"The diversified structure of European data protection enforcement - national authorities between autonomy, hierarchy and cooperation"

Marcel Kaiser, LL.M. (Luxembourg), Bonn*

Administrative cooperation in a European context can be regarded as highly multifaceted. The essay examines the enforcement-structures of the upcoming Data Protection Regulation (GDPR) which is supposed to be a necessary progress for the new challenges in the digital age. After giving an overview of the compliance strategies, the new supranational system of cooperation between European and national supervisory authorities in the GDPR will be observed in depth. In the main part, the reader will get a picture of the multifaceted administrative structure that causes efficiencies and problems at the same time. Therefore, the article questions whether various hierarchical instruments and mixed administrative responsibilities contribute to a real enforcement-interplay or might even endanger consistent data protection in the future. In the end, the author discovers that the described structures not only reveal ambiguous aspects but that specific advanced solutions could have been possible.

I. Introduction

Modern online services facilitate not only large capacities for processing personal data but huge financial and strategic powers for several digital global players. When the GDPR was finally published in May 2015, the interesting question arose if this might be the final step towards a level-playing field of data-security.[1] In this level-playing field the co-existence of privacy protection and economic growth depends most on coherent and robust conditions for prior protection mechanisms. In order to enforce these structures, the new GDPR will vest the data protection authorities (DPA) not only with powers for cooperation but also for hierarchical supervision which will cause various questions. What are the criteria for an exclusive national competence and which solutions are foreseen in cases of multiple points of contact? Which role is given to the new European Data Protection Board (EDPB) and how does this respective system of hierarchical supervision work? As this may introduce a form of administrative hierarchy, the delicate question of what the advantages and limits of this new European data protection system are, must be answered.

II. The ambiguous role of compliance mechanisms as prior enforcement strategies

It lies within the nature of data protection that in the global digital age the companies are not only operating worldwide but have a big influence and thus solutions have to be determined with and not against them. In this light, the new GDPR aims at initiating more autonomy in an officially set framework that can contribute to economic advantages for both public and private sector. This system of self-regulation evidently has become a central element of modern data protection enforcement.[2] In this sense, the Data Protection Directive 95/46/EC (DPD)[3] as well as the upcoming GDPR contain not only strict obligations for processor and controller but also prior compliance mechanisms. Another *telos* may be to relieve the DPAs to a certain extent and make them just one of many legal options for the data subject which e.g. could exercise its rights directly with the responsible controller. First and foremost, prior privacy protection ultimately depends on the coherent condition of consent (Art. 7 GDPR) as the basis of a lawful processing (Art. 6 I GDPR). In general, the prohibitive criteria of a lawful processing ensure that any processing has to fulfil certain standards, giving rise to specific rights and obligations. In detail, this condition depends on any legitimate interests pursued by the controller or a third party which is not overridden by fundamental rights of the data subject. More specifically, the condition of a purpose-limitation

* The German author studied law at the University of Bonn and Toulouse between 2009 and 2015. Having finished the first state examination he wrote his Master Thesis "The enforcement of Data Protection Rules by National and European Agencies – between unification and contradiction" at the University of Luxembourg in 2016. This paper is a revised and adapted fragment of this work. He is currently passing his "Referendariat" and working for Mr. Prof. Dr. *Shirvani* at the University of Bonn.

1 Regulation (EU) 2016/679 of the EP and of the Council of 27 April 2016 on the protection of individual with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

