The Europeanisation of data protection law

Abstract:

EU data protection law has, to date, been monitored and enforced in a decentralised way by independent supervisory authorities in each Member State. While the independence of these supervisory authorities is an essential element of EU data protection law, this decentralised governance structure has led to competing claims from supervisory authorities regarding the national law applicable to a data processing operation and the national authority responsible for enforcing the data protection rules. These competing claims, evident in investigations conducted into the data protection compliance of Google and Facebook, jeopardise the objectives of the EU data protection regime. The new General Data Protection Regulation will revolutionise data protection governance by providing for a centralised decision-making body, the European Data Protection Board. While this agency will ensure the 'Europeanisation' of data protection law, given the nature and the extent of this Board's powers it marks another significant shift in the EU's agency-creating process and must therefore also be considered in its broader EU context.

Key words:

Data protection – EU agency – governance – independence – fundamental rights – jurisdiction – applicable law

THE 'EUROPEANISATION' OF DATA PROTECTION LAW

I. INTRODUCTION

EU data protection legislation – the Data Protection Directive[1] – was enacted at a time when the Internet was at a nascent stage of its development and the so-called digital revolution was just beginning.[2] This legislation therefore had the potential to shape the emerging digital society and, in particular, to ensure that exponential increases in personal data processing did not come at the expense of fundamental rights, such as data protection and privacy. Despite this potential, data protection law has, until recently, been viewed as 'marginal and technical' by legal practitioners, policy-makers, academics and industry.[3] This perception is nevertheless changing as data protection has been thrust into the spotlight for a number of reasons. First, the drastic increase in scale of personal data processing has necessarily drawn attention to the legal regime governing its processing. Secondly, the legal framework itself has changed: the entry into force of the Lisbon Treaty[4] in 2009 bolstered the status of data protection within the EU legal order by

* Assistant Professor, Law Department, LSE.

[1] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23.

[2] Opinion of Advocate General Jääskinen in *Google Spain*, C- 131/12, EU:C:2013:424, para 13.

[3] Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (London, 2012), 999.

[4] European Union (EU), Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.

providing an explicit legal basis for data protection legislation[5] while also rendering the EU Charter of Fundamental Rights (the Charter) right to data protection binding on Member States as well as EU institutions and bodies. Thirdly, the Court of Justice of the EU (the Court) embraced data protection's recognition as a fundamental right and has set out to enhance the effectiveness of this right despite the mounting practical challenges to its effectiveness.[6] Indeed, the right to data protection has been instrumental in seminal judgments such as *Volker und Markus Scheke*[7] and *Digital Rights Ireland*[8], leading respectively to the partial annulment and annulment in its entirety of secondary legislation incompatible with this right. Finally, as a result of their enhanced relevance in a digital era, the EU data protection rules have been the subject of a lengthy and contentious reform process that culminated in the adoption of a new General Data Protection Regulation (GDPR) in May 2016.[9] The GDPR will enter into force in May 2018, almost six and a half years after the European Commission's initial proposal.[10]

This intensified interest in, and scrutiny of, the substantive elements of EU data protection law and policy is a welcome development. However, to date, there has been little attention devoted to the governance of data protection law[11], save for the oft-repeated assertion that this body of law is under-enforced.[12] This paper therefore focuses on data protection law from an institutional perspective and seeks to put data protection governance in its EU law context. In particular, it claims that the 'brand new governance model'[13] that the GDPR shall introduce will lead to the 'Europeanisation' of data protection law. As Olsen notes, the term Europeanisation is 'applied in a number of ways to describe a variety of phenomena and processes of change'.[14] The predominant

---

[5] Article 16, TFEU (EU, Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/47).

[6] BJ Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250.

[7] *Volker und Markus Schecke and Hartmut Eifert*, Joined Cases C-92/09 and C-93/09, EU:C: 2010:662.

[8] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, EU:C: 2014: 238.

[9] 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) [2016] OJ L119/1.

[10] European Commission, 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), COM(2012) 11 final.

[11] A notable recent addition to this literature is: H Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016), pp. 325-448.

[12] For instance, the UK Competition and Markets Authority (CMA) highlights in its report the perceived shift in power between individuals and data controllers (who determine the purposes and means of personal data processing) which respondents to its surveys was, in part, as a result of the 'lack of effective enforcement of the current regime. CMA, 'The commercial use of consumer data: Report on the CMA's call for information', CMA38, June 2015, p 169, para 5.51. The challenges to data protection enforcement are outlined by the European Data Protection Supervisor (EDPS). EDPS, Preliminary Opinion of the European Data Protection Supervisor, "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", March 2014, paras 28 and 29.

[13] Article 29 Data Protection Working Party, 'Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)', WP236, 2 Feburary 2016, p 2.

[14] JP Olsen, 'The Many Faces of Europeanisation' (2002) 40(5) Journal of Common Market Studies 921, p 921.

understanding of 'Europeanisation' in the political science doctrine concerns the domestic consequences of European integration.[15] Radaelli therefore states that:

> Europeanisation consists of processes of a) construction, b) diffusion and c) institutionalisation of formal and informal rules, procedures, policy paradigms, styles, 'ways of doing things' and shared beliefs and norms which are first defined in EU policy, processes and then incorporated in the logic of domestic (national and subnational) discourse, political structures and public policies.[16]

However, a second strand of Europeanisation doctrine views Europeanisation as the:

> 'emergence and development at the European level of distinct structures of governance, that is, of political, legal and social institutions associated with the problem solving that formalize interactions among the actors, and of policy networks specialising in the creation of authoritative European rules'.[17]

It is in this latter sense that Europeanisation is understood in this paper: the institutionalisation at European level of a system of governance with the authority to enact European-wide binding rules and to formalise interactions between domestic authorities. This paper claims that the GDPR will lead to the 'Europeanisation' of data protection law. This radical development will be brought about by a shift in the current decentralised application of data protection law to a new centralised system of enforcement.

This development of EU data protection law from a decentralised to Europeanised framework shall be mapped and its potential implications examined. Section two identifies the key characteristics of the current decentralised regime of data protection governance. In particular, it, firstly, highlights the role of 'independent' national supervisory authorities (supervisory authorities) in the data protection governance structure and, secondly, suggests that this decentralised structure enables regulatory competition between these independent supervisory authorities. This decentralised governance model therefore jeopardises one of the objectives of EU data protection law, namely the effective protection of individual rights.[18] Section three charts and analyses the shift from this decentralised model of governance to a centralised institutional framework. It highlights how the newly created European Data Protection Board will facilitate this shift and puts this transformation in a broader context by identifying its potential legal and regulatory ramifications.

II. DECENTRALISED DATA PROTECTION GOVERNANCE

A. The role of 'independent' supervisory authorities in data protection law

[15] Ibid, p 932.
[16] CM Radaelli, 'Europeanisation: Solution or Problem?' (2004) 8 European Integration online papers (EIoP), No. 16, p 3.
[17] T Risse, J Caporoso, and M Green Cowles, 'Europeanisation and Domestic Change. Introduction' in M Cowles, J Caporaso and T Risse (Eds), *Transforming Europe: Europeanisation and Domestic Change* (Cornell University Press, 2001), 3.
[18] See note 1 above, Article 1(1).

Supervisory authorities are the key actors in the current governance system for data protection in the EU. Pursuant to the Data Protection Directive, each Member State must designate one (or several) public authorities to monitor the application of the data protection rules within its territory.[19] These supervisory authorities have a wide range of powers at their disposal and in carrying out their role are said to act as 'ombudsman, auditor, consultant, educator, policy advisor, negotiator and law enforcer'.[20] Irrespective of the national law applicable to a data processing operation, each supervisory authority is competent to exercise its powers on the territory of its own State and may be asked to do so by other Member States.[21] Supervisory authorities also cooperate when necessary for the performance of their duties.[22] A defining feature of supervisory authorities is, however, their independence. According to the Directive, supervisory authorities 'shall act with complete independence in exercising the functions entrusted to them'.[23] This independence is described in the Directive as an 'essential component' of the protection of individuals[24], and this independence must be 'complete'.[25] Yet, the Directive provides little guidance on what independence entails: for instance, it is silent as to how supervisory authorities are independent, and of whom they are independent. Nor does the Directive elaborate on the rationale for this independence. The meaning of independence is therefore 'hard to define'[26] and needs to be parsed.

This lacuna has, to a certain extent, been filled by the Court, which has had the opportunity to adjudicate on the concept of independence on several occasions. A number of conclusions can be reached on the basis of this jurisprudence: independence includes horizontal independence vis-à-vis the State and private parties; independence is broadly construed; and, independence is subject to primary law and thus quasi-constitutional protection.

1. The relational dimension of independence

Independent regulatory agencies originated in the United States in the late 19th century. These agencies were designed to insulate certain public administration duties from the two dominant political parties in the US as these parties were viewed as 'engines of inefficiency, corruption and political favoritism in government administration'.[27] Independence therefore corresponded to independence of control by political parties. Outside of the US context, independence may not serve similar objectives. This begs the question of whom are supervisory authorities independent. It is suggested that their

[19] Ibid, Article 28(1).
[20] C Bennett and C Raab, *The governance of privacy: Policy instruments in global perspective* (MIT Press, 2006).
[21] See note 1 above, Article 28(6).
[22] Ibid, Article 28(6).
[23] Ibid, Article 28(1).
[24] Ibid, Recital 62.
[25] Ibid, Article 28(1).
[26] T Hüttl, 'The content of "complete independence" contained in the Data Protection Directive' (2012) 2(3) *International Data Privacy Law* 137, p 138.
[27] M Shapiro, 'The problems of independent agencies in the United States and the European Union' (1997) 4(2) *Journal of European Public Policy* 276, p 279.

independence might be broadly conceived in two ways: independence at national level (horizontal independence), or independence vis-à-vis EU institutions and agencies (vertical independence). Horizontal independence might further be sub-divided to determine whether supervisory authorities are independent of state organs, public authorities or natural and legal persons.

The Court's jurisprudence has repeatedly confirmed the horizontal independence of supervisory authorities. The Court first had the opportunity to provide guidance on the Directive's independence criterion in *Commission v Germany*.[28] Pursuant to the German system, federal and regional supervisory authorities were divided into two categories: those with responsibility for monitoring the application of data protection rules by public sector bodies, and those with responsibility for overseeing the compliance of private sector bodies and public bodies acting in a market capacity. This latter category – the authorities responsible for monitoring compliance by private entities and state entities acting in a market capacity – were subject to state scrutiny while authorities overseeing public sector bodies were subject to no state oversight and were responsible only to their respective parliaments.

