29. Data protection

Herwig Hofmann and Lisette Mustert

1. INTRODUCTION

The protection of personal data created by ever more ubiquitous technical devices, and processed in ever more complex ways, is a formidable regulatory challenge. The enforcement design, mechanisms and practices in place in the area of data protection are particularly relevant to this, especially given that political borders do not match the flows of data on the internet.

The regulatory approach to data protection consists of a patchwork of legislative and non-legislative sources of mandates and powers of relevant European Union (EU) and national enforcement authorities. Especially complex is the EU General Data Protection Regulation's (Regulation 2016/679 or GDPR) hybrid enforcement approach. It is based on co-regulatory approaches combining legislation and self-regulatory instruments and giving private parties an active role (Blok 2020), as well as the specific role of national data protection authorities (DPAs), and in some cases the European Data Protection Board (EDPB or the Board), to enforce alleged violations of the GDPR. Especially complex is enforcement of cross-border cases, which is organized in accordance with a novel cooperation and consistency mechanism.

We discuss in this chapter the complexities of the vertical, horizontal and diagonal composite procedures where both EU agencies and DPAs potentially from various Member States are linked. This raises various questions not only about administrative enforcement, but also of possibilities of judicial accountability in view of the multi-jurisdictional cooperation. This chapter argues that the enforcement system as set up under the GDPR offers in theory many possible tools to prevent violations of the GDPR, but addressing possible violations via a complaint mechanism – especially those violations with a cross-border element – remains problematic. This is due to the multiple EU and national administrative supervisory authorities involved and the lack of harmonized procedures and enforcement strategies. As this chapter will demonstrate, possibilities for individuals to challenge the data-processing activities of controllers and processors in the context of civil litigation, as well as to seek judicial review of supervisory (in)action, remain highly problematic.

2. AN OVERVIEW OF ENFORCEMENT OF THE GDPR: ELEMENTS OF A HYBRID ENFORCEMENT MODEL

The GDPR gives practical effect to the protection of fundamental rights in relation to the processing of personal data. It is the main legislative basis for limitations and balancing of rights of privacy in the EU, the protection of personal data with other rights, and public interests (Article 7 and 8(1) of the Charter of Fundamental Rights of the European Union (CFR); Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)). Its system of enforcement was designed as an answer to the problems caused by the fragmented

landscape of different data protection laws under the former Directive, that is, Directive 95/46/EC (Korff 2021). Nonetheless, the GDPR maintains a great diversity of national public supervisory authorities (DPAs), responsible for monitoring the application of the GDPR. Despite the unique status of these DPAs – in the sense that the protection of personal data is the only fundamental right listed in the CFR that explicitly requires protection by means of 'an independent authority' – the GDPR also placed enforcement in the hands of private parties (see section 2.2). Additionally, the GDPR allowed for the creation of an EU-level agency, the EDPB, which constitutes an independent data protection authority (next to the European Data Protection Supervisory (EDPS). The EDPB shall have a coordinating role in the 'cooperation and consistency mechanism', a form of procedural cooperation between various actors involved in the enforcement of data protection rights (Chapters VI and VII of the GDPR). Thus, the GDPR's acknowledged need for uniformity in the implementation and enforcement of EU law, while preserving this decentralized nature of these tasks within the EU (Polak and Versluis 2016, 106), has led to a *hybrid enforcement model*, involving both the EDPB, national DPAs and private parties.

2.1 A Combination of Deterrence and Compliance-based Approaches

The national DPAs are mainly responsible for enforcing alleged data protection violations. Such enforcement procedures can be initiated either on the basis of a complaint lodged by a data subject or on the DPA's own initiative – for example, when the DPA becomes aware of an alleged violation via a data breach notification sent out by the controller (Article 33 of the GDPR). In order to address alleged violations, the GDPR offers a wide range of investigative and corrective powers to the DPAs – for example, each DPA may carry out investigations in the form of data protection audits or may obtain access to any premises (Article 58(1) of the GDPR). However, the GDPR as a 'general' regulation does not provide great detail on such procedural provisions, and even explicitly mentions the possibility for Member States to provide for additional powers of their respective DPA. Hence, Member States are obliged to use their remaining procedural autonomy under the EU's general principles of loyal cooperation, equivalence and effectiveness to provide for detailed national rules on enforcement and procedure – either by general administrative law provisions or by data protection-specific norms and regulations. As DPAs act within the scope of EU law when enforcing the GDPR, national procedural safeguards are supplemented by the general principles of EU law and an important set of procedural rights arising from the EU treaties and CFR (Hofmann 2016; Mendes 2016).

In order to address GDPR violations, on the one hand, the GDPR provides DPAs with the possibility to impose corrective measures – such as high administrative fines of up to €20 million or 4 per cent of the company's global annual turnover, which should be of such a type and magnitude that the expected costs are higher than expected benefits of the violation of GDPR provisions – or the possibility to order a definite ban on processing, which often has severe financial consequences for the data controller or processor. Such measures reflect a *deterrence-based approach* (Voermans 2014, 47).