2 Compare *Bull*, "Sinn und Unsinn des Datenschutzes" 2015, pp. 88-91.

3 Directive 95/46/EC of the EP and of the Council 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.

for further processing and use of data was softened as the controller can, within various guidelines, assess these on its own. As the processing of data which is not covered by the original purposes of its collection is not automatically unlawful, the burden of proof for an infringement is turned around and those rules cannot be regarded as sufficient.[4] An Article that could support the DPA to analyse the lawfulness of the processed data is Art. 20 I DPD. Thereafter preventive controls can be enforced when a processing is likely to present specific risks to the rights and freedoms of data subjects. This risk-based approach was transferred into Arts. 35/36 GDPR and shall enlarge the accountability of the companies handling personal data in the following way. The controller, or where applicable the processor, shall firstly carry out an assessment of the potential impact of the intended data processing on the rights and freedoms of the data subjects.[5] Subsequently, the result of that analysis shall be transmitted to the DPA when a high risk is indicated. This prior consultation replaced the system of a stricter authorisation in former proposals of the GDPR.[6] On the one hand, this self-assessment can support the DPA in getting an overview for more intense controls. On the other hand, a preventive prohibition of unauthorised data processing would have been a much stronger instrument. The internal impact assessment will lead to underestimating specific risks and thus not necessarily but likely to deceptive results. In the end, these prior compliance mechanisms reveal a certain ambiguity. This so-called "fourth generation" of systematic data protection may connect general supervision, private self-protection and self-regulation. In general, the implementation of these mechanisms can reduce the extent of supervision because the companies will aim at avoiding external controls by introducing own but adequate data protection standards. Additionally, taking into consideration that competing companies could raise complaints to the DPA, delivering decisive secret information in order to cause fines for violations of data protection provisions, the general need for control could be reduced and lead to a self-promoting compliance. However, the prior impact assessment focusing only on security reveals a weaker point. In order to give an overview of the companies' activities, the social and ethical impact of the use of information should be made public and thus make the individual aware of these risks. Additionally, the ancient instrument of prior notification facilitated the registration of the masses of processing and is now replaced by a less imposing obligation of internal recording. As a consequence, hidden risks might be even harder to discover for the DPA and the goal to establish data protection safeguards before the information is processed may be endangered.

III. The "new" territorial scope and the problems of multiple competences

Art. 28 DPD confers powers on the national supervisory authorities concerning the processing of personal data carried out only on the territory of their own Member State. Therefore, exercising specific powers depends on the question of territorial competence of the supervisory authorities. Related to a possible answer the Court of Justice of the European Union (CJEU) decided that the national authority of the Member State in which a foreign controller is registered or exercises "a real and effective activity through stable arrangements" is competent for any supervision.[7] Codifying the results of this decision is a remarkable progress of the GDPR, because companies that are not established in the EU, are bound by Art. 3 I GDPR, when they provide data-services to EU citizens. However, the question of multiple jurisdictions that can apply in principle inside the Union still remains on the agenda. Rec. 22 GDPR emphasises that the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This entails that a national DPA can be competent even if the law of another might be applicable at the same time. On the contrary, the domestic authority cannot impose any restrictive measures if another Member States law is exclusively applicable.[8] This limitation of powers is based on the principle of legality, the rule of law and territorial sovereignty.[9] A more foreseeable approach the system of the "leading supervisory authority" (Arts. 51-56 GDPR) may bring. According to Art. 56 GDPR the obliged companies have to deal only with one supervisory authority, which will be usually the one of its establishment in Europe. This systematic structure of leading authorities is part of the idea of a 'one-stop shop'. More specifically, the aim is to give supervising powers over the data controller to one territorially competent authority and thus introduce less bureaucratic obstacles and enormous economic advantages for the companies in that sector.[10] Nevertheless, a problem will occur if a controller who has two or even no main establishment in one of the countries and thus will be confronted with different individual measures of the respective two competent DPAs. Without giving an adequate solution, Art. 56 II GDPR even reaffirms that each supervisory authority shall be competent to deal with an infringement if the subject matter substantially affects data subjects only in its Member State. The only legal solution

4 Argumentum *e contrario* out of Art. 6 IV GDPR and this may even be an intentional result: *Albrecht*, "No EU Data Protection Standard Below the Level of 1995" EDPLR 1, no. 1 (2015), pp. 3-4.