The Commission advocated a broad interpretation of 'independence' and argued that the state scrutiny of supervisory authorities monitoring the data protection compliance of market-based entities was incompatible with the 'complete independence' of these authorities. Complete independence, according to the Commission, entailed freedom from any influence, whether that influence was from other public authorities or from outside the administration.[29] The Federal Republic of Germany proposed a narrow, functional approach pursuant to which supervisory authorities must simply be independent of bodies which are under their supervision, and not independent of other state scrutiny.[30] The Advocate General offered a third approach to defining independence. He disagreed with Germany that the supervisory authority must be independent only of those entities it was supervising.[31] However, in light of the difficulty of enumerating all the factors necessary to satisfy the independence condition, he preferred to adopt a negative approach and to examine whether the state scrutiny at issue breached this condition.[32] He suggested that a purposive approach should be taken to independence and opined that state oversight serves the purpose of ensuring that supervisory authorities act in a rational, lawful and proportionate way thereby promoting the objectives of the Directive.[33] He therefore opined that the Commission had failed to discharge its burden of proving that the state scrutiny had hindered the independence of supervisory authorities and jeopardised the attainment of the Directive's objectives.[34]

The Court, like the Advocate General, rejected the narrow construction of independence advanced by the German government. It held that independence does not exclusively concern 'the relationship between supervisory authorities and the bodies

[28] *European Commission v Federal Republic of Germany*, C-518/07, EU:C:2010:125.
[29] Ibid, para 15.
[30] Ibid, para 16.
[31] Opinion of Advocate General Mazák in *European Commission v Federal Republic of Germany*, C-518/07, EU:C:2009:694, para 22.
[32] Ibid, para 24.
[33] Ibid, para 30.
[34] Ibid, paras 31-35.

subject to that supervision'.[35] Rather, according to the Court, 'complete independence' necessitates 'a decision-making power independent of any direct or indirect external influence on the supervisory authority'.[36] The Court, unlike the Advocate General, did not deem it necessary for the Commission to provide evidence that oversight might hinder the ability of the supervisory authorities to act with complete independence. Rather, it held that 'the mere risk that scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks'.[37]

The Court affirmed this horizontal independence in *Commission v Austria*.[38] Austria's supervisory authority (the DSK) followed the Austrian 'mixed council' administrative model. It was comprised of six members, five of whom were proposed by the Austrian *Lander*, the President of the Supreme Court and authorities representing various professional interests while the sole remaining member – the 'managing member' – was a lawyer working in the federal public administration. DSK members were appointed by the Federal President and the DSK's office was established by the Federal Chancellor, who retained the right to be informed at all time of all aspects of the DSK's work. The Commission initiated infringement proceedings against Austria on the basis that this administrative model was incompatible with the independence of supervisory authorities. Once again the Court agreed, re-iterating that independence is compromised not only by direct influence in the form of instructions but also by any indirect influence which is liable to have an effect on a supervisory authority's decisions.[39] Such independence was lacking in a system where the managing member in charge of the day-to-day operations of the DSK is a federal official, and the managing member's activities 'can be supervised by his hierarchical superior'.[40]

While it has been suggested that a 'one-size-fits-all' global standard for independence is undesirable given national cultural and legal specificities[41], there is doctrinal consensus that horizontal independence of supervisory authorities from organs of the state serves a number of legitimate objectives. Such independence should prevent the State from acting to pursue political objectives, as occurred when the term of office of the Hungarian Data Protection Commissioner was abruptly brought to a premature end in the context of a reorganisation of the supervisory authority in 2011.[42] Moreover, such independence prevents the State from applying data protection law to pursue its self-interest. In *Commission v Germany* the Court suggested that the government may have an interest in data processing operations if it is contractually involved with a private party (for instance, through public-private partnerships) or would like access to private

[35] See note 28 above, para 19.
[36] Ibid.
[37] Ibid, para 36.
[38] *European Commission v Republic of Austria*, Case C- 614/10, EU:C:2012:631.
[39] Ibid, para 43.
[40] Ibid, para 48.
[41] Kuner et al suggest that it is necessary to consider 'the complete legal and political structure of a country before determining whether its data protection regulator is independent' as in some countries a supervisory authority will have more 'clout' if situated within rather than outside a government ministry. Editorial, 'The Intricacies of Independence' (2012) 2(1) *International Data Privacy Law* 1, p 1.
[42] *Commission v Hungary*, C-288/12, EU:C:2014:237.

databases to fulfil its functions.[43] Furthermore, it might be argued that the placement of a supervisory authority within a government ministry may lead to 'administrative supervision' by the ministry and that this in turn may lead to 'anticipatory disobedience' by the supervisory authority.[44] The Court has confirmed however that the overriding objective of such independence is to ensure the reliable and effective oversight of data protection compliance and thus to 'strengthen the protection of individuals and bodies affected by the decisions of [supervisory] authorities'.[45]

This independence must however be counter-balanced by the accountability of supervisory authorities. Szydlo suggests that a failure to ensure such accountability will lead to conflicts in Member States with hierarchical administration models, and thus breach the national identity clause in Article 4(2) TEU.[46] This requirement for oversight stems from the idea that in a democratic society there is a chain of delegation of powers and corresponding accountability between citizens and political actors (government and parliament) and political actors and administrative actors (such as government departments or agencies). Political actors, acting as principals, can delegate to agencies, acting as agents, but remain ultimately accountable to citizens for agency actions.[47] Supervisory authorities may be 'accountable' in various ways ranging from statutory accountability (as they must act within defined statutory limits, and follow strict and transparent rules in exercising their tasks and powers) to personal accountability (an office-holder could be dismissed in cases of serious misconduct). It would also appear reasonable to assume that State organs can exercise oversight vis-à-vis supervisory authorities, for instance, through reporting obligations at defined intervals, or through limited supervision to ensure that a supervisory authority is acting within the confines of its mandate and in accordance with its obligations. Judicial oversight constitutes a final backstop to ensure the legality of supervisory authority actions and their compliance with the State's international legal obligations.[48] Indeed, as Zemánek rightly emphasises, the Union law prerequisites of independence:

> do not cut national authorities off from their social responsiveness (requirements of transparency in public, statutory basis of appointment of the authority's management, competence and accountability vis-à-vis the national parliaments), nor from the check of legality (their decisions may be appealed against through the national courts).[49]

---

[43] See note 28 above, para 35.

[44] P Schütz, 'Comparing formal independence of data protection authorities in selected EU member states', Conference paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference 2012, p 13. See also, M Szydło, 'Principles underlying independence of national data protection authorities: Commission v. Austria' (2013) 50(6) Common Market Law Review 1809, p 1819.

[45] *Maximillian Schrems v Data Protection Commissioner*, C-362/14, EU:C:2015:650, para 41; note 28 above, para 25;note 38 above, para 48.

[46] See note 44 above, p 1822.

[47] D Curtin, 'Holding (Quasi-)Autonomous EU Administrative Actors to Public Account' (2007)13(4) European Law Journal 523, p 525; See Schütz note 44 above, p 4.

[48] A Balthasar, '"Complete Independence" of National Data Protection Supervisory Authorities – Second Try' (2013) 9(3) Utrecht Law Review 26, 34.

[49] J Zemánek, 'Case C-518/07, *European Commission* v. *Federal Republic of Germany*, Judgment of the Court of Justice (Grand Chamber) of 9 March 2010 ECR I-1885 (2012) *Common Market Law Review* 1755, p 1767.

More controversial is the extent of the vertical independence of supervisory authorities vis-à-vis EU institutions and agencies. Supervisory authorities have a hybrid status in the European legal order in so far as they are 'attached to constitutional frameworks of the Member States as well as to that of the European Union'.[50] In *Schrems* the Court recalled the importance of independent supervisory authorities and held that the existence of a Commission decision adopted pursuant to the Directive does not preclude supervisory authorities from examining the compatibility of the same data processing activities with the Directive when they receive a complaint.[51] Although, in accordance with established EU law, only the Court has jurisdiction to declare EU acts invalid[52], supervisory authorities are thus ostensibly not bound by the data protection decisions of the EU Commission and appear to have some level of vertical independence vis-à-vis EU institutions. Whether this vertical independence of supervisory authorities is an essential component of data protection law will become a live issue following the entry into force of the GDPR, as shall be discussed below.

2. A broad interpretation of the notion of 'independence'

Beyond the question of 'relational independence', that is who supervisory authorities are independent of, the Data Protection Directive is also silent as to the requirements of independence. The Court has thus far focused on what has been labelled 'legal' independence – how supervisory authorities are 'set up and structured' so as to be free of undue interference.[53] This 'legal' independence incorporates aspects of functional and organisational independence and while there is no exhaustive list of the requirements of independence, a number of criteria can be deduced from the Court's jurisprudence.

First, there should be no direct or indirect external influence on the supervisory authority and the supervisory authority should neither take nor seek instructions relating to the performance of its duties.[54] In practice, this means that the decisions and other actions of the supervisory authority cannot be made subject to prior approval or be overruled (with the exception of overruling by a court or other pre-established appellate body) and that no other entity can 'decisively influence the supervisory authorities' decisions and other actions, in particular by setting standards for their decisions and actions'.[55] In finding that the level of independence of German supervisory authorities fell short of the requisite standard in *Commission v Germany*, the Court highlighted that the decisions of supervisory authorities could be cancelled and replaced in certain circumstances.[56] The supervisory authority should therefore have organisational independence (for instance, a separate legal personality so that it is not legally part of another public body); independent personnel who are not employed by other public bodies; and adequate financial and informational resources. The Court elaborated on the

[50] H Hijmans, *The EU as a constitutional guardian of internet privacy and data protection*, PhD thesis, University of Amsterdam, 2016, downloaded from UvA-DARE, the institutional repository of the University of Amsterdam (UvA), http://hdl.handle.net/11245/2.169421, p 287.
[51] See note 45 above, para 57.
[52] *Foto-Frost v Hauptzollamt Lübeck-Ost*, C-314/85, EU:C:1987:452.
[53] See note 41 above, p 1.
[54] See note 28 above, para 28.
[55] See note 44 above, p 1818.
[56] See note 28 above, para 32.

financial resources requirement in *Commission v Austria*.[57] Departing from its previous findings[58], it acknowledged that Member States can, from a budgetary law perspective, bring the budgets of supervisory authorities under a specified ministerial department provided that the 'attribution of the necessary equipment and staff' to the supervisory authority does not impede them acting with complete independence.[59] Some of these elements were lacking in the Austrian DSK, for instance the organisational overlap between the DSK and the Federal Chancellery prevented the DSK from 'being above all suspicion of partiality'[60] while the Court also highlighted that the right to information of the Federal Chancellor was far-reaching and 'unconditional'.[61]

Despite the guidance provided by the Court, several questions remain to be clarified. For instance, although the personnel of supervisory authorities must not be employed by other public bodies, it is unclear whether this prevents supervisory authorities from hiring employees from amongst members of a national civil service. On the one hand, it might be argued that close ties with former colleagues in government and state bodies would compromise the de facto independence of the supervisory authority.[62] On the other hand, the majority of supervisory authorities are publicly funded bodies and supervisory authorities might find it more difficult to attract high calibre candidates if they can neither compete with private sector salaries nor recruit from the existing public sector pool.[63] Such logistical problems may be exacerbated in smaller Member States, for instance, Digital Rights Ireland, an Irish civil society organisation, is challenging the independence of the Irish supervisory authority on the grounds, amongst others, that 'the Commissioner and all her office's employees are civil servants'.[64]

A further issue on which clarification may be required is whether the independence of supervisory authorities is compromised by entering into working relationships with private entities. Kuner et al astutely raise this query, highlighting that in future 'there will likely be increased "outsourcing" of compliance and enforcement functions to third parties (including, for example, the management of privacy seal programmes…) with appropriate supervisory authority supervision.' They suggest that in order for such third-party managed schemes to be effective and credible, the third-parties

---

[57] See note 49 above.