This logic of deterrence is combined with an orientation towards greater encouragement of compliance (a *compliance-based approach*) by offering a hierarchical range of sanctions available for the DPAs to address violations (Ayres and Braithwaite 1992). Therefore, on the other hand, DPAs may choose, *inter alia*, to issue warnings or reprimands, to order the

rectification or erasure of personal data or to impose merely temporary limitations to processing as a response to a violation of the GDPR (Article 58(2) of the GDPR). The GDPR, however, does not prescribe which enforcement approach is most appropriate for which kind of violation, which becomes especially problematic when DPAs are required to cooperate (see section 3.2.1). Therefore, the EDPB's role in ensuring more consistent enforcement is crucial, for instance via the adoption of non-legally binding guidelines, recommendations and best practices. Such documents guide the DPAs by offering interpretations and clarifications of substantive data protection matters but also of how certain enforcement procedures should function – see, for example, EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR. Due to the assistance these documents offer data processors and controllers in implementing and complying with the GDPR and DPAs to enforce the GDPR more consistently, they may produce legal effects in practice. In addition to the EPDB's guidelines coordinating national DPAs, the EDPB may also adopt binding decisions towards national DPAs and, exceptionally, private parties. In such binding decisions, the EDPB may, for instance, take a clear stance regarding the DPA's proposed enforcement strategy: in the second dispute brought before the EDPB, it obliged the Irish DPA to adopt corrective measures instead of mere recommendations by stating that if no corrective powers are exercised, this 'impairs the position of data subjects to be fully aware of the processing at stake *as a mere recommendation cannot be enforced and Whatsapp IE is not obliged to follow the view of the DPC in this regard*' (EDPB Decision 01/2021, para 216 (emphasis added)). This recommendation can be seen in the light of requirements of the Court of Justice of the European Union (CJEU) established in other policy areas where effective enforcement is requested. In fact, it is long established that Member States may not 'render virtually impossible or excessively difficult the exercise of rights conferred by Community law' by means of insufficient protection through their legal systems (see the standard formulation in the case law of the court, for example in Case C-651/19, para 34).

2.2 Enforced Self-regulation

Although the right to data protection is a fundamental right to be protected by legislation and public supervision, private parties may play an important role in the enforcement of data protection rights under the GDPR (Blok 2020, 97). In fact, the GDPR is characterized by a *hybrid co-regulation model* where legislation and self-regulatory instruments are combined. Therefore, the GDPR encourages the use of codes of conduct, data protection certification mechanisms, data protection impact assessments and technical standards to promote transparency, guide the implementation of the GDPR and demonstrate compliance (Kamara 2017, 2). Codes of conduct, for instance, have a positive impact on the level of data protection, as they raise awareness and lead to the clarification of abstract legal norms (Blok 2020, 113). Codes of conduct also adapt easily to advancements of technologies due to their faster development processes in comparison to legislation (Kamara 2017, 2). Such codes may even have EU-wide effects if the Commission decides that the code has general validity (Article 40(9) of the GDPR). Nevertheless, significant investment on the part of the DPAs is required to keep up with self-regulatory instruments and the technological developments they address.

While the GDPR maintains the leading position for DPAs to enforce violations, the regulation introduces a system of *private supervision* where accredited bodies may interpret, monitor and assess conformity with codes of conducts or certifications (Medzini 2021, 3).

Such monitoring of private bodies all acts in the shadow of hierarchical decisions of EU and national supervisory authorities (Medzini 2021, 3). However, these private bodies must receive accreditation from a public authority and will have to communicate the measures taken to the competent DPA in case of a violation of a code of conduct. This is crucial as the rights of individuals are not per se sufficiently protected by industry-led self-regulatory initiatives (Kamara 2017, 4). In any case, the monitoring and certification bodies may assist the DPAs and free up their time and resources (Medzini 2021, 4; Kamara 2017, 2).

Importantly, many of these self-regulation instruments are, furthermore, a means to demonstrate the existence of appropriate safeguards within the framework of personal data transfers to third countries in the absence of an adequacy decision – via which the Commission may declare a third country as offering an adequate level of protection, which allows personal data to flow from the EU to that third country without any further safeguard being necessary. The adoption of such adequacy decisions by the Commission is increasingly being scrutinized – for example, the Commission's Safe Harbour and Privacy Shield decisions allowing the transfer of data outside the EU to the United States were invalidated by the CJEU in the *Schrems I and II* judgment (Case C-362/14; Case C-311/18). In the absence of such an adequacy decision, data controllers or processors must make binding and enforceable commitments via contractual or other legally binding instruments (such as standard contractual clauses adopted by the Commission or a DPA, binding corporate rules, codes of conduct or certification mechanisms in order to transfer data outside of the EU and to thereby guarantee appropriate safeguards (see Articles 4(20), 40(3), 41(2), 46(1), 46(2)(b)–(f) and 47 of the GDPR). Many organizations transferring data make use of standard contractual clauses, which are model data protection clauses, approved by the Commission, which allow the transfer of personal data when embedded in a contract (see eg European Commission 2021). The clauses contain contractual obligations for the data importer and exporter, and rights for the individuals whose data is transferred. Via these binding and enforceable commitments, the EDPB not only acknowledges the 'Brussels effect' of the GDPR but actively uses the concept to expand the influence of the GDPR beyond the EU's territory – for example, the EDPB's guidelines 04/2021 determine that data transfers on the basis of a code of conduct between a data exporter (subject to the GDPR) and a data importer (an actor not subject to the GDPR) can take place as long as the data importer adheres to the code (Vander Maelen 2022).

