy Seal (EuroPriSe). EuroPriSe was established in 2007 as a voluntary privacy certification for IT products and services. It built upon the EDPD, national and European legislation, European court rulings, and policy papers adopted by the WP29. EuroPriSe draws its legitimacy from two sources. First, European policymakers and national regulators recognised and participated in EuroPriSe. The European Commission and the Directorate-General for Communications Networks, Content and Technology (DG Connect) supported EuroPriSe through the eTEN programme for the deployment of e-services in Europe. Also, three DPAs—the DPAs of the German state of Schleswig-Holstein (ULD), the French CNIL, and the Spanish APDCM—comprised one third of the EuroPriSe consortium. Second, EuroPriSe's evaluation and certification procedures also strengthened its legitimacy. Its consortium trains independent privacy and IT-security experts to evaluate candidate products and services. Their evaluation reports are then forwarded to the impartial certification body for

5. Some DPAs also introduce national-level certification schemes. A leading example are the French CNIL Labels aimed at providing assurances that a product or a procedure corresponds to the French data protection act and the CNIL's regulations. The CNIL issued four labels: 1) for auditing procedures; 2) for certifying training courses on data protection; 3) for digital safe boxes, and 4) for data protection governance procedures. According to the CNIL, the Labels would transform into certification schemes.
6. In practice, a sample of 249 privacy policies have shown that due to poor monitoring and weak enforcement mechanisms almost all firms misrepresented their claims of adherence to the SHA (Marotta-Wurgler, 2016).
7. Case C-362/14 Maximillian Schrems v Data Protection Commissioner (6 October 2015).
8. Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (16 July 2020).

validation of its methodology, and for consistency and completeness. If the evaluation shows compliance with the EuroPriSe criteria, a two-year certification and seal are issued. From 2009 to 2013, ULD ran EuroPriSe, but since 2013 it has been running as a private enterprise.

3.3. The adoption of a 'new' data protection regime

By the end of the decade, rapid technological developments and the processes of globalisation challenged European policymakers. They found that the existing legal and regulatory framework structured around the EDPD could neither cope nor offer sufficient harmonisation (European Commission, 2010; European Council, 2011). The adoption of the Lisbon Treaty, and with it, the now-binding EU Charter of Fundamental Rights, provided an opportunity to start promoting a new, comprehensive approach. This new approach would still build on the principles enshrined in the EDPD, yet it would also introduce new principles such as accountability, allow the Commission to further encourage the use of codes of conduct that had rarely been used under the EDPD, and formally establish European certification schemes (European Commission, 2010, pp. 12–13). Achievements reached during the development of such schemes could also enable the European Union to remain a driving force behind global data protection standards (European Commission, 2010, p. 16).

The Commission decided to resolve the legal and regulatory shortcomings of the existing governance framework around data protection by promoting a modernised legal framework (European Commission, 2012). The Commission preferred this alternative over two other alternatives. The first alternative was to amend the EDPD using soft action, imperative communications, and EU-wide self-regulatory initiatives. The second alternative was to establish a central, European data protection authority. The Commission identified that a modernised legal framework could have the potential for a positive impact on the identified policy problems, could not result in high compliance costs, and would not generate strong opposition. [9] The modernised legal framework alternative also included two consistency mechanisms. First, a single DPA would lead the regulation of rule-takers, while permitting other DPAs to object to decisions with pan-European implications through the newly-established European Data Protection Board (EDPB). Second, the Commission suggested awarding itself the competency to enact delegated and implementing acts to ensure, among other outcomes, an openness to future tech-

9. The Commission did, however, adopt from the two unselected policy alternatives the reliance on certification schemes and the abolishment of notification obligations.

nological developments and to give general validity to self-regulatory initiatives such as codes and certifications (European Commission, 2012, pp. 87–93).

When the European Council received the proposal for the GDPR, it started by criticising several decisions made by the Commission. The Council and its delegations primarily disapproved of the Commission's decision to use a regulation instead of a directive. It also criticised the Commission's proposal to give itself the competency to enact implementing and delegated acts, which spread across almost 50 provisions (European Council, 2012a). The Cypriot Presidency and the delegations argued that actions by the EDPB, as well as the use of codes of conduct, could make redundant the reliance on implementing and delegated acts (European Council, 2012b). The Cypriot Presidency also sought to better understand the member states' position on the possible administrative burdens that the proposal had raised, especially on small and medium-sized enterprises (SME), and whether a risk-based approach should be adopted to assess the rule-takers' obligations. The Cypriot Presidency later noticed that the delegations had reached a consensus that a mere horizontal and 'risk-based' obligation would be insufficient, and instead, there was also a need to define, on an article-by-article basis, the exact content and scope of the rule-takers' obligations (European Council, 2012c). For example, it was suggested that a stronger linkage between risk-assessment processes and the articles on codes of conduct and certification would promote their wider use (European Council, 2013a).