[58] In *Commission v Germany* (see note 28 above, para 28) the Court held that the Regulation governing data processing by the EU Institutions and the Data Protection Directive must be interpreted homogenously as they are based on 'the same general concept'. The Regulation governing data processing by the EU institutions provides the EDPS with a separate budget under the general budget of the EU.

[59] See note 38 above, para 58.

[60] Ibid, para 36.

[61] Ibid, para 29.

[62] Schütz, suggests that if supervisory authority officials continue their careers later on in the civil service this may be 'highly problematic in terms of the staffs' de facto commitment, orientation and willingness to comply'. See note 44 above, p 14.

[63] A notable exception is the UK's Information Commissioner's Office (ICO) which is funded through annual notification fees received from data controllers. See: https://ico.org.uk/about-the-ico/our-information/income-and-expenditure/ .

[64] E Edwards, 'Independence of Data Protection Commissioner Questioned', Irish Times, 28 January 2016. Available at: http://www.irishtimes.com/business/technology/independence-of-data-protection-commissioner-questioned-1.2513682 .

themselves must be 'seen to enjoy a high level of impartiality and independence from both governments and private sector interests'.[65]

Of more pressing concern perhaps is the ongoing uncertainty regarding the degree of discretion, and thus independence, supervisory authorities enjoy when exercising their powers. In particular, the extent of a supervisory authority's discretion to determine what data protection violations to pursue, and how best to remedy these violations, remains contested. It would appear that some supervisory authorities wish to take a *de minimis* approach to data protection enforcement. A Dutch tribunal made a reference to the Court querying whether such an approach is compatible with the Directive. It asked whether supervisory authorities are permitted to set priorities which result in no enforcement 'where only an individual or a small group of persons submits a complaint alleging a breach of the directive'.[66] This reference was unfortunately withdrawn before the Court had the opportunity to provide a reply.[67] Such a *de minimis* approach would however ostensibly deprive data subjects of their data protection rights pursuant to the EU data protection rules and, potentially, their right to an effective remedy in accordance with Article 47 of the EU Charter.

This situation – where a supervisory authority rejects individual or small group complaints outright in order to pursue more strategic issues – might be distinguished from a situation where enforcement resources are prioritised following a holistic assessment of the merits of a particular case. Some supervisory authorities have indicated that they may prioritise, or would wish to prioritise, their enforcement resources based on the circumstances of each individual complaint. For example, the UK's Information Commissioner's Office (ICO) may exercise discretion as to whether or not to initiate enforcement action against a data controller following a data protection breach. In exercising this discretion it considers the severity of the breach, how the data controller has dealt with the concerns raised before it and the context of the infringement.[68] Similarly, the Irish Data Protection Commissioner has lamented the diversion of resources from systemic and strategic enforcement priorities to deal with individual complaints. While recognising that individual complaints may entail embarrassment and distress for data subjects, she queried whether each complaint merits a resource intensive investigation and decision, particularly when the data controllers concerned had already taken steps to remedy their breach. The Commissioner suggested that such formal findings may benefit 'digital ambulance chasers' rather than individual data subjects.[69]

It might be argued that such a resource-sensitive approach to formal enforcement – whether used systematically or only on occasion – would put the Irish Data Protection Commissioner (and, by analogy, the ICO) 'on a collision course with the European

---

[65] See note 41 above, p 1.

[66] Request for a preliminary ruling from the Raad van State (Netherlands), lodged on 24 April 2015 (Case C-192/15)[2015] OJ C236/26.

[67] *T. D. Rease and P. Wullems v College bescherming persoonsgegevens*, C-192/15, EU:C:2015:861.

[68] ICO, 'How we deal with complaints and concerns: a guide for data controllers', 1 April 2014. Available at: https://ico.org.uk/media/for-organisations/documents/1561/how-we-deal-with-complaints-and-concerns-a-guide-for-data-controllers.pdf .

[69] See note 64 above.

Commission and the Court'.[70] This view could be supported by the Article 29 Working Party's statement that 'rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved'[71] and the Court's finding that an interference with data protection rights does not depend on whether there has been any material harm or inconvenience to an individual.[72] Yet, a supervisory authority may argue to the contrary that rights continue to be respected and upheld even when formal enforcement resources are prioritised. Such prioritisation may, in fact, lead to a more efficient and effective system of rights protection: the data protection rights of individuals are secured through informal channels where possible and, where not possible, formal resource-intensive proceedings are initiated. The GDPR seems to be support this latter view by leaving the possibility for 'amicable settlement' between controllers and a supervisory authority open. It suggests that when a supervisory authority, which should act as the lead authority in the case of cross-border processing matters, is dealing with a purely domestic matter, the supervisory authority should 'seek an amicable settlement with the controller' and then subsequently exercise its full range of powers if the amicable settlement proves unsuccessful.[73]

3. The 'constitutionalisation' of independence

The expansive and strict interpretation of the notion of independence by the Court has attracted doctrinal debate and criticism.[74] First, the legal basis for such an obligation has been challenged: Zemánek queries whether 'the obligation of Member States to exempt supervisory authorities from their executive hierarchies [can] be based merely on an act of secondary legislation of the Union without its express authorization in the Treaty?'[75] This is particularly so in light of the impact 'complete independence' has on existing administrative structures and balances of power at State level.[76] Furthermore, the Court's interpretation of 'independence' has been criticised for failing to differentiate sufficiently between oversight of public and private sector data processing activities. Balthasar suggests that the 'institutional safeguards needed for a public authority to "act objectively and impartially" with regard to private persons most probably differ fundamentally from those needed with regard to other, in particular higher ranking, public authorities'.[77] He thus implies that the Court has left little leeway to interpret this concept more restrictively in future when the oversight by supervisory authorities of private sector processing activities is at stake. The desirability of such a distinction between public and private sector data processing operations, and the stringency of their oversight, must however be

[70] F Logue, 'Data protection chief must not distance herself from complaints', Irish Times, 9 August 2016. Available at: http://www.irishtimes.com/business/technology/data-protection-chief-must-not-distance-herself-from-complainants-1.2750669
[71] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', adopted on 30 May 2014 (WP218), p 3.
[72] See note 8 above, para 33
[73] See note 1 above, recital 131.
[74] See note 44 above, p 1825.
[75] See note 49 above, p 1762.
[76] See note 49 above, p 1755.
[77] See note 48 above, p 28 fn 9.

questioned in light of data-sharing and the blurring of boundaries between these two sectors.[78]

Perhaps the most significant critique of the Court's stringent interpretation of this notion of independence is that it is out of line with other areas of law and thus arbitrarily offers data protection an elevated level of protection when compared to other fundamental rights. In *Commission v Austria* the Court dismissed the argument that because a supervisory authority is sufficiently independent to satisfy the criteria for judicial independence pursuant to Article 267 TFEU, it should satisfy the criteria for independence for data protection purposes.[79] Instead, it emphasised that the term 'complete independence' must be given an 'autonomous interpretation' based on the actual wording of the provision and the aims and scheme of the Data Protection Directive.[80] While it could be argued that a literal interpretation of the term 'complete independence' necessitates such a broad construction[81], it could equally be claimed that, taken to its logical conclusion, this strict interpretation leads to an untenable practical outcome. As Balthasar highlights, if the independence of courts falls short of that of a supervisory authority then judicial review of supervisory authority actions by courts would, in itself, indirectly but effectively compromise the independence of supervisory authorities.[82] Balthasar thus reaches the damning conclusion that the 'horizontal negative impact' of this strict definition of independence in the data protection context 'seems to be a price which is (too) high for a "premium class" institutional protection of one single fundamental right (which does not even belong to the indispensable essence of human rights).'[83]

It is interesting to note that other rights recognised in the EU Charter, for instance the employment rights protected under Title IV or the right to property protected in Article 17, are subject only to judicial protection and not also to protection by independent specialised bodies with the same institutional safeguards as supervisory authorities. Furthermore, this facet of the protection of the right to data protection has been given primary law status through its incorporation in Article 16(2) TFEU and by anchoring the independence of supervisory authorities to the right to data protection. The Court has affirmed that the independence of supervisory authorities is derived from primary law.[84] However, one might note that the requirement of '*complete* independence' of supervisory authorities is not visible in the 'more realistic' wording of the Charter[85], leaving potential scope for a less onerous interpretation of the concept of independence in the future.

B. Regulatory arbitrage between independent supervisory authorities

A second notable feature of the current system of data protection governance linked, albeit perhaps only indirectly, to the independence of supervisory authorities is that there

[78] Z Bauman and D Lyon, *Liquid Surveillance: A Conversation* (Wiley, 2012).
[79] See note 38 above, para 39.
[80] Ibid, para 40.
[81] See note 44 above, p 1818.
[82] See note 48 above, p 29.
[83] Ibid, 31.
[84] See note 45 above, para 40.
[85] See note 48 above, p 38.

is significant 'regulatory arbitrage' between these institutions. Pursuant to the system established by the Data Protection Directive, each national supervisory authority is responsible for the enforcement of data protection law within its own territory.[86] As a result, supervisory authorities work, to a large extent, independently of one another and of vertical oversight by the European Commission or other EU institutions. Despite its name, the European Data Protection Supervisor (EDPS) has no centralised power of supervision over supervisory authorities: it is responsible solely for ensuring that EU institutions and agencies comply with the rules governing personal data processing applicable to the EU Institutions.[87] Likewise, the Article 29 Working Party, a body comprised of a representative of each of the national supervisory authorities, should, according to its mandate, act merely in an advisory capacity.[88] This lack of centralised oversight and coordination of the activities of the supervisory authorities has proven to be problematic in two particular ways: it has led, firstly, to suboptimal enforcement of the data protection rules in transnational contexts, and, secondly, to regulatory arbitrage between independent supervisory authorities who wish to tackle the same data processing problems in distinct ways.