Other forms of self-regulation are also encoded in the requirements for the controller to register data processing activities, thereby assisting the DPAs in monitoring compliance with the GDPR; to designate a Data Protection Officer who guides the implementation of the GDPR; to notify the competent DPA when a data breach occurs; and to conduct Data Protection Impact Assessments (DPIA) if a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) of the GDPR). Such obligations play a very important role as they may free up scarce resources of DPAs by offering a helpful monitoring tool for DPAs (Recital 141 and Article 77(1) of the GDPR). However, these mechanisms will only work if the actor uses them, and they require a considerable investment of the controller with regard to time, money and expertise (Blok 2020, 117). Furthermore, it is questionable how the protection of a fundamental right to data protection is subject to an enforcement mechanism that is dependent upon a *risk-based approach*, where only processing with the highest risk to materialize or with the most serious implications is brought to the attention of the competent DPA. The former Article 29 Working Party was also critical of this and argued that 'the risk-based approach is being increasingly and wrongly presented as an alternative

to well-established data protection rights and principles, entailing that it couldn't accept the point of view whereby legal compliance should shift to a strong harm-based approach' (Gellert 2020, 4; A29 WP 2014). The fundamental right to data protection should be respected regardless of the risks incurred through the data processing involved.

3. ELEMENTS INFLUENCING ENFORCEMENT OF GDPR RIGHTS AND OBLIGATIONS

There are various factors influencing the possibilities of enforcement in the field of data protection law. A central problem for enforcement in the field of the GDPR is the concept of territoriality of law, which does not sit well with a per se deterritorial digital world. The solution to this offered by the GDPR, where both EU and several national DPAs act together in one procedure, results in often complex and time-intensive forms of cooperation. Such composite procedures may lead to legal uncertainty for all actors involved. Furthermore, possibilities of judicial review of enforcement activities as well as private litigation against offences are two elements to be taken into account in the following discussion of enforcement.

3.1 Challenging Administrative Enforcement in Case of Cross-border Cases

In the EU's single market and with an internet that is not based on physical borders, alleged violations of the GDPR are often not merely a national affair. Therefore, in the case of administrative enforcement by DPAs and the EDPB of alleged GDPR violations with a cross-border element, the GDPR created a novel cooperation and consistency mechanism, giving rise to procedural cooperation involving both national and EU authorities. Although one DPA shall take the lead in order to address the violation in accordance with the one-stop shop mechanism (this is the DPA of the Member State where the data processing company locates its 'main establishment'), it shall cooperate with the other 'concerned' authorities (either because the controller or processor has an establishment also in their territory, because affected data subjects reside in their territory, or because the complaint is lodged with that DPA). This will allow the concerned DPAs to effectively protect the data subjects in their territory if they do not have the leading role. The extraordinary complexity of involving so many DPAs in cumbersome diagonal composite procedures will, however, slow the enforcement of cross-border violations considerably, and thus it becomes questionable whether this system truly enables the DPAs to effectively protect their data subjects, or whether it instead leads to under-enforcement.

3.1.1 Cooperation between national DPAs: complex and cumbersome

The DPAs are required to reach consensus on every stage of the enforcement procedure, meaning that DPAs shall reach consensus, *inter alia*, on the scope of the investigation, the necessary investigative actions – for example, when is an on-site inspection, an audit or merely desk research required – the enforcement actions to be taken and the outcome of the decision-making process. In reality, finding consensus on such questions is not an easy task, since DPAs located in different Member States may have highly differing opinions on the scope of the investigation and the necessary investigative and enforcement actions to be undertaken. Such national approaches and strategies are often laid down in national policy guidelines which are formulated in rather vague terminology. The Austrian DSB, for instance,

shall make sure that 'supervisory activities are to be exercised in a way that least interferes with the right of the controller or processor or third parties', which is not per se an obligation for other DPAs (AU Data Protection Act, para 22(1)).

Besides different opinions on the appropriate enforcement strategy, concerns arise with regard to the GDPR's lack of detailed procedural rules regulating the DPAs' cooperative duties. The GDPR requires, for instance, the lead and concerned DPAs to provide each other with all relevant information, but it does not elaborate on this requirement and, thus, questions such as what constitutes relevant information, when shall this be exchanged and who shall be able to access the information are determined through contextual criteria established at national level. In addition to this general obligation for DPAs to inform each other, DPAs may request mutual assistance – for example, requests for supervisory measures such as carrying out authorizations, consultations, inspections or investigations – or organize joint operations if the lead DPA requires information or measures to be carried out in another Member State (Blume 2020, 61). Such requests may not be ignored and, thus, DPAs will have to take all appropriate measures required to reply to a request within one month (Articles 61(4) and 62(7) of the GDPR). In theory, making use of such mechanisms – for example, requesting the lead DPA to investigate a certain matter or exchanging knowledge and best practices – leads to a form of peer pressure that may speed up enforcement and increase decision-making quality (Majone 2000; Coen and Thatcher 2008; Mastenbroek and Martinsen 2018, 428). DPAs, however, experience these duties as a large burden on their limited human and financial resources. In general, these resources do not seem to be sufficient for dealing with the immense workload and for keeping up with technological developments, which requires a high level of technical know-how within DPAs (Raab and Szekely 2017, 421). It is therefore not surprising that so far only one joint investigation has been conducted since the entry into force of the GDPR (EDPB 2021, 69).