5 Compare the nature of this obligation in depth: *Hempel/Lammerant*, "Impact Assessments as Negotiated Knowledge" in "Reforming European Data Protection Law" 2015, pp. 125-147.

6 Original title of Art. 34 P-COM was "Prior authorisation and prior consultation" in proposal of the Com. for a GDPR, COM (2012) 11 final 2012/0011 (COD).

7 *CJEU*, Weltimmo, C-230/14; Google Spain, C-131/12 and recently in VKI v Amazon, C-191/15.

8 Compare in depth: *Cole/Giurgiu*, "The 'Minimal' Approach: The CJEU on the Concept of 'Establishment' Triggering Jurisdiction for DPAs and Limitations of Their Sanctioning Powers (Case C-230/14, Weltimmo)" EDPLR 1, no. 4 (2015), p. 309.

9 Ibid. (Fn. 9). p. 314.

10 "[…] meaning that an organisation only needs to comply with the data protection laws in place in the jurisdiction in which it has its main establishment." *Com*. - Fact Sheet, Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, 28 January 2015.

proposed by the new Regulation is Art. 60 GDPR that sets out a cooperation between the concerned supervisory authorities. Notwithstanding, in these cases the general rule of Art. 55 I GDPR will apply and therefore each DPA shall be competent to perform the tasks and exercise the powers on the territory of its own Member State. In the end, the new GDPR does not clearly define the territorial scope in these specific cases but introduces a dispute resolution mechanism (Art. 65 GDPR) which will be explained further in the ongoing work. However, in order to avoid such incoherent constellations, the one-stop shop must mean a robust power for the competent authority in every aspect and primarily excluding any other competing ones.

IV. The importance of cooperation in European data protection enforcement

In her speech at the "eco MMR congress-data protection 2012" Viviane Reding stated that close and consistent cooperation in any matters of the internal market represents one fundamental aspect of European data protection.[11] Following this idea, the GDPR introduces a system built on an enhanced coordination between the authorities and the EDPB ensuring a certain level of consistency (Arts. 63 ff. GDPR). These forms of cooperation can be seen as a condition for a harmonised application of data protection rules but simultaneously may reveal contradictive enforcement-elements. The more detailed the procedures of cooperation are, the less they leave a certain margin of discretion for the national administrative autonomy.

1. National cooperation during multiple procedural stages

The systematic analysis of the structure of territorial powers and multiple competences revealed a potential for remaining conflicts. As these problems might not always be appropriately and effectively solved by supranational decisions of the EDPB, transnational cooperation gains a prior importance. A possibility to gain a wider jurisdiction to some extent is to cooperate with the actual supervising authority. First and foremost, such assistance is, due to the conflicts concerning the territorial competence, especially needed between the "leading" DPA and the other supervisory authorities concerned. During the enforcement-process, they shall, due to Art. 60 I-III GDPR, not only reach a consensus and exchange all relevant information but provide mutual support. The entire provision codifies in detail the prior interaction between authorities regarding themselves as competent and thus avoids incoherent and conflicting measures. The specified description of the mutual assistance-processes provides Art. 61 GDPR. Thereafter, each supervisory authority shall take all appropriate measures required to reply to a request of another DPA. More specifically, during these common examinations, each national DPA substantially affected by the processing, shall have the right to participate and confer powers, including investigative powers. In case an authority denies joint actions, Art. 62 VII GDPR constitutes the remarkable possibility of adopting provisional measures. The joint operations of supervisory authorities including investigations and common enforcement measures is a novelty. As the new Regulation provides one directly applicable legal source, why these detailed provisions and the accompanied interference within the national administrative autonomy still should be necessary? Firstly, certain provisions still offer a margin of appreciation that has to be coordinated by coherent instruments of cooperation. Secondly, as the idea of the one-stop shop is to avoid parallel competences, the possibility of transnational collaboration and information of the national DPAs shall not be excluded. Thirdly, a possible complaint at the domestic authority for executive measures in another Member State requires the described cooperation and mutual assistance.[12] In detail, the request of the data subject is simplified but demands the facilitation of extra-territorial actions and highly challenges the internal responsibilities of every DPA. As a consequence, extensive problems of joint responsibilities may arise and were approached in Art. 62 IV-V GDPR. It codifies that a supervisory authority operating in another Member State cannot be held liable for any damage caused during their operations. More specifically, in accordance with its domestic legislation, the hosting Member State shall assume responsibility for all their actions. Subsequently, the Member State of the seconding supervisory authority shall reimburse the payment of the host State. When introducing such complex forms of common investigations these provisions can be seen as the minimum liability conditions. In the end, joint administrative measures may not go further than the exchange of information if they cannot provide a higher level of protection. At least any common administrative enforcement can be regarded as legal, as long as the final arbiter may be identified and judicially responsible for the respective decision.