One development during deliberations within the Council on Chapter IV of the proposal for the GDPR—which deals with the obligations of rule-takers—was the inclusion of private institutions in the regulatory process. Based on a German proposal, it was suggested that private institutions could receive accreditation from the DPAs based on detailed criteria provided by the GDPR and recommendations made by the EDPB. Accredited private institutions could then monitor rule-takers against approved codes of conduct in exchange for allowing the DPAs to lodge complaints against the institutions, subject them to administrative fines, and revoke their accreditation. As the deliberations continued, the Council also introduced similar provisions for assessing conformity through accredited certification bodies. The delegations further agreed that codes and certifications would confirm compliance with the legal requirement of the GDPR (European Council, 2013b). As the Council moved to discuss Chapter V of the proposal—which deals with the transfer of personal data to non-European countries and organisations—the compromised text explicitly provided that rule-takers could transfer personal information if they applied appropriate safeguards, including the use of approved codes or

certifications. Such appropriate safeguards would not require any additional authorisation from DPAs (European Council, 2014a, p. 3).

The European Parliament had a different approach to certification. [10] It proposed, based on the original suggestion by the Commission, that qualified and impartial auditors accredited by the DPAs could assess rule-takers in order for the DPAs to certify that their processing operations complied with the GDPR. Rule-takers that passed the certification process would receive the European Data Protection Seal, which would be valid for five years (European Council, 2014b, pp. 123–25). The Parliament also suggested that while EDPB could certify that standards for data-protection-enhancing technologies comply with the regulation, the Commission could specify the criteria for awarding certifications, set the accreditation criteria for auditors, and lay down technical standards for certification mechanisms. Following the discussions in the trilogue between the Commission, the Council, and the Parliament, the Council's position was adopted. However, the agreement included provisions for the European Data Protection Seal, and it placed limitations on the time during which accreditation and certifications could be awarded.

4. A comparison between European data protection codes of conduct and certification

As process-tracing shows, policymakers have introduced codes of conduct and certification mechanisms into the new European data protection regime in order to serve similar functions. The codes of conduct and certification mechanisms help rule-takers manage their risk-based obligations, as well as make assurances and apply appropriate safeguards for international data transfers. Additionally, while both codes of conduct and certification have distinct origins within the European data protection regime, both mechanisms emerged with regulatory governance regimes that were structured around enhanced self-regulation via regulatory intermediation that allowed self-regulation in the shadow of European and national hierarchies. Regulators first need to approve the accreditation and certification criteria and then accredit *private* certification and monitoring bodies in order for them to certify and monitor rule-takers according to pre-approved criteria. Some differences between codes of conduct and certification do however exist.

Codes of conduct originated from national data protection legislation and were used as an industry-level, market-based, self-regulatory mechanism. During the

10. With regards to codes of conduct, the European Parliament slightly amended the Commission's proposal but for the most part kept it unchanged (European Council, 2014b, pp. 122-23).

discussion to adopt the EDPD, the Commission suggested repurposing the codes in order to further pan-European implementation, but the Council disagreed and preferred to maintain the codes' national and interpretative characteristics. The limited surplus offered by adopting codes of conduct arguably lowered the stakeholders' interest in relying on the codes. Conversely, during the deliberations about the GDPR, it was the Council that pushed to have codes with European-wide and extra-territorial implementation. The Council saw the codes as a way of contributing to the proper application of the GDPR, thus replacing the need to assign to the Commission the competency of adopting numerous delegated and implementing acts. A combination of institutional regulatory arrangements around the EDPB—the 'one-stop-shop' principle—and the consistency mechanism could now help push national codes to the European level.