In transnational situations implicating multiple supervisory authorities the current decentralised system of enforcement by independent Supervisory authorities has come under pressure. This is because cooperation between supervisory authorities is 'not "institutionalised" through clear rules and strict time frames but takes place at a rather informal level'.[89] This is best illustrated by reference to the response of supervisory authorities to Google's 2012 changes to its privacy policy. Following these changes, Google's distinct privacy policies for each of its services (for instance, services such as Gmail, Google +, Google Maps and YouTube) were replaced by a merged privacy policy applicable to all Google's services. While this change had the potential to benefit users by providing them with a single comprehensive document outlining Google's privacy policy for all services, it also risked falling foul of data protection principles.

Google was initially contacted by the Article 29 Working Party prior to the enactment of these changes, and asked to stall the roll-out of its new policy while a coordinated procedure, led by the French supervisory authority (the Commission Nationale de l'Informatique et des Libertés – CNIL), was undertaken.[90] Following this initial investigation, during which the CNIL sent Google two questionnaires 'on behalf of the Article 29 Working Party'[91], the Article 29 Working Party then composed a letter to

---

[86] See note 1 above, Article 28(1).

[87] Article 41, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.

[88] See note 1 above, Article 29(1).

[89] A Giurgiu and TA Larsen, 'Roles and Powers of National Data Protection Authorities' 2016 (3) European Data Protection Law Review 342, p 344.

[90] Article 29 Data Protection Working Party, Letter to Google Inc. CEO Larry Page, 2 February 2012, Ref. Ares (2012)123126-02/02/2012, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf .

[91] Letter from CNIL President Isabel Falque-Pierrotin to Google Inc CEO Larry Page, 27 February 2012, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120227_letter_cnil_google_privacy_policy_en.pdf .

Google outlining its main findings.[92] In particular, the Article 29 Working Party highlighted two main shortcomings of this revised, amalgamated policy. First, it suggested that the policy lacked transparency as it provided users with vague and incomplete information regarding their personal data processing.[93] Secondly, it suggested that the aggregation of personal data of Google's users from across Google's services was incompatible with established data protection principles such as purpose limitation[94] and, in some instances, lacked a legal basis. The Article 29 Working Party therefore set out a number of recommendations for Google.[95] When Google failed to implement these changes after several months, the Article 29 Working Party established a taskforce with representatives from six supervisory authorities to consider the privacy policy's compliance with respective national laws. Google then met with representatives of the taskforce and identified measures it would take to fulfil the Working Party's original recommendations. Meanwhile, the six supervisory authorities also issued separate data protection recommendations to ensure compliance with national data protection rules.[96] The following year, Google was notified by the Article 29 Working Party of a number of further recommendations that had been agreed by supervisory authorities.[97] Google identified steps it would take to address these concerns, while continuing to engage with supervisory authorities in order to implement these changes and ensure compliance with the domestic rules.[98]

This process highlights some of the shortcomings of the current system of decentralised enforcement. First, although the Data Protection Directive was enacted as an instrument of maximum harmonisation to facilitate the free flow of personal data in the EU by limiting national legislative divergences[99], this procedure gives the impression that data controllers must still comply with distinct laws and enforcement procedures across EU Member States. For instance, in the context of this investigation the CNIL lamented that, contrary to Google's suggestion, it had failed to 'pre-brief' all authorities, and that those that were informed only heard about the changes a few days before they were publicly announced.[100] Secondly, in the absence of a pan-European regulator to enforce the data protection rules, an ad hoc transnational enforcement system involving a

---

[92] Article 29 Data Protection Working Party, Letter to Google Inc. CEO Larry Page, 16 October 2012, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf .

[93] See note 1 above, Articles 10 and 11.

[94] Article 6(b). According to this principle, data must be collected for specific purposes and cannot be processed for other incompatible purposes.

[95] Article 29 Data Protection Working Party, Appendix: Google Privacy Policy – Main Findings and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_google_privacy_policy_recommendations_cnil_en.pdf .

[96] For instance, the ICO informed Google that the changes did not comply with the UK Data Protection Act 1998 and Google therefore implemented changes in two stages, while in dialogue with the ICO, to conform to the UK law. ICO, 'Google to change privacy policy after ICO investigation', 30 January 2015. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/01/google-to-change-privacy-policy-after-ico-investigation/ .

[97] Article 29 Data Protection Working Party, Letter to Google Inc. CEO Larry Page, 23 September 2014, Ref. Ares(2014)3113072 - 23/09/2014, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

[98] For a timeline of the Google investigation see note 96 above.

[99] *ASNEF*, C-468/10, EU:C:2011:777, para 29.

[100] See note 91 above.

to-and-fro between supervisory authorities and the Article 29 Working Party was created. Therefore, while the Article 29 Working Party originally took the initiative to contact Google, it was the supervisory authorities, led by the CNIL, which conducted the preliminary investigation before the Article 29 Working Party again took the lead by addressing a series of recommendations to Google. However, this ad hoc mechanism exposed the weakness of the current enforcement regime. When Google failed to react to the Article 29 Working Party's recommendations, it fell upon the supervisory authorities to initiate their formal proceedings against Google. In the absence of a legal basis, Google had no obligation to recognise the authority of the Article 29 Working Party or to comply with its recommendations. Moreover, the Article 29 Working Party seemingly failed to recognise these institutional and substantive limits to harmonisation. For instance, the Working Party suggested to Google that it 'must meet its obligations with respect to the European and national data protection legal frameworks', thereby implying that there is a supranational body with the power to apply the rules directly to a private entity like Google and that the Data Protection Directive is directly applicable to Google. No such supranational body exists while in order to apply the Directive against a private party before a national court it would be necessary to prove that the relevant provisions of the Directive had direct effect.[101]

A further implication of the current enforcement system is that the vertical independence of national supervisory authorities from EU institutions and bodies facilitates, or at least does little to prevent, regulatory arbitrage between supervisory authorities. According to the Data Protection Directive, a Member State's law applies to a data processing operation where the processing is 'carried out in the context of the activities of an establishment of the controller'[102] in that State and the national supervisory authority is responsible for monitoring 'the application within its territory of the provisions adopted by the Member States pursuant to the Directive'.[103] Although Article 4 of the Directive, and its relationship with Article 28, 'has always been shrouded in a veil of mystery'[104], these provisions were initially understood to mean that the supervisory authority in the place of a data controller's establishment would be competent to monitor the compliance of that data controller with data protection law. However, in the Google investigation referred to above, multiple supervisory authorities sought to apply their national law to Google and to exercise their enforcement powers. The multiple ongoing investigations regarding Facebook's data processing activities reveal similar confusion.

---

[101] The criteria for direct effect (*Van Gend en Loos v Administratie der Belastingen*, C-26/62, EU:C:1963:1) – that a text is clear, precise and unconditional– are ostensibly difficult to satisfy for the open-textured principles set out in the Directive. However, the Court has recognised the direct effect of vaguely worded provisions of the Directive (Art 6(1)(c) and Arts 7(c) and (e)) in Österreichischer Rundfunk and Others, C-465/00, EU:C:2003:294, para 101.

[102] See note 1 above, Article 4(1)(a).

[103] Ibid, Article 28(1).

[104] D Svantesson, 'Article 4(1)(a) "establishment of the controller" in EU data privacy law – time to rein in this expanding concept' (2016) 6(3) *International Data Privacy Law* (pending publication), 1. Svantesson notes in regard to Article 4 that '[n]o one seems to have been quite certain as to exactly what the role of that Article is and how it relates to other provisions; especially how it relates to Article 28 dealing with jurisdiction'.

Facebook – which has its primary European establishment in Ireland – falls under the jurisdiction of the Irish Data Protection Commissioner (DPC) and, consequently, the group Europe-v-Facebook[105] initially submitted its complaints regarding Facebook's data protection compliance to the Irish DPC.[106] The Irish DPC has also audited Facebook's activities in the past[107], and approved Facebook's new Data Use Policy and Terms of Service of January 2015 by audit.[108] Consensus regarding jurisdiction over transnational data processing operations was however lacking. In February 2015 four EU supervisory authorities formed a taskforce to investigate these changes to Facebook's policy while continuing to pursue their ongoing domestic probes into Facebook's data processing practices in some cases.[109] The Belgian supervisory authority therefore published a preliminary report in May 2015 assessing the compatibility of Facebook's new policy with Belgian data protection law.[110] It claimed jurisdiction for this assessment in a 'recommendation' by, firstly, asserting that Facebook Inc (established in the USA) rather than Facebook Ireland is the data controller.[111] It highlighted, for example, that Facebook Inc had launched this new policy and that the policy was applicable globally and not tailored in any way to comply with EU data protection law.[112] Secondly, it noted that Facebook Belgium, which is tasked with public policy and legislative and outreach initiatives, is a subsidiary of Facebook Inc.[113] In *Google Spain* the Court held that Google had a revenue-generating advertising subsidiary established in Spain. In finding that the Spanish supervisory authority was competent to oversee Google's search engine activities, the Court held that Google's search engine activities were activities in the context of this establishment and that the search engine activities could not be decoupled from the advertising activities.[114] The Belgian supervisory authority's argument was therefore that the activities of Facebook's subsidiary in Belgium were inextricably linked to Facebook's social networking service in an analogous way. It therefore initiated litigation against Facebook before its domestic courts, winning its case at first instance. However, Facebook's appeal against this decision on jurisdictional grounds was upheld by the Belgian Court of Appeal, which found that the Irish regulator was competent to oversee Facebook's data processing activities in Belgium.[115] While some supervisory authorities continue to recognise the jurisdiction of the Irish DPC to monitor Facebook's

[105] See http://europe-v-facebook.org/EN/en.html .
[106] See http://europe-v-facebook.org/EN/Complaints/complaints.html .
[107] Data Protection Commissioner, 'Report of Audit – Facebook Ireland Ltd.', 21 December 2011, available at: https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
[108] No documentation on this point is available on the website of the Irish Data Protection Commissioner.
[109] L Essers, 'EU data protection authorities get serious about Facebook's privacy policy', PCWorld, 4 February 2015, available at: http://www.pcworld.com/article/2879872/eu-data-protection-authorities-get-serious-about-facebooks-privacy-policy.html .
[110] SPION and Emsoc, 'From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms', 25 August 2015.
[111] Commission de la Protection de la Vie Privée, Recommandation n° 04/2015 du 13 mai 2015.
[112] Ibid, paras 25 – 31.
[113] Ibid, paras 32 – 35.
[114] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, C-131/12, EU:C: 2014: 317, para 60.
[115] J Fioretti, Facebook wins privacy case against Belgian data protection authority, 29 June 2016, Reuters, available at: http://uk.reuters.com/article/us-facebook-belgium-idUKKCN0ZF1VV .

data protection compliance[116], others have clearly sought to challenge this jurisdiction leading to regulatory competition between national supervisory authorities. For its part, Facebook has on occasion refused to comply with these competing regulatory demands. For example, Facebook suggested that the regulators participating in the taskforce to investigate its new policy are not empowered to investigate it, and on another occasion Facebook refused to answer questions addressed to it by the supervisory authority of Hamburg citing a lack of jurisdiction.[117]

The Court has been asked to adjudicate on these issues in a preliminary reference from Germany in the so-called 'Facebook fanpages' case. In this reference, the referring court highlights that decisions regarding data processing are taken by a parent company that is located outside the EU (Facebook Inc) but that has legally independent subsidiaries in the EU. It also acknowledges that according to Facebook's internal allocation of competences, it is Facebook's Irish subsidiary that is exclusively responsible for personal data processing within the EU.[118] By its questions, the referring court queries whether, in light of this situation, the German supervisory authority can exercise its powers of investigation and intervention, and can address orders to Facebook's German subsidiary that sells advertising and promotes marketing measures to German residents. It also asks the Court to consider the respective responsibilities of supervisory authorities in situations where a first party in one state's responsibility is engaged as a result of its failure to exercise a duty of care by involving a third party in another state in data processing operations. In particular, the Court is asked to consider whether the supervisory authority responsible for overseeing the first party can conduct its own preliminary appraisal of the lawfulness of the processing by a third party although this third party is subject to oversight by another state's supervisory authority. These questions go to the heart of the regulatory competition that has, thus far, impeded the uniform interpretation and application of the EU data protection rules by seeking to delimit more clearly the boundaries between the respective spheres of competence of independent supervisory authorities.