During the decision-making phase, DPAs will have to continue to cooperate in an endeavour to reach consensus. Therefore, the lead DPA shall consult the concerned DPAs on its draft decision before adopting a final decision addressed to the data processing company (Article 60 of the GDPR). The importance of sufficient cooperation during the investigation stage becomes visible here: in order to participate in the decision-making process in a meaningful way, concerned DPAs must have gained an in-depth understanding of the case which means that it is essential that the lead DPA informed the other concerned authorities well and that all relevant information is exchanged. If concerned DPAs disagree with the proposed draft decision and, therefore, submit relevant and reasoned objections, the lead DPA cannot ignore such objections and shall take due account of them. Hence, the concerned DPAs may have a large role in steering the final outcome of the decision (although the first two decisions submitted to the EDPB for dispute resolution demonstrate that concerned DPAs struggle with the submission of relevant and reasoned objections, see EDPB Decisions 01/2020; 01/2021). The consequence of rejecting the objections or considering them not to be relevant and/or sufficiently reasoned, is that the matter shall be referred to the EDPB for dispute resolution (see section 3.1.2).

The implementation of these cooperative duties is supported by the Internal Market Information System (IMI system), which is a central database where different procedures can be started. DPAs are, for instance, able to identify their role as lead or concerned DPA; they can request mutual assistance to each other, commence joint operations and share their draft decision consultations. The IMI system, however, allows for other forms of cooperation too:

voluntary mutual assistance instead of formal mutual assistance, and *informal* consultation procedures instead of making use of the formal consultation procedure – which is, according to the Commission, based on the GDPR's general obligation for DPAs to cooperate with each other laid down in Article 57(1)(g). More informal and open interaction will enable DPAs to learn about each other's national implementing laws, national procedural laws, enforcement strategies and practices, which could potentially lead to more consistency in enforcement (Polak and Versluis 2016, 121; Hijmans 2016a, 386; Giurgiu and Larsen 2016, 352). However, there are no legal deadlines and responding to informal requests remains voluntary. For this reason, DPAs prefer to cooperate informally rather than making use of formal cooperative tools that the GDPR provides for, as it releases some DPAs from the high administrative burden that formal cooperation requests create (Dutch DPA Jaarverslag 2020, 11; Barnard-Wills et al. 2016, 590). This leads to many requests that may be ignored, and therefore do not create any peer pressure among DPAs. This is, however, crucial to have when enforcement slows down due to the huge backlog that some DPAs have, or the economic advantages that certain Member States gain from underenforcement (see ICCL 2021).

All in all, the resulting composite procedures are highly integrated but can be lengthy and cumbersome. Reaching consensus on enforcement actions to be taken may be hindered by differences in national procedures, differences in enforcement strategies, the lack of available human and financial resources, the possibility to cooperate informally – without legal deadlines – and in some Member States the unwillingness to enforce strictly. Thus, the enforcement network seems to achieve the opposite of its original aim: protecting data subjects more effectively.

3.1.2 Role of the EDPB: too soft and marginal

The EDPB is a central node in the enforcement network which coordinates and supports the functioning of DPAs at national level. The board shall, for instance, assist the DPAs with keeping up with new technologies by the creation of a Technology Expert Subgroup, by seeking advice from other supervisory authorities – for example, the Chair of the EDPB cooperates with ENISA on security issues with a focus on the health care sector and the cloud certification scheme – and by promoting cooperation among national DPAs via common training programmes, the organization of personnel exchanges and the creation of a Support Pool of Experts (Article 70(1)(u)(v) of the GDPR; EDPB 2020a, 11; EDPB 2021, 94; EDPB 2022; EDPB 2020c).

Besides such supportive tasks, the Board has a coordinating role when cooperation at national level does not proceed. When a DPA, for instance, fails to act in accordance with formal cooperation requirements – for example, when a DPA does not comply with its obligations regarding mutual assistance or joint operations – DPAs may request the Board's opinion or may trigger an urgency procedure (Articles 64(2) and 66 of the GDPR; Hijmans 2016b, 370). Such non-binding opinions may be turned into legally binding decisions via the Board's dispute resolution mechanism if it is not followed (Article 65(1)(c) of the GDPR). Thus, non-binding opinions should be applied and cannot simply be ignored, regardless of their legal status (Docksey 2020, 1061). As the Chair of the Board can initiate the adoption of such an opinion – and perhaps even a binding decision – the EDPB could have a final say in many cases with a cross-border element. Unfortunately, however, both DPAs and the EDPB do not often make use of these tools, which are potentially a great way to push for advancement in individual cases.