2. Supranational interplay between national agencies and the EDPB

In addition to the one-stop shop, the consistency mechanism of Art. 63 GDPR shall guarantee that digital companies not only have to deal with one single authority but that they will comply with a harmonised enforcement of data protection rules throughout Europe. As the possibility of forum shopping, under the constellation of competing authorities for a company without any establishment, may still exist, the following cooperating

[11] *Reding*,"Sieben Grundbausteine für Europas Datenschutzreform", p. 6, Berlin, 20 March 2012, SPEECH/12/200.

[12] Art. 77 I GDPR entails a data subject's right to lodge a complaint against its domestic authority when another DPA might primarily be competent.

procedures with the EDPB shall extinct this exemption.[13] This European Board replaces the current interaction between the DPAs and the WP. In general, the national supervisory authorities, as the members of this panel, are given a platform for a voluntary cooperation. One of the most important tasks of the EDPB is, according to Art. 64 GDPR, not only anymore to ensure the consistent application of the rules but to answer or give opinions on concrete questions of administrative practices. During this novel process the national DPA communicates a draft decision to the EDPB before taking specific measures. In order to guarantee a commitment, Art. 64 VII/VIII GDPR claims that the supervisory authority has not only utmost take it into account but to justify any denial of the opinion. Accordingly, this mechanism guarantees that certain administrative decisions will be guided and commonly accepted by other actively participating DPAs. Furthermore, it implies that also local DPAs can play a decisive part in the process because they can express diverging opinions. The consistency mechanism, in which the DPAs commonly determine balanced solutions under the guidance of the EDPB, will be a strong and diversified instrument of supranational cooperation. On top of that, the future EDPB can, through a more intense and independent elaboration of guiding instruments, reinforce the coherent implementation of the data protection provisions. While retaining the essential element of national administrative autonomy, various instruments contributing to a special coordination and, where necessary, even a strict supranational enforcement are introduced. As a consequence, national and European authorities now have individual tasks in an alternative system of checks and balances.