Data protection and privacy certification mechanisms, in turn, are mostly considered market-led and self-regulatory. The EDPD did not formally recognise the certification schemes as viable regulatory mechanisms. Nevertheless, given the broad discretion that the EDPD awarded the DPAs, the DPAs could have decided to establish and support their own certification schemes. The Commission, which supported one such DPA-led certification, also introduced certifications into the proposed GDPR. The Commission introduced certification schemes even though the policy option it chose originally did not include certification as a mechanism. The Council then revised the Commission's proposal and ensured that national regulators, and consequently also the EDPB, would replace the Commission in approving the criteria for certification. European policymakers consequently also limited the ability of DPAs to establish certification schemes that did not follow the procedures set out by the GDPR. While private actors might choose to adopt certification schemes that did not receive DPA approval, they have no guarantees that the DPAs would acknowledge the schemes when considering whether they infringed European or national data protection rules.

TABLE 1: A comparison of codes of conduct and certification

	CODES OF CONDUCT	CERTIFICATION
PURPOSE SPECIFICATION	1. To demonstrate compliance (Article 24.3) 2. To contribute to the proper application of the GDPR and to specify its application (Articles 40.1 and 40.2) 3. To safeguard personal data	1. To demonstrate compliance (Article 24.3) 2. To demonstrate compliance with Privacy-by-Design requirements (Article 25.3) 3. To safeguard personal data transfers to third countries and

	CODES OF CONDUCT	CERTIFICATION
	transfers to third countries and international organisations (Article 46.2(e)) 4. To engage in risk-mitigation and risk negotiation (Article 83.2(j))	international organisations (Articles 42.2 and 46.2(f)) 4. To engage in risk-mitigation and risk negotiation (Article 83.2(j)) 5. Cannot be used to certify data protection officers
MODE OF SELF-REGULATION	Voluntary *industry-level* self-regulation	Voluntary *single corporate* self-regulation

The GDPR sets the basic accreditation criteria for both monitoring and certification bodies. Both accreditation processes require that the certification and monitoring bodies would be experienced and independent; would have procedures for assessing the eligibility of rule-takers; would have procedures to handle complaints, and would have no conflict of interest. With monitoring bodies, DPAs are able to define the requirements for accreditation, which the EDPB would then have to approve. Once the requirements for monitoring bodies are approved, the DPAs could accredit them. In addition to the criteria set by the GDPR, certification bodies also needed to show that their procedures could *periodically* assess eligibility, and that they respect the certification criteria. If the member states decided that national accreditation bodies (NABs) would award accreditation—instead of, or together with, DPAs—then the accreditation requirements also needed to complement the requirements set by regulation (EC) 765/2008 and the EN-ISO/IEC 17065/2012 standards. [11]

TABLE 2: A comparison of the accreditation criteria for codes of conduct and certification

	CODES OF CONDUCT	CERTIFICATION
WHO ACCREDITS?	Data protection supervisory authorities	1. Data protection supervisory authorities 2. National accreditation bodies 3. A joint accreditation
WHO SET THE ACCREDITATION CRITERIA?	1. Basic criteria by the	1. Basic criteria by the GDPR (Article

11. The EDPB has clarified that it is best that the DPAs would also follow the requirements set by Regulation (EC) 765/2008 and the EN-ISO/IEC 17065/2012 standards. It reasoned that doing so would contribute to a harmonised approach to accreditation (EDPB, 2018b).

	CODES OF CONDUCT	CERTIFICATION
	GDPR (Article 41(2)) 2. DPAs define requirements for accreditation 3. EDPB approves the requirements	43(2)) 2. Requirements set by either the DPAs or the EDPB 3. Where accreditation is by NABs: 1. EN-ISO/IEC 17065/2012 2. Additional requirements and technical rules set by DPAs and complement Regulation (EC) 765/2008
BASIC CRITERIA FOR ACCREDITATION	1. Independence and expertise 2. Having procedures and structures to assess eligibility 3. Having procedures and structures to handle complaints about infringement 4. No conflict of interest	1. Independence and expertise 2. Having procedures and structures to *periodically* assess eligibility 3. Having procedures and structures to handle complaints about infringement 4. No conflict of interest 5. Respect for the certification criteria
DURATION	Until revocation	Up to five years (renewable) or until revocation

The criteria for approving certification and codes are, or at least should be, distinct from the criteria for their accreditation. The GDPR details several criteria for approving codes. First, codes need to be submitted by a representative body or a trade association. This is to achieve and maintain their industry-level self-regulatory nature. [12] Second, codes need to contain details of their purpose, scope, and applicability. Among other details, the codes must specify the application of the GDPR, facilitate the effective application of the GDPR, and provide sufficient safeguards to mitigate risks (EDPB, 1/2019, pp. 14–17). [13] Third, codes should also consider the specific features and needs of the relevant sector, specifically the