Additionally, the EDPB shall function as a dispute resolution body when national DPAs cannot reach consensus in the co-decision making process on the outcome of a case, and refer the matter to the Board (Article 65(1)(a) of the GDPR). In that context, the Board shall see whether all objections are well reasoned and relevant, assess the merits of these objections and adopt a final binding decision addressed to the lead and concerned DPAs. This may include the difficult task for the Board to interpret and apply national implementing and procedural laws (Feiler et al. 2018, 262). Although the Board is competent to adopt a final decision on the matters brought before it, it cannot initiate such a procedure by itself and it cannot collect any information or conduct any investigation either. The EDPB's ability to adopt a decision is, thus, highly dependent on whether it receives the required information from the DPAs. The first two disputes brought before the Board indeed demonstrate that the EDPB's decision making may well be hampered by a lack of relevant and required information (EDPB Decisions 01/2020; 01/2021). Compared to other EU agencies with decision-making powers, this is peculiar and seems to be rather ineffective (see Chapter 10 of this Handbook). EU agencies with decision-making powers, such as for example the trade mark agency in Alicante, will investigate and collect information itself. On the other hand, agencies that do not have such competences usually lack externally binding decision-making powers and are limited to more coordinating roles.

It is also relevant to note that the Board's final decision is not addressed directly to the data-processing company or the individual complainant. Instead, the competent DPA, which may be the lead DPA, shall implement the Board's decision and shall give full effect to the Board's binding directions in its further decision making regarding the data controller or processor as well as any complainants. Some of these binding directions, however, remain rather broadly formulated – such as the obligation to adopt a higher fine – leaving discretion to the national level. The current system means that in practice, a final decision can be based partly on the Board's decision – as only those aspects brought to the EDPB are subject to a decision taken at EU level – and perhaps also partly on the basis of preparatory acts of DPAs from several Member States. This leads to the mixing of procedural rules from various jurisdictions as well as to the creation of a highly challenging situation for judicial review of decision-making, which will generally be conducted within the jurisdiction where a finally binding decision is taken. Even more complex may be the situation where the EDPB adopts a binding decision after its opinion was not followed by the competent DPA. By such decision, the EDPB can overrule a national decision which, in its view, may have to be altered (Hijmans 2020, 1017). This additional level of decision making with direct effect vis-à-vis individuals further illustrates the complexity of decision-making in case of cross-border GDPR violations, which takes place in diagonal composite procedures.

Irrespective of this, the Board's role seems to be designed predominantly to steer procedural developments by non-binding measures, highly dependent on whether the DPAs refer a matter to the Board. The EDPB cannot investigate or collect information by itself. It is thus not easy for the Board to push for advancement in enforcement at national level.

In this regard, comparing the GDPR approach to the new legislative acts proposed by the Commission regulating digitalization reveals some interesting insights. Under the Digital Services Act, the European Board for Digital Services does not have decision-making powers. It has a larger coordinating role since it may, *inter alia*, request matters to be assessed by national Digital Services Coordinators, recommend the organization of joint investigations by those coordinators or refer the matter to the Commission if it substantially disagrees with

preliminary positions on infringements communicated by the national authorities. These provisions are however highly disputed in terms of details – with the Council suggesting many amendments fine-tuning the role of the respective parties, which do not reduce the complexities of procedures by comparison to the GDPR model, this being an example for the difficulties arising from complexity (see for example the suggested amendments to Articles 45 and 46 of the Digital Services Act in European Council 2022).

3.1.3 Limited possibilities for judicial review of acts stemming from composite procedures

The GDPR provides that the adoption of legally binding decisions may give rise to judicial review by the national court in the Member State of the DPA that adopted the decision (Feiler et al. 2018, 282; Article 78(1) of the GDPR). Such an effective judicial remedy must also be available against the inactivity of a DPA. Judicial proceedings must be brought before the national courts of the Member State where the decision-making DPA is established (Article 78(2)(3) of the GDPR). Thus, if the lead DPA adopts a final binding decision, the court of the Member State where the lead DPA is established is competent, and if the concerned DPA adopts the decision in which it rejects or dismissed a complaint, the court of the Member State where this concerned DPA is established is competent. Data subjects not residing in that Member State may have difficulty challenging a decision in a foreign legal system or different language.

A complicating situation arises when the complaint is partly rejected or dismissed by the DPA with whom the complaint was lodged, and the lead DPA partly acts on the other elements of the complaint. Here, judicial review would need to be sought before two courts in two different Member States, which are then competent to review two decisions based on the same set of facts. The GDPR provides that in such case, the court seized later *may* suspend the proceedings awaiting the ruling of the first seized court (Article 81(2) of the GDPR). This however only partially addresses the matter, since the first seized court may not be in a position to rule on the decisive elements of a case.