V. Independent national DPAs facing new hierarchical powers of the EDPB

The big difference between the upcoming GDPR and the current DPD are the various possibilities to guide and lead the data protection system in Europe. This was necessary because substantial differences affect not only the application of the rules but "Member State DPAs seem to remain helplessly bound to national borders."[14] In this perspective, the critical question is whether those enforcement mechanisms will approach a single supranational supervisory system that reduces the enforcement-autonomy of the national agencies. Therefore, the new dispute resolution system (DRS) of Art. 65 GDPR has to be critically analysed. Although being part of the more general consistency mechanism, this DRS reveals a structural difference converting the mentioned cooperative guidance to a direct enforcement. The EDPB's binding DRS can establish harmonised decisions even in important individual cases.[15] It goes without saying that not every national decision can be subject to such a dispute resolution because this would overload and erode the effectiveness of the mechanism and simultaneously endanger the principle of subsidiarity and thereby the authorities´ national autonomy. Therefore, the DRS should be seen as an exceptional mechanism applying only and insofar as a real issue of consistency arises. In order to exclude a conflict of interests, the EDPB can intervene through the Arts. 64/65 GDPR. Beneath those are special conflicts concerning draft decisions of the lead authority, the main establishment, the competent supervisory authorities and about opinions of the EDPB (Art. 65 I a-c GDPR). When in exceptional circumstances certain flexibility is needed, Art. 66 GDPR allows the national supervisory authorities to derogate from that obligation in an urgency procedure. As clear as the accelerating intention of this provision is, as unclear remains when 'exceptional circumstances' might be given. Even the clarification of 'an urgent need to act in order to protect the rights and freedoms of data subjects' is not helpful because then any case may deserve the term of urgency. A sensible verification could have been that the infringements may bear concrete dangers for additional fundamental rights violations. Nevertheless, the DRS marks a remarkable step for consistency of concrete administrative practices allowing the Board to intervene each time a national supervisory authority intends to take a decision affecting data subjects or data controllers located in another country. It pressures the leading DPA who might tend to follow a lenient practice in order to be economically attractive for digital companies: e.g. when there is a lack of effective enforcement of supervision, as seen in the *Schrems* case where the Commissioner of the Irish supervisory authority denied the respective complaint.[16] More specifically, the suspension of decisions of the concerned supervisory authorities on the subject matter in the meantime (Art. 65 IV GDPR) and the obligation to adopt the final decision on the basis of the decision of the EDPB (Art. 65 VI GDPR) are essential progresses of this institute. On the contrary, the described European mechanisms reveal in its central position a mixture of administrative enforcement practices. It is essential that the extinction of the national autonomy to render final decisions and the independency of the DPAs are general limits of a complete harmonisation. In this light, the new system of integrated administration through the EDPB also raises difficulties with regard to judicial protection, because the complex decision-making process takes several preforming stages before the final decision. Initiating this supranational enforcement through the consistency mechanism and the DRS, severe problems arise

[13] And shall also limit the introduced centralism of decisions by the EDPB: *Dix*, "Datenschutzaufsicht im Bundesstaat - ein Vorbild für Europa" DuD 36, no. 5 (2012), pp. 320 f.

[14] *De Hert,/Papakonstantinou*, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals" CL & SR 28, no. 2 (April 2012), p. 138.

[15] *EDPS*, recommendations on the EU's options for data protection reform 2012/0011 (COD), 27 July 2015, Document attached to the procedure.

[16] *CJEU*, Schrems, C-362/14, para. 29.

when neither the EDPB nor national authorities may be predominantly responsible for the execution of the law. A solution concerning proceedings brought against a decision of a DPA, preceded by an opinion or a decision of the EDPB, offers Art. 78 IV GDPR stating that this prior measure can be forwarded to court. As remarkable this first approach for the review of guiding supranational measures may sound, as unclear remain the practical consequences for the illegality of an opinion of the EDPB and the determined national measure after a courts´ decision. Due to the constitutional principles of legal transparency and the vertical separation of powers, such commingling of executive bodies is restricted in Germany.[17]