The Court has however already begun to provide guidance on this horizontal division of labour between independent supervisory. In *Weltimmo*[119] the Court was asked to consider the compatibility with EU law of a fine imposed on Weltimmo by the Hungarian supervisory authority. Weltimmo ran a website dealing in Hungarian properties but had its registered office in Slovakia. It advertised properties for free for the first month, charging a monthly fee thereafter. As a result, many advertisers sought to have their advertisements, as well as the personal data processed for these purposes, deleted after one month. Weltimmo failed to honour these requests and continued to charge these advertisers for its services. When the advertisers failed to pay Weltimmo, it provided their personal data to a debt collection agency and, as a result, Weltimmo was

---

[116] For instance, in its 2014 investigation of the legality of Facebook's psychological study of users without consent, the ICO stated that it planned to liaise with the Irish Data Protection Commissioner on the matter. K Fiveash, 'British and European data cops probe Facebook user-manipulation scandal', The Register, 1 July 2014. The ICO has also previously stated that it recognises 'the role of the Irish data protection authority in ensuring Facebook comply with European data protection rules'.

[117] N Graham and J Bentham, 'The slow death of EU forum shopping', Lexology, 7 August 2015, available at: http://www.lexology.com/library/detail.aspx?g=97b1f899-9acf-417a-ba93-2652b6d10cfa .

[118] *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, [2016] OJ C260/18 (pending).

[119] *Weltimmo*, C-230/14, EU:C:2015:639.

fined by the Hungarian supervisory authority for breach of data protection law. Weltimmo's ensuing appeal culminated in the referral of a number of questions regarding the applicable law to the Court.

The Court was asked, in essence, whether Articles 4(1)(a) and 28(1) of the Directive must be interpreted as permitting the supervisory authority of one Member State to apply its national data protection law to a data controller which is running a website dealing in properties in that Member State but whose company is registered in another Member State. The Court endorsed a broad interpretation of the applicable law provisions. It reiterated that a Member State's law applies where the processing is 'carried out in the context of the activities of an establishment of the controller'.[120] It noted that the place of establishment is where the 'real and effective exercise of activity through stable arrangements' takes place and that the legal form of establishment is not decisive.[121] It also found that any real or effective activity – even minimal – could constitute a 'stable arrangement'[122] and that Weltimmo had such an establishment in Hungary.[123] It held that the online publication of the property owners' personal data as well as the use of those data for invoicing constituted processing taking place in the context of the activities pursued by Weltimmo's establishment in Hungary. Therefore, while the Court confirmed in Weltimmo that a supervisory authority cannot exercise its supervisory and sanctioning powers when the law applicable is that of another Member State[124], this territorial restriction was offset by its expansive interpretation of applicable law.

Most recently in *Verein für Konsumenteninformation*[125] the Court was asked, inter alia, to provide guidance on the national data protection law applicable in a dispute between an Austrian consumer protection group and Amazon EU, which has its legal establishment in Luxembourg, regarding transactions concluded on Amazon's German domain name website (www.amazon.de). In its sparse judgment, the Court simply recalled its *Weltimmo* findings that establishment implies the exercise of real and effective activity through stable arrangements[126] and that processing of personal data does not need to be carried out by the establishment but only 'in the context of the activities of the establishment'.[127] It therefore left it to the national court to apply its conclusion that, in the e-commerce context, data processing is

> governed by the law of the Member State to which the undertaking directs its activities, if it shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State.[128]

---

[120] Ibid, para 24.
[121] Ibid, para 28.
[122] Ibid, para 31.
[123] Ibid, para 32.
[124] Ibid, para 57.
[125] *Verein für Konsumenteninformation v Amazon EU Sàrl*, C-191/15, EU:C:2016:612
[126] Paras 75-77.
[127] Para 78.
[128] Para 81.

This conclusion leaves two questions open: first, whether the Court's logic in *Google Spain* can be applied beyond that factual scenario. It is recalled that in *Google Spain* the Court held that if (non-EU) data processing operations by one subsidiary are inextricably linked to the establishment of another (EU-based) subsidiary, the law applicable will be that of the establishment irrespective of where processing takes place. Secondly, it fails to clarify whether, as is implied by the German supervisory authority in the Facebook fanpages case, the law applicable to a data processing operation will be the law of each country where a data controller has an effective establishment.

The Advocate General's Opinion was, however, more illuminating.[129] The Advocate General distinguished between two functions of Article 4: first, to determine whether the Directive applied at all (as occurred in *Google Spain*) and, secondly, to identify which of the potentially relevant Member State laws applied in a given circumstance (as occurred in *Weltimmo*).[130] He recalled that the Directive was founded on an idea of mutual trust and that, according to its *travaux préparatoires*, it seeks to prevent the same data processing operation from being governed by the laws of more than one Member State.[131] In determining the applicable law, it is necessary to have both an establishment and data processing in the context of the activities of that establishment. The Advocate General opined that this second criterion is decisive where an undertaking has establishments in more than one Member State[132] and refused to extend the broad interpretation of this condition in *Google Spain* to the facts before him. He distinguished *Google Spain* by suggesting that the Court's interpretation in that case related to the question of whether the relevant legal framework was applicable or not, and was motivated by its desire to 'prevent Google's processing from escaping the obligations and guarantees provided for by the directive'.[133] He opined that this case concerned the distinct issue of which, among several national laws transposing the directive, is intended to govern the data processing operations and thus involves the identification of the establishment in the context of whose activities the data processing operations are most directly involved.[134]

The generous interpretation of the concept of 'establishment' adopted by the Court in *Weltimmo* and 'processing carried out in the context of the activities of an establishment' in *Google Spain* could therefore both be viewed as an attempt by the Court to ensure that data controllers cannot strategically locate their data processing operations in order to shelter them from oversight by supervisory authorities, or the application of the data protection rules. In this regard, one must agree that 'it does not seem like an exaggeration to say that, to a great extent, it is a concern for the protection of the rights afforded under Articles 7 and 8 of the Charter that has driven the direction of the interpretation' of the Directive's applicable law provisions.[135] As will now be demonstrated, the changes that shall be introduced by the GDPR shall consolidate this enforcement process and this

[129] Opinion of Advocate General Saugmandsgaard Øe in *Verein für Konsumenteninformation v Amazon EU Sàrl*, C-191/15 , EU:C:2016:388.
[130] Ibid, para 110.
[131] Ibid, para 109.
[132] Ibid, para 112.
[133] Ibid, para 124.
[134] Ibid, para 125.
[135] Above note 104, p 10.

fundamental rights protection, thus bringing the 'Europeanisation' of data protection law one step closer to completion.

III. FROM DECENTRALISED TO 'EUROPEANISED' GOVERNANCE

A. The 'centralising' effect of the European Data Protection Board

The GDPR continues to mandate the independence of supervisory authorities. It outlines the criteria required for a supervisory authority to be independent in detail thereby rendering the 'general' independence condition in the Regulation redundant.[136] However, the GDPR departs significantly from the Directive's current decentralised data protection enforcement regime by complementing the increased substantive harmonisation of data protection law it will entail with a new system of governance designed to achieve the uniform application of these rules.

The GDPR, like the Directive, affirms that each supervisory authority shall be competent for the performance of its tasks and the exercise of its powers on the territory of its own Member State.[137] It therefore specifies that only the supervisory authority of a relevant Member State is competent when data processing is carried out in order to comply with a legal obligation, or is necessary for the performance of a task in the public interest or for the exercise of official functions.[138] Moreover, where a complaint submitted to a supervisory authority relates only to a controller or processor established on its territory or substantially affects data subjects only in its Member State, it alone is, in principle[139], competent to handle such complaints.[140] However, the GDPR provides that each supervisory authority shall contribute to its consistent application throughout the Union and shall thus 'cooperate with each other and with the Commission' in accordance with Chapter VII governing cooperation and consistency.[141]

The GDPR therefore stipulates that in investigations involving cross-border data processing, a lead supervisory authority should be designated. The competent lead supervisory authority will be the supervisory authority of the main or single establishment of the data controller or processor.[142] This lead supervisory authority becomes the sole interlocutor of the controller or processor regarding its data processing operations while continuing to cooperate with other supervisory authorities.[143] The lead supervisory authority can request other supervisory authorities to carry out investigations or monitor the implementation of a measure addressed to a controller/processor established in another member state.[144] Moreover, the lead supervisor must submit its draft decisions to other relevant authorities for their input and takes due account of this

[136] Above note 44, p 1820.
[137] Above note 9, Article 52.
[138] Ibid, Article 55(2).
[139] Ibid, Article 56(3).
[140] Ibid, Article 56(2).
[141] Ibid, Article 51(2).
[142] Ibid, Article 56(1).
[143] Ibid, Article 56(6).
[144] Ibid, Article 60(2).

input.[145] The supervisory authority to which a complaint was lodged can also, of its own initiative, submit a draft decision to the lead authority which in turn must take 'utmost account' of this draft decision.[146] Where there is disagreement over a draft decision, and the lead authority does not incorporate the objections of another supervisory authority into its decision, the lead authority must invoke the GDPR's 'consistency mechanism'.[147] The consistency mechanism, as its name suggests, seeks to ensure that consistent application of the GDPR throughout the Union.[148]