12. Member states, the DPAs, the EDPB, and the Commission can only encourage representative bodies to draw up the codes.

13. Article 40(2) provides 12 non-exhaustive examples for the possible purpose of using codes of conduct. The codes should also indicate 1) how they meet a particular need of a sector or a processing activity; 2) how they facilitate the application of the GDPR; 3) how they specify the application of the GDPR; 4) how they provide sufficient safeguards, and 5) how they provide effective mechanisms for monitoring compliance. (EDPB 1/2019, p. 14). Additionally, in July 2021, the EDPS adopted for public consultation "Guidelines 04/2021 on codes of conduct as tools for transfers". Guidelines 04/2021 specify how codes of conduct can be approved and then used for the purpose of providing appropriate safeguards to transfer data to third countries. The EDPB clarifies that codes can be drawn up only for the purpose of specifying the application of the GDPR ("GDPR codes"), only for the purpose of data transfer to third party countries ("codes intended for transfers"), or for both purposes.

characteristics of the SMEs in that sector. Fourth, while the GDPR uses a terminology that explains that the monitoring of codes *may* be carried out by monitoring bodies, the EDPB (2019) interprets this statement as a requirement. Therefore, the codes need to include mechanisms to enable accredited bodies to monitor compliance. Fifth, the codes should have appropriate review mechanisms to ensure that they remain up to date. Lastly, if the codes can also apply to non-European controllers and processors, they need to include binding and enforceable commitments to apply appropriate safeguards. [14] When codes are ready, the DPAs would review them in order to approve them or to provide an opinion on them. Codes with a European-wide application would also have to be reviewed by the EDPB for the Commission to give them European-wide validity. Codes are valid until they are revoked.

Conversely, the GDPR gives little information on what the criteria are for approving certifications. One major difference, in comparison with the codes, is that the GDPR does not assign exclusivity to the actors who can own certification schemes (EDPB, 2018b, p. 6). Additionally, European policymakers explain that the purpose of certification is to demonstrate compliance with the GDPR. Hence, the EDPB added that certifications should address the data protection principles of lawful processing, data subjects' rights, and the obligations of rule-takers (EDPB, 2018a). Furthermore, as with codes, certifications should also consider the specific needs of SMEs and should require certified rule-takers to provide information and access to certification bodies. [15] Lastly, as with codes, if non-European controllers and processors are allowed to rely on these certifications, the certifications should also include binding and enforceable commitments to apply appropriate safeguards. [16] Once the codes are drawn up, the DPAs or the EDPB need to approve the criteria, and, if the latter, then the certifications may receive the title of 'European Data Protection Seal'. After the certifications are approved, the Commission can specify the requirements to be considered for the mechanisms of the data protection certification. The Commission may also lay down technical standards to promote and recognise these certification mechanisms.

Once both the accreditation and certification criteria are approved, private bodies can be accredited and certified. European policies have therefore clarified who the

14. According to the EDPB, only when the Commission decides that a code has European-wide validity can non-European controllers and processors rely on the code (EDPB 1/2019, p. 21).

15. The EDPB further explained that certifications need to be produced in a transparent manner. They should include supporting documents and descriptions of corrective actions (EDPB 2018a, p. 7).

16. Guidelines 04/2021 only apply to codes of conduct and not to certifications. The EDPB has yet to issue similar guidelines for certifications.

actors are who can award accreditation, assess conformity with certifications, and monitor compliance with the codes. The policies specify that only DPAs, as public bodies, can assess conformity with the accreditation criteria and can accredit monitoring bodies. The monitoring bodies would then monitor compliance with the codes and issue decisions on suspension or exclusion from them. The codes might also allow the monitoring bodies to take additional action against rule-takers. Only monitoring bodies can take such actions. DPAs, in this regard, cannot take appropriate action in cases of infringement of the codes, and they cannot add rule-takers to the codes, or decide who should be excluded from them. DPAs can either investigate whether rule-takers who violated the codes also violated the GDPR, or they can decide to take action against the monitoring bodies. Such actions can include the administrative fines usually aimed at rule-takers. A decision to revoke the monitoring bodies' accreditation does not have to mean that the codes themselves become void.