Another concern relates to the question whether national courts, when reviewing final decisions in which multiple authorities at EU and national level were involved, are allowed to involve the acts of authorities from other Member States or the EU in their review. Regarding EU acts that influence the DPA's final decision, the GDPR provides that where proceedings are brought against a decision of a DPA which was preceded by an opinion or decision of the Board, the DPA shall forward that opinion or decision to the CJEU. Thus, opinions or decisions of the Board can only be reviewed by the CJEU (Hofmann et al. 2011, 12). Problematic in this regard, however, is the question whether natural persons have legal standing before the CJEU in accordance with Article 263(4) of the TFEU, since they are most likely not directly concerned by the Board's decisions because national DPAs will implement the Board's decision, which entails discretionary choices. This was recently confirmed by the General Court in case T-709/21 (on appeal), where the court held that WhatsApp could not challenge the EDPB's decision addressed to the Irish DPA as the data processing company was not directly concerned by the Board's decision (Case T-709/21, para 61). It is less clear whether national courts are able to review acts of authorities established in different Member States. In the *Berlioz* case, the 'CJEU has held that a national court is able to review the lawfulness of acts taken by foreign authorities in order to comply with Article 47 CFR' (Case C-682/15, para 59; Lanceiro and Eliantonio 2021, 389). Therefore, the national court where the action

against the final measure is brought should be able to review the preparatory acts adopted at earlier stages of the enforcement process by the DPAs in other Member States, using EU law as a parameter (Mazzotti and Eliantonio 2020, 53). In particular, preparatory acts stemming from informal forms of cooperation may not qualify as reviewable preparatory acts and may, therefore, escape judicial review here (Mazzotti and Eliantonio 2020). Thus, DPAs may not only circumvent the complex cooperation procedures laid down in the GDPR by choosing to go for voluntary cooperation, but may also escape judicial review.

A general concern, furthermore, relates to situations where the complainant is no longer a party to the procedure – that is, where they are deprived of any procedural right such as access to the file, the right to be heard and the right to an effective judicial remedy. This may be the case when complaints are lodged with a concerned DPA not being the lead DPA. These complainants are 'demoted' to the role of an informant being merely informed by the concerned DPA of the outcome of procedures between the lead DPA and the data-processing company. This situation also arises when DPAs, such as the Irish DPC, obfuscate procedural rules and principles by beginning with opening own-initiative investigations in parallel to addressing individual complaints, consequently opting to put the treatment of individual complaints on hold until such own-initiative investigation would be completed, thereby ensuring that individuals have no procedural rights in the process and will be confronted with results established in the procedure exclusively conducted between the DPA and the targeted entity.

All in all, the review of DPA decisions following composite procedures, especially complex diagonal composite forms of cooperation, is made particularly difficult by the fact that input may arise from various jurisdictions, each with differing procedural rules and languages. Some elements of DPA decision making may therefore *de facto* escape judicial review.

3.2 Private Enforcement: Not Always an Alternative for Failing Administrative Enforcement

Private enforcement before national or EU courts is an important alternative to the existing system of enforcement but does not always fill this gap. Private parties can directly challenge violations of the GDPR before a national court in accordance with Article 79 of the GDPR, which will often involve actions in the form of seeking orders to desist or damage claims. Article 82 of the GDPR, therefore, provides that any person that has suffered material or non-material damage as a result of a GDPR infringement shall have the right to claim compensation from the controller or processor. Data subjects, however, may face several obstacles. First, data protection violations do not per se result in a financial loss, but instead the data subject may have a feeling of unease because they are being monitored or are under surveillance (Requejo Isidro 2019, 7; Lynskey 2015). Research has shown that, therefore, individuals may not see this harm as being actionable. This is not made easier by the fact that the GDPR does not offer an interpretation of 'damage' – for example, is a mere violation of the GDPR, without further harm, sufficient to claim damages (Requejo Isidro 2019, 14)? This question is currently subject to a preliminary reference procedure before the CJEU (*Austrian Oberster Gerichtshof*, 6Ob35/21x). Additionally, individuals may be deterred from going to court either because they believe that the controller or processor is too powerful to challenge them, because the amount of damages awarded for data protection violations is so low in some Member States or because of the costs, the length of civil proceedings and the difficulty of gathering evidence (Requejo Isidro 2019, 7; FRA 2014, 30–1). The problems that individ-

uals face may be circumvented by non-governmental organizations (NGOs) bringing cases to court that have a collective dimension, which is allowed by the GDPR under Article 80. Unfortunately, Member States are reluctant to implement this provision and so far Spain is one of the few Member States that allows NGOs to bring actions for compensation without a data subject's mandate (Requejo Isidro 2019, 12).

Furthermore, it is not unproblematic that Article 79 of the GDPR states that seeking national judicial remedies is 'without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a DPA' (Article 79(1) of the GDPR). In practice, this means that a data subject could submit a complaint with a DPA and challenge the actions of the data processing company in a civil court, for example as a damages case, at the same time. The question whether the DPA and the court both have an obligation to assess the matter independently, meaning that they could arrive at different outcomes, or whether the DPA's decision takes priority when it comes to the question of whether an infringement has been committed is currently subject to a preliminary reference procedure before the CJEU (pending Case C-132/21).

4. CONCLUSION

The GDPR specifies rights to privacy and the protection of personal data. These rights must be protected by public authorities entrusted with the task to monitor the application of the GDPR. This is not only a requirement by Article 8(3) of the CFR, but also a necessity in view of the various difficulties which private enforcement faces, as described above. Both public and private enforcement approaches have to cope with the fact that the internet is not designed around political borders. DPAs are therefore involved in monitoring and enforcing cross-border processing operations. Although the GDPR offers many tools for monitoring non-compliance through hybrid self-regulation combined with regulation by authorities, the possibilities to address these violations are limited. In order to address, especially, cross-border violations, it is essential that DPAs sincerely and effectively cooperate, which has been highlighted by the CJEU (see Case C-645/19).