The primary actor in this mechanism is the newly established 'European Data Protection Board' (EDPB). The EDPB is an official body of the Union with legal personality[149], composed of the heads of a supervisory authority from each Member State and of the EDPS, or their respective representatives.[150] The EDPB shall adopt binding decisions where the lead authority refuses to incorporate relevant and reasonable objections raised by another supervisory authority in its decision.[151] The EDPB can equally enact such binding decisions to resolve disputes regarding which authority should be designated the lead authority[152] or where a competent authority adopts specified actions without seeking the opinion of the EDPB, or subsequently overlooks its opinion once given.[153] The decision of the EDPB is addressed to the lead supervisory authority and all other supervisory authorities concerned and is binding on all of them.[154] These binding decisions of the EDPB are ordinarily adopted by a two-thirds majority of EDPB members.[155]

The lead supervisory authority or, where relevant, the supervisory authority of the State where the complaint was lodged, must then adopt a final decision based on the binding decision of the EDPB within one month of notification of the EDPB's decision.[156] The final decision of the supervisory authority must refer to the EDPB's decision and attach this decision to its final decision.[157] This final decision is adopted in accordance with the division of labour foreseen for supervisory authorities by Articles 60(7) to 60(9) of the GDPR. As such, the lead authority must communicate a final decision to the data controller or processor based on an EDPB decision while the supervisory authority of the complainant must notify the final decision to it, in keeping with Article 77(2) GDPR.[158] However, where a final decision dismisses a complaint in whole or in part, the supervisory authority of the complainant takes responsibility for

[145] Ibid, Article 60(3).
[146] Ibid, Article 56(4).
[147] Ibid, Article 60(4).
[148] Ibid, Article 63.
[149] Ibid, Article 68.
[150] Ibid, Article 68(3).
[151] Ibid, Article 65(1)(a).
[152] Ibid, Article 65(1)(b).
[153] Ibid, Article 65(1)(c).
[154] Ibid, Article 65(2).
[155] Ibid, Article 65(2).
[156] Ibid, Article 65(6).
[157] Ibid, Article 65(6). It must also specify that the EDPB's decision will be published on the EDPB website (Art 65(6)).
[158] Ibid, Article 77(2). The supervisory authority with which a complaint has been lodged shall inform the complainant of the progress and outcome of a complaint.

notifying this dismissal (or partial dismissal) to both the complainant and the relevant data controller or processor.[159]

Articles 57 and 58, setting out the tasks and powers of supervisory authorities respectively, continue to indicate that each supervisory authority is responsible for monitoring and enforcing the GDPR's application on its own territory[160] and that each supervisory authority is entitled, as part of its corrective powers, to impose an administrative fine pursuant to Article 83 GDPR or other corrective measures.[161] Yet, once the consistency mechanism is engaged it is solely the lead authority that addresses a final decision to the data controller. It would also therefore seem logical to assume, although not expressly stipulated by the GDPR that it is solely that lead authority that can impose an administrative fine on the data controller (and therefore that each supervisory authority that is an addressee of the EDPB decision cannot impose an administrative fine on its own territory). Given the enhanced administrative fines foreseen by the Regulation[162], which are arguably now criminal in nature as a result of their severity, one could query whether the imposition of sanctions by multiple Member States would comply with the principle of *ne bis in idem*. Pursuant to this principle, set out in Article 50 of the EU Charter, '[n]o one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law.' The GDPR does however make explicit the remedies it offers to affected individuals, who can exercise their right to legal redress against the lead or relevant supervisory authority as this final decision is legally binding.[163] In such circumstances, the supervisory authority must simply forward the decision of the EDPB which preceded its final decision to the relevant judicial authority.[164]

It can thus be seen that while supervisory authorities remain competent to tackle 'purely internal' data processing problems, the consistency mechanism ensures that cross-border data processing problems are 'Europeanised'. Such problems are dealt with by endeavouring to reach consensus between the various relevant supervisory authorities and where consensus is wanting, by a binding decision of the EDPB that is then subsequently notified by the lead authority, or another competent authority where relevant. One could therefore conclude that the interpretation and application of the law has become centralised and thus to a large extent harmonised. The driving force behind this centralised harmonisation will be the newly created EDPB. The implications of this new institutional landscape and new dynamic for data protection governance shall now be considered.

B. The consequences of 'Europeanisation'

This centralisation is likely to have significant legal and practical ramifications. Three in particular can be emphasised. First, although the GPDR continues to assert the

[159] Ibid, Articles 60(8) and (9).
[160] Ibid, Article 57(1)(a)
[161] Ibid, Article 58(2)(i).
[162] Ibid, Article 83.
[163] Ibid, Article 78(1).
[164] Ibid, Article 78(4).

independence of national supervisory authorities, this centralisation will reduce the existing independence of these authorities. Secondly, as this centralisation alters the current institutional and legal balance between the EU and Member States in the field of data protection it may raise issues of subsidiarity and national identity. Finally, the creation of the new EDPB as an independent EU agency with the power to enact binding decisions on normative rather than purely technical issues may raise queries regarding its accountability and democratic legitimacy.

1. Curtailing the 'complete independence' of national supervisory authorities

To date, national supervisory authorities have had horizontal independence vis-à-vis domestic public institutions, private parties and their international counterparts. Supervisory authorities have also enjoyed vertical independence vis-à-vis EU institutions and bodies: as discussed above, neither the EDPS nor the Article 29 Working Party could bind a national supervisory authority through its decision-making. If the European Commission deemed a decision of a supervisory authority to be unlawful and incompatible with the EU data protection rules, it could merely initiate infringement proceedings against that Member State for breach of its obligations to respect EU law.[165] Only national courts could annul decisions of a national supervisory authority on the grounds that they were incompatible with EU law, or where that assessment raised questions regarding the interpretation (or validity) of EU data protection law they could refer preliminary questions to the Court of Justice.[166]

The EDPB's ability to address binding decisions to supervisory authorities therefore alters the existing legal balance, for instance, by rendering largely redundant the Commission's competence to initiate infringement proceedings against a State for the failure of one of its organs to respect EU law. Given that national supervisory authorities will be required to respect the terms of a binding EDPB decision in all contentious cross-border disputes, there will be less scope for such a breach of EU data protection law in the first instance.

However, these new EDPB powers will also alter the extent of the independence of supervisory authority decision-making. The Article 29 Working Party warned against this possibility suggesting that consistency should not 'encroach upon the independence of national supervisory authorities and should leave the responsibilities of the different actors where they belong'.[167] However, as Hijmans notes, when the EDPB uses its binding powers 'the national DPAs are no longer sovereign to ensure the control of the EU rules on data protection'.[168] Supervisory authorities will, henceforth, take direct and binding instructions from the EDPB thereby limiting their vertical independence vis-à-vis this EU agency. Therefore, a supervisory authority may be compelled to enact a final decision based on an EDPB decision and address this to a data controller or processor even if it disagrees with the substantive findings of that decision. In such circumstances, the only option for a supervisory authority to assert its independence vis-à-vis the EDPB

[165] Article 258 TFEU.
[166] Article 267 TFEU.
[167] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals', WP 191, 23 March 2012, 20.
[168] See note 12 above, p 386.

would be to ignore its binding opinion and address a distinct final decision to the alleged wrongdoer. The GDPR does not envisage such a situation. However, in such circumstances, the European Commission could take infringement proceedings against the Member State concerned. It is unclear whether other relevant supervisory authorities could take any legal action to enforce the EDPB's decision while such proceedings are pending. This scenario also reveals that the new consistency and cooperation mechanisms continue to require a limitation of the horizontal independence of supervisory authorities vis-à-vis one another by putting an end to the regulatory competition discussed above.

In light of these curtailments to the independence of supervisory authorities, an 'essential element' of the right to data protection, one might query whether this new governance mechanism is compliant with EU primary law. However, if a teleological approach is taken to the interpretation and application of the criterion of independence the changes brought about by the GDPR are ostensibly compatible with primary law. The independence requirement is 'not an end in itself but rather a means to achieving higher-level objectives'.[169] Szydlo suggests that independence enhances efficiency as independent supervisory authorities have 'incomparably greater chances to perform their tasks efficiently' as they can 'focus solely on their main mission (without dispersing their resources across activities not related to data protection), and may autonomously set their own priorities'.[170] However, the Court has emphasised the role of independence in ensuring effective and reliable individual rights protection and has suggested that independence 'must be interpreted in light of that aim'.[171] As discussed above, the current lack of substantive and procedural harmonisation of data protection law is leading to regulatory competition between supervisory authorities and an unequal level of data protection throughout the EU. This plurality of national administrative practices could, as Zemánek suggests, jeopardise the 'entire *effet utile* of the Union regulatory framework' in a manner that is incompatible with the protection offered by the EU Charter.[172] The Court has equally, when interpreting other provisions of EU data protection law, repeatedly emphasised the need to interpret data protection requirements in a manner which enhances the effectiveness of these rules.[173] It is therefore suggested that while the centralisation of data protection governance will limit the independence of national supervisory authorities, this centralisation is compatible with EU law as independence must be interpreted in a teleological way that enhances the effectiveness of individual rights protection.

2. The compatibility of the EDPB with general principles of EU law

Subsidiarity is a general principle of EU law, provided for by Article 5(3) TEU. According to this principle, the EU shall only act in areas which do no fall within its exclusive competence 'if and so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States' and can be better achieved at Union level because of their scale and effects. In *Commission v Germany*, Germany had argued that it

[169] See note 44 above, p 1815.
[170] Ibid, p 1816.
[171] See note 44 above, para 41.
[172] See note 49 above, p 1766.
[173] See note 114 above, paras 30,34, 38, 53, 58 and 84.

would be contrary to the principle of subsidiarity to require it to abandon an administrative system for data protection that had been established almost 30 years previously. In support of its claim it relied upon paragraph 7 of the Protocol on Subsidiarity and Proportionality, which provides that 'care should be taken to respect well established national arrangements and the organisation and working of Member States' legal systems.[174] The Court however rejected this argument simply reiterating that the requirement that supervisory authorities are free from State scrutiny does not go beyond what it is necessary to achieve the Treaty objectives.[175] Balthasar suggested that the Court's disregard for the principle of subsidiarity and the strict interpretation of 'independence' led to concerns that independent supervisory authorities were 'only a first step to direct administration by Union authorities, and therefore a political aim not fully backed by the Treaties'.[176] Similarly, Chiti notes that the process of agencification 'directly and indirectly influences the structure and functioning of national administrative systems'.[177]

Nevertheless, although the EDPB may bring us one step closer to such 'direct administration by Union authorities', very few Member States took action pursuant to the 'Subsidiarity Protocol'[178] to protest against this development. The Commission's original proposal provided the Commission with extensive powers of intervention vis-à-vis national supervisory authorities, such as the power to compel the supervisory authority to suspend the adoption of a decision[179] or to enact implementing acts to overrule a supervisory authority.[180] Yet, despite this extensive interference by the Commission with the independence of national supervisory authorities only one national parliament (the Swedish) and four national parliamentary chambers[181] opposed the proposal. It is possible that given that the EDPB is to replace the existing and well-established Article 29 Working Party Member States viewed this governance development as a minor one, despite the extensive powers of the EDPB.