As with the accreditation of monitoring bodies, only public bodies can accredit certification bodies. However, unlike the codes, the GDPR enables member states to decide whether their DPA, NAB—or both together—would accredit certification bodies. In that regard, NABs usually benefit from having greater expertise in accreditation, while DPAs have greater expertise in data protection. Accreditations for certification bodies are awarded for at least five years and can be renewed. Certifications and codes also differ significantly with regards to the actors who can assess and award certification; both the DPAs and the accredited certification bodies can certify rule-takers. [17] Certifications are awarded for three years. When a certification body decides to award a certification, it has to provide its reasoning to the DPA. DPAs can sanction both the certification bodies and the rule-takers for infringing the criteria. For both, such sanctions can reach 10 million Euro, or 2% of worldwide annual turnover of the preceding financial year of that undertaking.

TABLE 3: A comparison of the certification phase for codes and certification

	CODES OF CONDUCT	CERTIFICATION
WHO MONITORS OR CERTIFIES?	Accredited monitoring bodies	1. Accredited

* This does not take away the authority of DPAs to monitor and sanction rule-takers.

17. The EDPB clarified that certification bodies are accredited locally and are based on the decision about where to offer certifications. When the certification body seeks to certify against European Data Protection Seals, it would need to seek accreditation based on the location of its EU headquarters. Schemes that are intended for a single member state cannot receive the title of a European Data Protection Seal (EDPB, 2018a).

	CODES OF CONDUCT	CERTIFICATION
		certification bodies 2. DPAs
THE FUNCTION OF ACCREDITED BODIES*	1. Monitor compliance 2. Suspend or exclude from the code 3. Other actions or sanctions (as defined in the code)	1. Assessment 2. Issue or renew certification 3. Provide reasons for granting or withdrawing certifications
BASIC CRITERIA FOR CODES OF CONDUCT AND CERTIFICATION	1. Specification for the application of the GDPR (Article 40(2)) 2. Facilitation of the effective application of the GDPR 3. Contain suitable and effective safeguards to mitigate risks 4. Having mechanisms for allowing accredited bodies to monitor and overall effective oversight 5. Consideration for the specific features and needs of market sectors or SMEs 6. For non-Europeans: having binding and enforceable commitments to apply appropriate safeguards 7. When feasible, consultation with stakeholders, including data subjects 8. Review mechanisms	1. Consideration for the specific needs of SMEs 2. Provide information and access to processing activities 3. For non-Europeans: having binding and enforceable commitments to apply appropriate safeguards 4. Specified requirements set by the Commission 5. Technical standards set by the Commission 6. Cannot be used to certify people (e.g., data protection officers)
WHO PREPARES THE CODES OR CERTIFICATION?	1. Member states, the DPAs, the EDPB, and the Commission encourage drawing up of codes	1. The member states, the DPAs, the EDPB, and the Commission encourage the

* This does not take away the authority of DPAs to monitor and sanction rule-takers.

	CODES OF CONDUCT	CERTIFICATION
	2. Associations or bodies that represent rule-takers prepare the codes 3. DPAs provide an opinion on the draft codes or approve them 4. Supranational application: the EDPB also provides an opinion and the Commission gives EU validity (via implementing acts)	establishment of certification mechanisms 2. The DPAs or the EDPB approve the criteria 3. The Commission specifies requirements and defines technology standards
DURATION	Unlimited (until exclusion)	For three years (or until withdrawal)
WHO CAN JOIN THE CODES OR RECEIVE CERTIFICATION?	1. Rule-takers 2. Non-European controllers and processors	1. Rule-takers 2. Non-European controllers and processors
WHO CAN BE FINED UP TO 10 MILLION EURO OR 2% OF WORLDWIDE ANNUAL TURNOVER OF THE UNDERTAKING (ARTICLE 83(4))?	Monitoring bodies	1. Rule-takers 2. Certification bodies 3. Unclear about non-Europeans

* This does not take away the authority of DPAs to monitor and sanction rule-takers.

5. Conclusions

The two case studies of codes of conduct and certification under the European data protection regime have shown that policymakers can establish self-regulation in the shadow of hierarchy by enhancing the regime with regulatory intermediaries. Under this new enhanced data protection regime, rule-takers can only use codes or certifications that have been previously approved by European or national regulators. Rule-takers must also rely on accredited private bodies to monitor the codes and depend on them to assess conformity to certification schemes. Rule-takers can use both mechanisms to manage their risk-based obligations and to show their commitment to applying appropriate safeguards. In addition, rule-takers who adhere to the enhanced codes and certifications may also benefit from the ability to transfer data internationally, knowing that the codes and certifications provide ap-

propriate safeguards (Article 46), and that regulators can consider adherence to codes and certification as a factor for reducing administrative fines (Article 83.2(j)).