However, the cooperation mechanism is complex and does not always lead to the promptest response. The complexity stems from the patchwork of instruments – including the GDPR, national implementing acts, national administrative laws, EDPB guidelines and Commission implementing and delegated acts – and the multitude of actors at EU and national level acting each in accordance with the GDPR and their own national rules. The resulting composite procedures are highly integrated but risk being lengthy and cumbersome. Reaching consensus on enforcement actions to be taken may thus be hindered by differences in national procedures, such as the interpretation of certain concepts essential for a smooth functioning of the cooperation mechanism and differences in perspectives on the most appropriate enforcement strategy. A first step to overcome this challenge to administrative cooperation could be to further streamline the process, for instance through clarification and harmonization of crucial parts of the enforcement procedure – for example, what constitutes 'relevant information', the document defined as the 'draft decision', when to involve the other concerned authorities and communicate information to them, who can access the information and under what conditions, what to do with relevant and reasoned objections and how to ensure that individuals have

rights as 'parties' to a procedure. Which form such procedural rules may take will need to be studied further.

Cooperation may also be hindered by the lack of available human and financial resources. Currently available resources are not sufficient for dealing with the immense workload that is created due to the DPAs' additional duties under the cooperation mechanism, and this may also be problematic for keeping up with technological developments. It is, therefore, not surprising that national DPAs prefer to cooperate via informal means. In such cases, no legal deadlines apply, which offers the DPAs the possibility to prioritize other matters and respond to requests of other DPAs whenever it suits them. Circumventing formal obligations under the GDPR, however, means that the tools to push another DPA to cooperate are not available. Under current rules, the EDPB has great difficulty stepping in when DPAs are not able to address violations of the GDPR. The Board is only able to adopt an opinion or binding decision when DPAs refer the matter to it, and as the EDPB is not able to conduct any investigation or collect any information itself, its functioning is highly dependent on the DPAs' input. Therefore, the role of the EDPB could, and in our view should, be subject to review – that is, granting the EDPB more direct enforcement powers in cases of significant importance may be a step forward, at least for big transnationally active data processors and controllers. Although at the time of writing this chapter, four years since the entry into force of the GDPR, problems with the chosen enforcement model are beginning to show, it is too early to draw definite conclusions on whether alternative models of enforcement would, in the complex and fast-moving world of digital mass data production, return better results. In this regard, it is a welcome step forward that the Board acknowledges the difficulties with administrative enforcement, and tries to find solutions within the current system – by further enhancing cooperation in strategic cases, by diversifying the range of cooperation methods used and by identifying a list of procedural aspects that could be further harmonized in EU law (see EDPB 2022a). This should not, however, lead to further blurring of responsibilities which would allow acts of DPAs to escape judicial control.

REFERENCES

Academic and Policy Sources

Article 29 Data Protection Working Party, 'Statement on the role of risk-based approach in data protection legal frameworks' 14/EN WP 218 (30 May 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (last check 30 November 2022)

Autoriteit Persoonsgegevens, 'Jaarverslag 2020' (2021) www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf (last check 8 December 2022)

I Ayres and J Braithwaite, Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press 1992

D Barnard-Wills, C Pauner Chulvi and P de Hert, 'Data Protection Perspectives on the Impact of Data Protection Reform on Cooperation in the EU' (2016) 32(4) Computer Law and Security Review 587

P Blok, 'The Role of Private Actors in Data Protection Law' in M de Cock Buning and L Senden (eds), Private Regulation and Enforcement in the EU, Hart Publishing 2020, 95–120

P Blume, 'Article 61 Mutual Assistance' in C Kuner, LA Bygrave, C Docksey and L Drechsler (eds), The EU General Data Protection Regulation, Oxford University Press 2020, 973–85

D Coen and M Thatcher, 'Network Governance and Multi-Level Delegation: European Networks of Regulatory Agencies' (2008) 28(1) Journal of Public Policy 49

C Docksey, 'Article 70 Tasks of the Board' in C Kuner, LA Bygrave, C Docksey and L Drechsler (eds), The EU General Data Protection Regulation, Oxford University Press 2020, 1069–84

European Commission, 'Commission Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System' [2018] OJ L 123/115 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.123.01.0115.01.ENG (last check 30 November 2022)

European Commission, 'Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council' C/2021/3972 [2021] OJ L 199/31 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (last check 30 November 2022)

European Council, 'Interinstitutional Document 2020/0361(COD) of 15 June 2022' https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf (last check 30 November 2022)

EDPB, 'Annual Report 2019' (2020a) https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2019_en (last check 30 November 2022)

EDPB, 'First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities' (2020b) www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf (last check 30 November 2022)

EDPB, 'Document on terms of reference of the EDPB support pool of experts' (2020c) https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en (last check 30 November 2022)

EDPB, 'Annual report 2020' (2021) https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2020_en (last check 30 November 2022)

EPDB, 'Plenary minutes 62nd plenary meeting' (2022) https://edpb.europa.eu/system/files/2022-04/20220314plenfinalminutes62ndplenarymeeting_en.pdf (last check 30 November 2022)

EDPB, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR (9 November 2020) https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/decision-012020-dispute-arisen-draft_en (last check 30 November 2022)

EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (28 July 2021) https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en (last check 30 November 2022)