Equally, the EDPB's intergovernmental (or representative) composition may help to alleviate subsidiarity concerns by providing all supervisory authorities with a voice and a vote at the EDPB table. Indeed, doubt has been cast as to whether such representative bodies can truly be independent of their 'home' constituencies[182] and, unlike other independent agencies which are 'acting in the Union interest alone' or 'in the sole interest

---

[174] See note 28 above, paras 53 and 54.
[175] Ibid, para 55.
[176] See note 48 above, p 33.
[177] E Chiti, 'An Important Part of the EU's Institutional Machinery: Features, Problems and Perspectives of European Agencies' (2009)46 Common Market Law Review 1395, p 1410.
[178] Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality [2004] OJ C310/07.
[179] European Commission, 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) COM(2012) 11 final. Art 60(1).
[180] Ibid, Article 62(1)(a).
[181] Namely, the German Upper House, the Belgian House of Representatives, the French Senate, and the Italian Chamber of Deputies.
[182] Busuioc suggests that European agencies which are largely composed of Member State representatives are 'problematic in terms of possible risks of paralysis and conflict' and 'creates the potential for tremendous conflicts of interests'. M Busuioc, 'Rule-Making by the European Financial Supervisory Authorities: Walking a Tight Rope' (2013) 19(1) European Law Journal 111, p 120.

of the Union'[183], there is no such reference in the GDPR regarding the EDPB. Indeed, Busuioc suggests that groups of national supervisors could thwart agency rule-making and queries '[w]ho safeguards and polices that members of the board of supervisors act *in the sole interest of the Union rather than act as vessels for a variety of national interests?*'.[184]

It is important to recall that despite over two decades of data protection legislation in the EU, there remains a lack of consensus regarding the normative objectives of this legislation and its place within the broader framework of the digital economy and digital rights. In other fields of EU law, institutional design decisions have exposed the 'deep-set constitutional, institutional and political fault-lines'[185] which underpin the relevant system: data protection law is unlikely to be any different. The EDPB's intergovernmental composition is therefore equally likely to lead to 'coordination problems'. In particular, it would seem likely that 'policy issues will arise at EU level[s] before they have solidified and been coordinated at national levels'.[186] The EDPB will therefore function as a driver to force consensus, irrespective of whether this reflects the national identity of the Member States concerned. Indeed, Zemánek already speaks of 'normative permeability' in this field as a result of the dialogue between national supervisory authorities. He distinguishes this dialogue from that taking place in sectoral administrative agencies, suggesting that it goes further than a 'narrow "expertocratic" self-governing approach, and detects rather the idea underlining the cooperative partnership as a part of the *European constitutional union*, which is based on shared values'.[187] This observation forces one to consider a further potential concern regarding the activities of an independent EDPB: in other sectors, the use of 'independent regulatory agencies' and centralised boards is ordinarily limited to technical matters, or in normative areas agencies tend to exercise restricted functions[188], whereas in the data protection context the EDPB is equipped with extensive powers to engage in an inherently normative decision-making field. This, in turn, may lead to concerns regarding the democratic legitimacy of the EDPB.

3. The democratic legitimacy of the EDPB

EU agencies may be defined as 'specialized, non-majoritarian bodies, established by secondary legislation, which exercise public authority and are institutionally separate

---

[183] Ibid, fn 44.
[184] Ibid, p 121.
[185] N Moloney, 'Institutional Governance and Capital Markets Union: Incrementalism or "Big Bang"' ECFR 2/2016 376, 384.
[186] See note 27 above, p 283.
[187] See note 49 above, p 1767.
[188] For instance, the purpose of the 'European Union Agency for Fundamental Rights' is to 'provide the relevant institutions, bodies, offices and agencies of the Community and its Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights'. Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights' [2007] OJ L53/1. The Agency thus 'follows the model of a European information and coordination agency'. A Hinarejos, 'A Missed Opportunity: the Fundamental Rights Agency and the Euro Area Crisis' (2016) 22(1) European Law Journal 61, 63.

from the EU Institutions and are endowed with legal personality'.[189] Following the creation of two independent informational agencies in 1975, there was a lull in the establishment of agencies until two further waves of agency-creation in the 1990s and 2000s.[190] At present, there are over 30 'decentralised agencies', that have been established to 'perform technical and scientific tasks that help the EU institutions implement policies and take decisions'.[191] These agencies have been described as a 'relatively new attempt to cope with societal challenges that elude traditional models of governance'.[192] It is possible to distinguish between EU agencies from a functional perspective, and agencies could be said to sit on a spectrum between information-providing agencies, at one end, and quasi-regulatory agencies, at the other.[193] In between these two extremes there are agencies which ensure operational cooperation between authorities and decision-making agencies. While the legal basis for the establishment of some EU agencies is questionable[194], and although the creation of the EDPB is not foreseen by the Treaties[195], Article 16(2) TFEU does provide that compliance with the data protection rules 'shall be subject to the control of independent authorities' without further specifying whether these authorities should be national or supranational or both.

The Court has had the opportunity to assess the legality of delegating EU institutional powers to agencies on numerous occasions. In the seminal *Meroni*[196] judgment, the Court laid out a doctrine which remains, formally at least, good law today.[197] Pursuant to the *Meroni* doctrine, only clearly defined, executive powers can be delegated under the Treaty while discretionary powers cannot be delegated. This doctrine has been interpreted to mean that

> the setting up of Community offices endowed with legal personality may be considered legitimate under the Treaty only if necessary in order to carry out the objectives connected to the Community powers and does not imply any delegation of powers involving a real margin of discretion.[198]

Agencies are therefore lawful provided they exercise non-discretionary powers and do not adopt acts of a regulatory nature.[199] This coincides with the rationale for EU agencies – that by delegating technical tasks to those with expertise, administrative efficiency can

---

[189] M Busuioc, *European Agencies: Law and Practices of Accountability* (OUP, 2013), p 21 (emphasis removed).
[190] Ibid, p 14.
[191] See further: https://europa.eu/european-union/about-eu/agencies_en .
[192] See note 44 above (Schütz), p 2.
[193] See note 189 above, p 38.
[194] Maloney, notes that the use of Article 114 TFEU as a legal basis for the ESAs is a 'somewhat shaky competence for a radical institutional reform'. N Maloney, 'The European Securities and Markets Authority and Institutional Design for the EU Financial Market – A Tale of Two Competences: Part (1) Rule-Making' (2011)12(1) *European Business Organisation Law Review* 41, 49.
[195] Unlike, for instance, Article 105(1) which explicitly foresees that the Commission can ensure the application of the treaty Competition law provisions.
[196] *Meroni*, C559/14, EU:C:2016:349.
[197] Busuioc argues that the financial supervisory authorities' rule-making powers 'stretch the boundaries of the legal doctrine to the maximum'. See note 182 above, p 114.
[198] See note 177 above, p 1421 and the references cited in fn 74.
[199] See note 189 above, p 19.

be enhanced.[200] However, the Meroni doctrine has ostensibly become increasingly marginalised following recent legal and practical developments. From a legal perspective, the Court reiterated in *Romano* that the legislature was prohibited from empowering a body other than the Commission to 'adopt acts having the force of law'.[201] However, in its more recent 'Short Selling' judgment[202], the Court rejected the UK government's argument that one of the ESAs (the European Securities Market Authority – the ESMA) had been given broad discretionary tasks, breaching the *Meroni* (and *Romano*) limits. The Court acknowledged that under 'strictly circumscribed circumstances' the ESMA is required to adopt measures of general application but held that the provision setting out this requirement is not at odds with the Romano judgment. The Court recalled that 'the institutional framework established by the TFEU, in particular the first paragraph of Article 263 TFEU and Article 277 TFEU, expressly permits Union bodies, offices and agencies to adopt acts of general application'.[203]

From a practical perspective, it is 'extremely difficult to define a clear typology for the classification of each non-majoritarian agency in a homogenous category'.[204] However, as Busuioc highlights, the quantitative and qualitative change in agencification reached its peak in 2010 following the creation of three new agencies in the financial sector (the European Supervisory Authorities, or ESAs).[205] These ESAs 'break the mould' as a result of the heavy emphasis on their independence as well as their powers to 'direct binding decisions to national supervisory authorities as well as to overrule them' in exceptional circumstances.[206] Although the EDPB can be distinguished from these ESAs in various ways (for instance, unlike the ESAs the EDPB does not have the power to issue decisions directly to individual financial institutions in a member state), the EDPB could be said to mark a further significant step in this existing 'agencification'. Chiti suggested, in 2009, that European agencies are a 'peculiar organizational arrangement, distinct from other contiguous models of the EU administration', including EU independent authorities.[207] He therefore suggested that even 'those EU agencies expressly qualified as independent by establishing regulations' are not independent as a result of their direct and indirect influence from the Commission and the private sector.[208] It is suggested, however, that the EDPB marks a departure from Chiti's framework as a result of the extent and nature of its powers.

First, the powers of the EDPB, once the dispute resolution mechanism in the GDPR is invoked, are extensive. This mechanism is engaged, as outlined above, when consensus cannot be reached between supervisory authorities regarding the designation of the lead supervisory authority[209] or the substance of a decision with transnational

---

[200] As Curtin suggests, the 'necessity to bring expertise into the public policy process, or to ensure its credibility, features prominently in the motivations attributed to those who promoted this new trend [of decentralised agencies] in Europe'. See note 47 above, p 527.
[201] *Romano*, C-98/80, EU:C:1981:104, para 20.
[202] *United Kingdom v Parliament and Council ('Short Selling')*, C-270/12, EU:C:2014:18.
[203] Ibid, paras 64 and 65.
[204] See note 47 above, p 527.
[205] See note 189 above, pp 14-15.
[206] See note 182 above, p 112.
[207] See note 177 above, p 1398.
[208] Ibid, pp 1399-1400.
[209] See note 9 above, Article 65(1)(b).

implications.[210] Pursuant to Article 64, any supervisory authority, the Chair of the EDPB or the Commission can request that 'any matter of general application or producing effects in more than one Member States be examined by the Board'.[211] The EDPB then adopts an opinion on that matter.[212] However, where the relevant supervisory authority indicates to the EDPB that it does not intend to follow its opinion, in whole or in part, the dispute resolution mechanism is engaged[213] and the EDPB can issue a decision that binds the supervisory authority.[214] It would therefore appear that, unlike other EU agencies, the decision-making powers of the EDPB include, but are not limited to, individual decision-making (ie applying general rules to specific cases) but extend to 'any matter of general application' and are therefore regulatory in nature. Moreover, the EDPB will also act as a 'quasi rule-maker' as it has the power to adopt soft law measures (guidelines, recommendations and best practices) of its own initiative or at the request of an EDPB member or the Commission on 'any question covering the application of [the] Regulation'.[215]

Secondly, the nature of the power exercised by the EDPB is also noteworthy. It is suggested that the EDPB shall engage in normative, rather than neutral technical or scientific, decision-making. The extent to which the activities of independent regulatory agencies can be neutral has been questioned.[216] Shapiro, for instance, highlights that even informational agencies – the least interventionist form of agency from a functional perspective – can have political influence for 'as soon as information becomes highly relevant to policy outcomes, the information and the information gatherers cease to be defined as neutral and objective and are redefined as part of the political struggle'.[217] Indeed, many areas in which independent agencies operate are linked to long-term policy-making objectives (for instance energy policy is linked to environmental protection) and therefore necessarily involve 'public policy design and management in one way or another'. [218] Florio argues that the balancing of policy objectives is a core function of government and cannot be delegated to independent regulators alone.[219] The tensions between data protection policy and other societal interests, such as innovation, and rights, such as freedom of expression and freedom of information, are well-documented.