Policymakers and regulators can also benefit from the successful adoption of codes or certification and the consequential development of a regime of enhanced self-regulation. Regulators can directly regulate the intermediaries and the benefits and certainty that their mechanisms may provide. Regulators who successfully regulate through the intermediaries can also free up their limited time and resources and indirectly nudge rule-takers towards compliance by tracking the work of the intermediaries, and they only need to respond to cases of noncompliance. Regulators may even decide to disregard or sanction the use of any certification scheme or regulatory intermediation that has not been approved or ratified by European or national regulators. The overall result is that private actors who seek to receive an accreditation undergo a conformity assessment to obtain a certification—or to establish new or join existing codes of conduct—and they must self-regulate in the shadow of hierarchy of European and national regulators.

Differences between the two hierarchical modes of governance do, however, exist. Codes of conduct under the GDPR are a form of industry self-regulation that can enable autonomy as well as reduce the compliance costs for rule-takers. Industry or sectoral codes of conduct only work if trade associations or other bodies that represent a *group* of rule-takers understand that the sector can benefit either from setting best practices or from having consistency in how data protection rules should apply in their sector (Bennett & Raab, 2006, p. 156). The codes would not work if DPAs decided that every violation also meant a violation of the GDPR. Regulators making such a decision might be able to use their full investigative and corrective capacities, yet they risk harming the self-regulatory nature embedded in the codes. Another counterproductive decision might result from the decision to always follow the EDPB's interpretation that the codes *must* have a monitoring body. For instance, if representative bodies seek to establish codes of conduct that consider the specific needs of micro, small, and medium-sized enterprises, then requiring them to establish and finance a monitoring body with detailed procedures for oversight might reinstate the costs that the codes aim to reduce. The flexibility originally embedded in the regulatory intermediation around the codes enables the market to make decisions that reduce costs. Therefore, a careful interpretation should ensure that the costs saved would not be lost by establishing and maintaining the codes.

Conversely, certification is a self-regulatory mechanism that focuses on the individual organisation. Even if certification owners drafted certification criteria and

the regulators approved them, it does not mean that private bodies would adopt them. The ability of DPAs to sanction both certification bodies and certified rule-takers, as well as their ability to order certification bodies how to act, might allow them to have more influence over the certification process. However, these actions might also increase the risk of having too many restrictions, which would disincentivise private actors from relying on certification schemes. Therefore, regulators must ensure that there are sufficient incentives not only for individual organisations to receive certification but also for certification bodies to take the additional risks and costs of assessing conformity and issuing certifications. Each private body that seeks to become a certification body needs to be able to balance the risks and benefits of undergoing a conformity assessment to receive accreditation. Each rule-taker must similarly decide for itself whether to voluntarily undergo a conformity assessment to receive certification. One option DPAs have is to assess how they can rely better on the periodic nature of the accreditation and certification processes with greater confidence. The periodic assessments provide DPAs with more points of interaction with the certification bodies and the certified rule-takers. Therefore, DPAs should balance between their ability to regulate at a distance through accreditation, their ability to regulate at the point of awarding or renewing certifications, and their ability to regulate directly at the point of investigating a possible infringement. A decision to simultaneously use the full investigative and corrective capacities at all three points of decision might unbalance the self-regulatory nature of the certification mechanisms.

This paper therefore refocuses the debate on self-regulation in the shadow of hierarchy around the enhancement of self-regulation via regulatory intermediation and the decisions of the DPAs acting as regulators. It suggests that DPAs should adopt a meta-regulatory approach of regulating at a distance through regulatory intermediation. The paper shows how both codes of conduct and certification under the European data protection regime mix enforced self-regulation, through accreditation and the ratification of criteria, with components of enhanced self-regulation, through regulatory intermediation. It suggests how policymakers and meta-regulators might use regulatory arrangements and decisions to incentivise and constrain intermediaries, and thereafter also the regulated organisations, to self-regulate in the shadow of hierarchical decisions of the meta-regulator.