EDPB, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers', (2022) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en (last check 8 December 2022)

EDPB, 'Statement on enforcement cooperation' (2022a) https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf (last check 30 November 2022)

EDPB, 'Guidelines 04/2022 on the calculation of administrative fines under the GDPR', (2022) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (last check 8 December 2022)

L Feiler, The EU General Data Protection Regulation (GDPR): A Commentary, Globe Law and Business 2018

Fundamental Rights Agency, 'Access to data protection remedies in EU Member States' (2014) at https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (last check 30 November 2022)

A Gellert, The Risk-Based Approach to Data Protection, Oxford University Press 2020

A Giurgiua and TA Larsen, 'Roles and Powers of National Data Protection Authorities' (2016) 3 European Data Protection Law Review 342

H Hijmans, 'The EU as a constitutional guardian of internet privacy and data protection' PhD thesis, University of Amsterdam (2016a)

H Hijmans, 'The DPAs and their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?' (2016b) 2(3) European Data Protection Law Review 362

H Hijmans, 'Article 65 Dispute Resolution by the Board' in C Kuner, LA Bygrave, C Docksey and L Drechsler (eds), The EU General Data Protection Regulation, Oxford University Press 2020

HCH Hofmann, 'Inquisitorial Procedures and General Principles of Law: The Duty of Care in the Case Law of the European Court of Justice' in L Jacobs and S Baglay (eds), The Nature of Inquisitorial Processes in Administrative Regimes: Global Perspectives, 2nd edn, Routledge 2016, 153–66
HCH Hofmann, GC Rowe and AH Türk, Administrative Law and Policy of the European Union, Oxford University Press 2011
ICCL, 'ICCL alerts Irish Government of strategic economic risk from failure to uphold the GDPR' Letter to the Irish Minister of Finance (2021) www.iccl.ie/news/iccl-alerts-irish-government-of-strategic-economic-risk-from-failure-to-uphold-the-gdpr/ (last check 30 November 2022)
I Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardization "Mandate"' (2017) 8(1) European Journal of Law and Technology 2
D Korff, 'EC Study on Implementation of Data Protection Directive 95/46/EC' (2021) https://ssrn.com/abstract=1287667 (last check 8 December 2022)
R Lanceiro and M Eliantonio, 'The Genetically Modified Organisms' Regime: A Playground for Multi-Level Administration and a Nightmare for Effective Judicial Protection?' (2021) 22 German Law Journal 371
O Lynskey, The Foundations of EU Data Protection Law, Oxford University Press 2015
G Majone, 'The Credibility Crisis of Community Regulation' (2000) 38(2) Journal of Common Market Studies 273
E Mastenbroek and D S Martinsen, 'Filling the Gap in the European Administrative Space: The Role of Administrative Networks in EU Implementation and Enforcement' (2018) 25(3) Journal of European Public Policy 422
P Mazzotti and M Eliantonio, 'Transnational Judicial Review in Horizontal Composite Procedures: Berlioz, Donnellan, and the Constitutional Law of the Union' (2020) 5(1) European Papers 41
R Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-Regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review 1
J Mendes, 'Discretion, Care and Public Interests in the EU Administration: Probing the Limits of Law' (2016) 53(2) Common Market Law Review 419
J Polak and E Versluis, 'The Virtues of Independence and Informality: An Analysis of the Role of Transnational Networks in the Implementation of EU Directives' in S Drake and M Smith (eds), New Directions in the Effective Enforcement of EU Law and Policy, Edward Elgar Publishing 2016, 105–29
CD Raab and I Szekely, 'Data Protection Authorities and Information Technology' (2017) 33(4) Computer Law and Security Review 421
M Requejo Isidro, 'Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection' Max Planck Institute Luxembourg for Procedural Law Research Paper Series No 2019 (3)
C Vander Maelen, 'Codes of (Mis)Conduct? An Appraisal of Articles 40–41 GDPR in View of the 1995 Data Protection Directive and Its Shortcomings' (2022) 6(2) European Data Protection Law Review 231
W Voermans, 'Motive-Based Enforcement' in L Mader and S Kabyshev (eds), Regulatory Reforms: Implementation and Compliance, Proceedings of the Tenth Congress of the International Association of Legislation, Nomos 2014, 17–38

Legal Texts and Case Law

Austrian Federal Act concerning the Protection of Personal Data (Datenschutzgesetz) last amended by BGBl. I Nr. 148/2021
Austrian Supreme Court, Case 6Ob35/21x [2021]
Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650
Case C-682/15 Berlioz Investment Fund SA v Directeur de l'administration des contributions directes [2017] ECLI:EU:C:2017:373
Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559
Case C-645/19 Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit [2021] ECLI:EU:C:2021:483

Case C-651/19 Commissaire général aux réfugiés et aux apatrides [2020] ECLI:EU:C:2020:681
Case T-709/21 Whatsapp Ireland Ltd v European Data Protection Board [2022] ECLI:EU:T:2022:783
Pending Case C-132/21 Nemzeti Adatvédelmi és Információszabadság Hatóság
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 L 119/1
Consolidated Version of the Treaty on the Functioning of the European Union, C 326/47
Charter of Fundamental Rights of the European Union, C 326/391