---

[210] Ibid, Article 65(1)(a).
[211] Ibid, Article 64(2).
[212] Ibid, Article 64(3).
[213] Ibid, Article 64(8).
[214] Ibid, Article 65(1)(c).
[215] Ibid, Article 70(1)(e). It can also issue guidelines, recommendations and best practices in a number of other situations (see, Article 70(1)(d),(f),(g),(h),(i),(j) and (m)).
[216] Chiti, for instance, states that even the instrumental powers conferred on EU agencies may be less notable than those granted to other EU administrations but not necessarily less relevant. See note 177 above, p 1405.
[217] See note 27 above, p 284.
[218] Massimo Florio, *Network Industries and Social Welfare: The Experiment that Reshuffled European Utilities* (OUP, 2013), p 351. Similarly, Shapiro notes that 'activities which in the abstract and/or most of the time are perceived as non-discretionary, managerial and technical will be reconstituted in the public perception as discretionary and political when they produce results that are significant to public policy choices or to the clash of political interests'. See note 27 above, p 284.
[219] Ibid (Florio), p 351.

Normative decision-making is therefore inevitable in a hybrid policy area like data protection in which the regulated 'asset' – personal data – is both of economic and dignitary value. Szydlo implies that there is an 'axiological convergence' between data protection and other areas in which sector-specific regulators operate as a result of this nexus between economic and social regulation in data protection law. This, in turn, he suggests 'might justify the convergence between these two kinds of authorities on the institutional plane'.[220] However, the data protection governance system unlike, for instance the governance system for telecommunications or financial services, is an integral part of the 'emerging fundamental rights architecture' of the EU.[221] While data protection was initially enacted as a regulatory internal market policy, its legal basis has now been decoupled from the internal market and it is recognised as a fundamental right in the EU legal order. Supervisory authorities are therefore the 'guardians of those fundamental rights and freedoms' protected by EU data protection law and thus the existence of supervisory authorities is an essential component of human rights protection.[222] It follows that when decision-making formerly conducted by supervisory authorities is conducted by the EDPB it too will be acting as part of this fundamental rights architecture. Indeed, one rationale advanced for the existence of the EDPB is to render the protection of the right to data protection more effective. The so-called 'Paris Principles' of the UN[223], which set out recommendations for national human rights institutions, recognise that human rights institutions should be composed in an independent and pluralistic manner. However, these principles do not elaborate on the powers that independent human rights institutions should exercise. While some other EU Agencies also pursue human rights objectives, for instance the Foundation for the Improvement of Living and Working Conditions or the EU Fundamental Rights Agency, the nature and extent of the powers of these agencies are distinct. For instance, as Hinarejos notes the EU Fundamental Rights Agency 'follows the model of a European information and coordination agency'and has several significant limitations that curtail its effectiveness, including that it cannot issue binding decisions and does not set its own agenda.[224]

The key concern regarding EU agencies is that they 'operate at arm's length from traditional controls and cannot easily be held accountable for their actions'.[225] Moreover, as has been outlined, the EDPB is qualitatively distinct from other agencies as a result of the extent and nature of its powers. While the *Meroni* doctrine was enacted by the Court to ensure that the delegation of executive decision-making by the Commission was compatible with the principle of institutional balance, and thus to ensure some level of accountability, as Curtin has highlighted this principal-agent model of accountability

---

[220] See note 44 above, p 1824.
[221] See note 44 above, p 1826.
[222] See note 28 above, para 23 and note 27 above, para 37.
[223] Principles relating to the Status of National Institutions (the Paris Principles), adopted by General Assembly resolution 48/134 of 20 December 1993. U.N.Doc. A/RES/48/134, available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx .
[224] See note 188 above, pp 63-64.
[225] See note 189 above, p 2.

does not capture the power dynamics agencies entail.[226] Rather, as Dehousse suggests, '*Europeanization* would be a better description of the process in which powers are transferred vertically (from national to the EU level) rather than horizontally (from Community institutions to specialized agencies).'[227]

The challenge will therefore be to ensure the accountability and legitimacy of this Europeanised agency. The EDPB itself, like national supervisory authorities, must 'act independently'[228] and 'in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody'.[229] In *Commission v Germany* Germany had argued that the principle of democracy precludes a broad interpretation of supervisory authority independence as this principle requires the administration to be subject to the instructions of government which then, in turn, answers to parliament.[230] However, the Court rejected this argument stating that the principle of democracy does 'not preclude the existence of public authorities outside the classic hierarchical administration'. It highlighted that supervisory authorities remain regulated by law, subject to judicial review and are overseen by Parliament.[231] The principles of accountability and transparency therefore 'require that a supervisory authority be answerable for its actions'.[232] The EDPB shall therefore be subject to the general democratic checks on EU agencies: its decisions can be appealed by EU Institutions and Members States as well as by directly and individually concerned actors pursuant to Article 263(1) TFEU; it is subject to a check of legality by the Commission in accordance with the Commission's general oversight powers under Article 17(1) TEU and the EDPB's annual report must be made public and transmitted to the European Parliament, the Council and the Commission.[233] This report must include a review of specified guidelines, recommendations and best practices it has issued as well as of the binding decisions it has enacted under the dispute resolution mechanism.[234] Moreover, although the Commission has no voting rights on the EDPB, it is entitled to designate a representative to the EDPB, to participate in its meetings and the Chair of the Board communicates the activities of the EDPB to the Commission.[235] This role for the Commission appears difficult to reconcile with the EDPB's institutional independence however it will enable the Commission to exercise its general powers of oversight more effectively.

Thus, one might conclude that despite its questionable compatibility with the *Meroni* doctrine given the nature and the extent of its powers, the EDPB shall be subject to oversight by the EU Institutions. While for some the new governance system brought about by the GDPR will therefore represent the beginning of a 'bureaucratic network in

---

[226] See note 47 above, pp 528-529. Curtin identifies three problems in employing the principal-agent model of delegation to EU level agencies, including that 'the tasks being "delegated" may be those of the Member States, not of the formal principals'.
[227] R Dehousse, 'Misfits: EU Law and Transformation of European Governance' in Christian Joerges and Renaud Dehousse, *Good Governance in Europe's Integrated Market* (OUP, 2002) 207, 221.
[228] See note 9 above, Article 69(1).
[229] Ibid, Article 69(2).
[230] See note 28 above, para 40.
[231] Ibid, para 42.
[232] See note 41 above, p 1.
[233] See note 9 above, Article 71(1).
[234] Ibid, Article 71(2).
[235] Ibid, Article 68(5).

being, composed of national and Union bodies outside any democratic control'[236], others may simply argue that this 'Europeanisation' or more 'integrated administration'[237] of EU data protection law is necessary in order to increase Member State cooperation in this transnational field of law and the EDPB shall act as a 'catalyst of compliance'.

IV. CONCLUSION

Despite the increasing importance and prominence of substantive data protection law, the governance of data protection law has been largely overlooked to date: data protection laws have been under-enforced and the data protection governance structure has not attracted much doctrinal attention. This paper claims that the current governance structure will be 'Europeanised', and thus radically reformed by the GDPR. In order to illustrate the extent of this reform, it proceeded in two parts. First, it illustrated that the current data protection governance system is characterised by its enforcement by independent supervisory authorities. This system is also, however, characterised by a lack of centralised coordination of the activities of these independent supervisory authorities. In the absence of such vertical oversight, cross-border cases involving multiple supervisory authorities are governed by ad hoc mechanisms while there is evident regulatory arbitrage between supervisory authorities in contentious cases.

This paper asserts that these shortcomings of the current decentralised system of enforcement will be rectified by the 'Europeanisation' of data protection law, in particular the creation of the EDPB – a centralised agency that will provide co-ordination and coherence to the actions of supervisory authorities through binding mechanisms. However, this process of 'Europeanisation' will, it is suggested, pose other challenges for data protection governance. First, 'Europeanisation' will necessarily curtail the vertical independence of supervisory authorities vis-à-vis the EU. Its compatibility with the primary law requirement for supervisory authority independence may thus be questioned. This paper suggests however that a purposive approach is taken to the interpretation of the independence criterion: independence enhances the effectiveness of the data protection rules. As the creation of the EDPB is designed to enhance the effectiveness of these rules also, and will thus contribute to this over-arching aim, it should not be viewed as an unlawful interference with supervisory authority independence. The EDPB must also sit in a broader EU law context and, in this regard, it challenges existing principles of subsidiarity and national identity. Indeed, 'Europeanisation' through a centralised institutional framework will lead to 'Europeanisation' in the second sense – in terms of its impact on national structures and policies. The democratic legitimacy and accountability of the EDPB might also be questioned, particularly in light of the *Meroni* doctrine. The EDPB differs in some respects from other agencies as it represents the Europeanisation of existing national powers rather than the delegation of EU powers. Nevertheless, it is also suggested that the EDPB represents a further step in the 'agencification' process: the EDPB shall exercise quasi-regulatory powers and, crucially,

[236] Zemánek queried, prior to the enactment of the GDPR, whether the independence of supervisory authorities provided an illustration of this tendency. See note 49 above, p 1762.

[237] Curtin suggests that 'integrated administration' encompasses 'both European and national levels with now no rigid separation between these levels'. See note 47 above, p 523.

its decisions are not of a purely technical nature but instead require normative decision-making. This institutional 'Europeanisation' is therefore set to change EU data protection governance in a drastic manner. The 'domestic consequences' for Member States of this centralised governance structure – 'Europeanisation' as it is most widely understood – are as of yet unknown. However, the impact of this new governance system may go beyond structural and policy changes as European data protection values have the potential to shape discourse and identities at the domestic level if internalised.