VI. Limits and prospects of future supranational enforcement

Having analysed the European system of data protection supervision one might draw the picture of a strongly emerging and effective mechanism. Taking into consideration that *a priori* the enforcement powers of supranational agencies are limited, this conclusion seems to be even more surprising. In general, data protection cannot be regarded as a classic part of regulation because it primarily serves the fundamental right of privacy and not political interests. Due to the hidden nature of the data processing and the speed of the infringement, which will be in most of the cases irrecoverable, preventive controls constitute a central part of this system. In this sense, the vanishing of a general authorisation mechanism will be a remarkable loss, even if it introduces a more pragmatic, more economically-friendly approach. The possibility of an abuse of market power could provide danger for a "race to the bottom" of privacy protection.[18] As this danger is real but also part of certain mistrust to private entities processing personal data, how can this weakness be encountered? If the behaviour of digital giants depending on their customers shall be changed, transparency has to be a central element. In addressing that, a central role can be played by a more rigorous prior impact assessment of big data processing, not only focussing on data security, but considering the data's social and ethical impact. This is not different from the procedure of people using cars or taking medicines: due to the users' lack of competence to know the details of these products or the possibility of choice, the risks must be assessed objectively.[19] Under the supervision of national DPAs defining the professional requirements of external controls, it should be conducted by third parties. In this light, it can facilitate identifying how data processing affects collective interests. Part of a better solution would also be the publishing of the assessments' results on the product and thus making data subjects aware of data processing and the respective risks. As a consequence of prior compliance and examination, companies and their machines or software could install technologies that a priori do not process special types of data. As the 'Europeanisation' of the national administrative structures by the new Regulation follows the aim to prevent an inconsistent national application and lack of legal certainty, might even further European guidance play an important role? A definitely more far reaching system would have been the introduction of one single European Supervisor ensuring not only legality but the appropriateness of every national DPAs' actions. As reasonable as this argument, due to the necessity of a standardised enforcement in the field data protection, firstly may sound, as weak turns it out to be in a different light. Especially it remains critical that civil protection is a constitutional task of every Member State: such a supervisory authority at European level, pursuant to Art. 16 II TFEU, with a decisive right of direction vis-à-vis national DPAs would endanger the principle of subsidiarity, thus of prior national enforcement. It would erode the developed national structures and be overloaded with too much concentrated power that in the end violates the fundamental condition of every authority's independence. In this perspective, the introduced mechanisms of particular supervision and cooperation may be more complex but contribute to a balance between harmonised data protection and national autonomy. Other positive borders that the described structure of hierarchical and multiple administrative enforcement may not cross is the overall value for the individual in the complex European universe of data protection, namely effective judicial protection. Although the general question of effective remedies will be clarified in Arts. 77/78, the problem of public liability remains entirely unanswered: in former Art. 56 III a-III c Proposal of the Com for a GDPR, such responsibilities for operative-damages of the supervisory authorities were explicitly codified. As they are nowhere to find in the final version, this implicates that the quality of compensation in case of any administrative misconduct can be framed by the Member States' jurisdictions. A solution could have been to clarify the current procedural provisions and set up task forces especially in supranational forums that are the centre of mixed responsibilities. In addition, the possibility of litigations in alternative dispute resolution systems has been entirely ignored in the new GDPR. Such a mechanism in a tribunal for consumer claims, maybe in form of class actions, could not only assist data subjects and business operators in negotiating an agreed settlement, but relieve DPAs and courts from masses of requests. The positive effect of such alternative tribunals, especially in the complex and individual field of the right to be forgotten or other delicate consumer rights would be to develop common standards before legal actions have to be taken by

[17] *German Constitutional Court*, Judgment of 20 December 2007-2 BvR 2433/04, paras. 128 ff.

[18] Compare thereto: EDPS, preliminary Opinion "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. p. 34.

[19] Compare in depth: *Mantelero/Vaciago*, "Data Protection in a Big Data Society. Ideas for a Future Regulation" Digital Investigation, 15 (December 2015), p. 105 f.

the individual. Of course this mechanism cannot entirely replace a court system in the field of data protection but easily help to create a forum where global players face real concerns of their customers in advance of long trials. In the end, these enhancements could have a double effect. Firstly, our own system in the Union would be more robust and a real factor for a digital development accompanied by the essential trust of data subjects. Secondly, the impact that the EU system may have as a role-model approach on other international data protection systems, could in the end improve our own protection outside the territorial borders. Furthermore, we have to consider that, although it will be impossible to entirely combine technological revolutions, economic growth and fundamental rights protection, this may not inevitably imply that there might be no way to govern our privacy regulation. While the new mechanisms are progressively empowering data subjects, national DPAs and supranational structures at the same time, the future equilibrium of data protection and economic interests can be created as follows: breathing life into autonomy of all involved parties by integrating a coordinated prior compliance.