These above-mentioned comparative analysis and suggestions are, nevertheless, limited by the scope of two case studies, the methodological approach used to study them, and the overall European data protection regime. Hence, future research should adopt a similar methodological approach to trace and assess how

other regulatory regimes use regulatory intermediaries to induce self-regulation in the shadow of hierarchy. Scholars should also address how regulatory arrangements and decisions under other regulatory regimes can either constrain or incentivise both intermediaries and rule-takers to join the regime. Lastly, researchers should study whether and how policymakers and regulators' decisions and actions impact or sanction self-regulatory practices that do not exist under approved hierarchical arrangements that permit rule-takers to self-regulate in their shadows.

References

Abbott, K. W., Levi-faur, D., & Snidal, D. (2017). Theorizing Regulatory Intermediaries: The RIT Model. *The ANNALS of the American Academy of Political and Social Science*, *670*(1), 14–35. https://doi.org/10.1177/0002716216688272

Article 29 Working Party. (2001). *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*.

Article 29 Working Party. (2003). *Opinion 3/2003 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing*.

Article 29 Working Party. (2010). *Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing*.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.

Bennett, C. J., & Raab, C. D. (2017). *The Governance of Privacy: Policy instruments in global perspective* (1st ed.). Routledge. https://doi.org/10.4324/9781315199269

Bignami, F. (2011). Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy. *American Journal of Comparative Law*, *59*(2), 411–461. https://doi.org/10.5131/AJCL.2010.0017

Black, J. (1996). Constitutionalising Self-Regulation. *The Modern Law Review*, *59*(1), 24–55. https://doi.org/10.1111/j.1468-2230.1996.tb02064.x

European Commission. (1992). *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

European Commission. (2003). *Report from the Commission—First Report on the implementation of the Data Protection Directive (95/46/EC)*.

European Commission. (2010). *A comprehensive approach on personal data protection in the European Union*.

European Commission. (2012). *Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the*

processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data.

European Commission. (2020). *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition—Two years of application of the General Data Protection Regulation*.

European Council. (1990). *Protection of individuals in relation to the processing of personal data in the Community and information security*.

European Council. (1991a). *Protection of individuals in relation to the processing of personal data in the Community and information security*.

European Council. (1991b). *Protection of individuals in relation to the processing of personal data in the Community and information security*.

European Council. (1992a). *Protection of individuals in relation to the processing of personal data in the Community and information security*.

European Council. (1992b). *Protection of individuals in relation to the processing of personal data in the Community and information security*.

European Council. (1993). *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

European Council. (1994). *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

European Council. (2011). *Council conclusions on the Communication from the Commission to the European Parliament and the Council – a comprehensive approach on personal data protection in the European Union*.

European Council. (2012a). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*.

European Council. (2012b). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Questionnaire on administrative burdens, delegated/ implementing acts and flexibility in data protection rules for the public sector*.

European Council. (2012c). *Data protection package – report on progress achieved under the Cyprus Presidency*.

European Council. (2013a). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – implementation of risk-based approach*.

European Council. (2013b). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – essential elements of the one-stop-shop mechanism*.

European Council. (2014a). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)—Outcome of the European Parliament's first reading*.

European Council. (2014b). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – partial general approach on Chapter V*.

European Data Protection Board. (2018a). *Guidelines 1/2018 on certifications and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (2016/679*.

European Data Protection Board. (2018b). *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679*.

European Data Protection Board. (2019). *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*.

European Data Protection Board. (2021a). *Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe*.

European Data Protection Board. (2021b). *Opinion 17/2021 on draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE*.

European Data Protection Board. (2021c). *Guidelines 04/2021 on codes of conduct as tools for transfers*.

Galland, J.-P. (2017). Big Third-Party Certifiers and the Construction of Transnational Regulation. *The ANNALS of the American Academy of Political and Social Science*, *670*(1), 263–279. https://doi.org/10.1177/0002716217694589

Gilad, S. (2010). It runs in the family: Meta-regulation and its siblings: Meta-regulation and its siblings. *Regulation & Governance*, *4*(4), 485–506. https://doi.org/10.1111/j.1748-5991.2010.01090.x

Héritier, A., & Eckert, S. (2008). New Modes of Governance in the Shadow of Hierarchy: Self-regulation by Industry in Europe. *Journal of Public Policy*, *28*(1), 113–138. https://doi.org/10.1017/S0143814X08000809

Héritier, A., & Lehmkuhl, D. (2008). The Shadow of Hierarchy and New Modes of Governance. *Journal of Public Policy*, *28*(1), 1–17. https://doi.org/10.1017/S0143814X08000755

Kamara, I., Leenes, R., Lachud, E., Stuurman, K., Lieshout, M., & Bodea, G. (2019). *Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679* [Study]. European Commission.

Leenes, R. (2020). Article 42 certification. In C. Kuner, L. Bygrave, C. Docksey, & L. Drechsler (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 732–743). Oxford University Press. https://doi.org/10.1093/oso/9780198826491.003.0081

Levi-Faur, D. (2011). Chapter 1: Regulation and Regulatory Governance. In D. Levi-Faur (Ed.), *Handbook on the Politics of Regulation*. Edward Elgar Publishing. https://doi.org/10.4337/9780857936110.00010

Loconto, A., & Busch, L. (2010). Standards, techno-economic networks, and playing fields: Performing the global market economy. *Review of International Political Economy*, *17*(3), 507–536. https://doi.org/10.1080/09692290903319870

Loconto, A. M. (2017). Models of Assurance: Diversity and Standardization of Modes of

Intermediation. *The ANNALS of the American Academy of Political and Social Science*, *670*(1), 112–132. https://doi.org/10.1177/0002716217692517

Marotta-Wurgler, F. (2016). Self-regulation and competition in privacy policies. *The Journal of Legal Studies*, *45*(S2), 13–39. https://doi.org/10.1086/689753

Marques, J. C. (2019). Private regulatory capture via harmonization: An analysis of global retailer regulatory intermediaries: Private regulatory capture. *Regulation & Governance*, *13*(2), 157–176. https://doi.org/10.1111/rego.12252

Mayer-Schönberger, V. (1997). Generational Development of Data Protection in Europe. In P. E. Agre & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape*. The MIT Press. https://doi.org/10.7551/mitpress/6682.003.0010

Medzini, R. (2021a). Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society*, 146144482198935. https://doi.org/10.1177/1461444821989352

Medzini, R. (2021b). Credibility in enhanced self-regulation: The case of the European data protection regime. *Policy & Internet*, *13*(3), 366–384. https://doi.org/10.1002/poi3.251

Newman, A. L. (2008). Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. *International Organization*, *62*(01). https://doi.org/10.1017/S0020818308080041

Ogus, A. (1995). Rethinking Self-Regulation. *Oxford Journal of Legal Studies*, *15*(1), 97–108. https://doi.org/10.1093/ojls/15.1.97

Pierson, P. (1996). The Path to European Integration: A Historical Institutionalist Analysis. *Comparative Political Studies*, *29*(2), 123–163. https://doi.org/10.1177/0010414096029002001

Porter, T., & Ronit, K. (2006). Self-Regulation as Policy Process: The Multiple and Criss-Crossing Stages of Private Rule-Making. *Policy Sciences*, *39*(1), 41–72. https://doi.org/10.1007/s11077-006-9008-5

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). *Review of the European Data Protection Directive*. RAND Corporation. https://www.rand.org/pubs/technical_reports/TR710.html.

Schillemans, T., & Busuioc, M. (2015). Predicting Public Sector Accountability: From Agency Drift to Forum Drift. *Journal of Public Administration Research and Theory*, *25*(1), 191–215. https://doi.org/10.1093/jopart/muu024

Schneider, A., & Scherer, A. G. (2019). State Governance Beyond the 'Shadow of Hierarchy': A social mechanisms perspective on governmental CSR policies. *Organization Studies*, *40*(8), 1147–1168. https://doi.org/10.1177/0170840619835584

van den Bulck, H. (2013). Tracing media policy decisions: Of stakeholders, networks and advocacy coalitions. In M. E. Price, S. Verhulst, & L. Morgan (Eds.), *Routledge handbook of media law* (pp. 17–34). Routledge. https://doi.org/10.4324/9780203074572-7

Vander Maelen, C. (2020). Codes of (mis)conduct? An appraisal of articles 40-41 GDPR in view of the 1995 data protection directive and its shortcomings. *European Data Protection Law Review (EDPL*, *6*(2), 231–242. https://doi.org/10.21552/edpl/2020/2/9

Legislation:

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals

with Regard to the Processing of Personal Data and on the Free Movement of Such Data. OJ No. L281, 24 October 1995.

Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. OJ L 218, August 13, 2008.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, April 27, 2016.

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et société

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies