Enforcing Data Protection Law – the Role of the Supervisory Authorities in Theory and Practice

Felix Bieker

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD, Independent Centre for Privacy and Data Protection), Kiel, Germany
fbieker@datenschutzzentrum.de

Abstract. This paper examines the role of the supervisory authorities for the enforcement of the EU data protection regulation. It therefore examines the case law of the Court of Justice of the European Union and the upcoming legislative changes under the General Data Protection Regulation, which includes detailed provisions for the cooperation of all European supervisory authorities. It is concluded that for the system to work as envisaged, the Member States have to allocate appropriate means to the supervisory authorities.

Keywords. Data Protection, Privacy, General Data Protection Regulation, Enforcement, Supervisory Authorities, Data Protection Authorities, Court of Justice of the European Union

1 Introduction[1]

The current legal regime for data protection in the EU, the Data Protection Directive 95/46/EC (DPD), obliges the Member States under Article 28 DPD to set up supervisory authorities to monitor its proper application. The provision requires that the authorities act in complete independence. In order to achieve this end, they must have investigative powers, including access to data and the collection of all necessary information, powers of intervention, such as ordering the erasure of data, imposing bans on processing or admonishing controllers, and the power to engage in legal proceedings when the national provisions implementing the DPD have been violated. In order to protect the rights of data subjects with regard to the processing of data, they may lodge complaints with the supervisory authorities.

The notion of independence has been interpreted by the EU's Court of Justice (ECJ or the Court) with regard to its implementation in Germany [1], Austria [2], as well as in Hungary [3, 4]. Additionally, there have been questions concerning the scope of application of the national rules implementing the DPD in the Member States before the ECJ [4, 5] and the competence of the authorities to hear claims of individuals

[1] This paper has received funding by the Bundesministerium für Bildung und Forschung (German Federal Ministry of Education and Research) for the project Forum Privatheit – Selbstbestimmtes Leben in der Digitalen Welt (Privacy-Forum), www.forum-privatheit.de.

under Article 28(4) DPD [5, 6]. Furthermore, the supervisory authorities have been [4, 5] and continue to be [7] involved in proceedings before the ECJ in order to request its interpretation of the EU data protection legislation.

While the legal framework for the supervisory authorities was limited to one Article in the DPD it has been extended considerably in the General Data Protection Regulation [8], which has recently been adopted by the European legislator and will become applicable in the first quarter of 2018.

Even though the data protection regime includes its own unique enforcement mechanism and the supervisory authorities are the prime enforcers of data protection law, this topic is barely discussed in academia. Therefore, this paper analyses the jurisprudence of the ECJ to define the status quo of the rules on supervisory authorities and examines in how far the forthcoming GDPR advances that status. Therefore, the requirements for the organization of the supervisory authorities will be examined (2) as well as the question of which supervisory authority is competent to enforce data protection law in a given case (3). Lastly, the power to hear individual claims (4) is assessed. It is concluded (5) that under the current and future regime, the supervisory authorities are supposed to work as agents of individual rights with regard to the processing of personal data. However, in order to honour this commitment the Member States will have to allocate the appropriate means for the effective enforcement of the data protection rules across 28 Member States.

2 Organization of Supervisory Authorities

Article 28 DPD requires completely independent supervisory authorities. Within the EU legal order – which is a legal order independent of those of its Members States – it is for the Court of Justice of the European Union to interpret any provision of EU law. Even though the DPD came into force in 1995, it took considerable time before the first cases concerning the work of the supervisory authorities were brought before the Court. It started with a series of proceedings instigated by the Commission against Member States for failure to fulfil obligations of EU law under Article 258 TFEU, namely the proper implementation of Article 28 DPD in national law.

The Court, holding in 2010 that the supervisory authorities are 'the guardians of […] fundamental rights and freedoms' with respect to the processing of personal data [1], largely followed the arguments advanced by the Commission. It defined the notion of acting with 'complete independence' as stipulated by Article 28(1) subparagraph 1 DPD as being without influence not just by those who are supervised – in the case at hand private sector companies – but generally without taking any instructions or being pressured, including direct as well as indirect influence. Thus, there was no room for state scrutiny, which might allow the government to cancel or even replace decisions in the interests of public contractors in the private sector or leniency on economically important companies [1].

Further, the members of the supervisory authorities had to be functionally independent from the government. While Member States were not obliged to grant them a separate budget, there could be no overlap in personnel between the government and

the authority, which could lead to direct influence of the former. However, even indirect influence such as an unconditional right to be informed about the work of the supervisory authority was seen by the ECJ as not permissible [2].

Another form of undesirable influence is any act of the government that might coerce the authority into a certain course of action in order to avoid disadvantages in the future. This issue was contentious in a case against Hungary, where the government decided to discharge the head of the supervisory authority before the end of his regular term [3]. The ECJ held that these measures, which in the case at hand did not even conform to the national rules and safeguards, were liable to induce such acts of prior compliance, which contravene the authority's independence.

The forthcoming EU data protection regime incorporates the ECJ's rulings into secondary law. Under Article 52(1) GDPR the supervisory authorities remain completely independent in their work and it is now expressly stated in Article 52(2) GDPR that they may not be subject to direct or indirect influence. The functional independence from the government is explicitly laid down in Article 52(6) GDPR. Article 53(3) and (4) GDPR include specific rules for the expiry of the term of office or a resignation of members of the supervisory authorities and the requirement that they may be dismissed solely in cases of serious misconduct or if they no longer fulfil the conditions required for their position, which are to be provided by the Member States according to Article 54(1) GDPR. While the ECJ found that under Article 28 DPD the Member States did not have to provide the authorities with a separate budget, that same obligation is now laid down in Article 52(7) GDPR.

3 Enforcement of Data Protection Law and Cooperation of Supervisory Authorities

3.1 Enforcement of Data Protection Law

The supervisory authorities have jurisdiction to enforce the data protection rules of their respective Member State's national implementation legislation within their territory according to Article 28(1) DPD. The determination whether the national law is applicable is therefore crucial. According to Article 4 DPD this is mainly the case when the controller carries out the processing in the context of the activities of an establishment. The ECJ interprets the provision's scope broadly in order to ensure effective and complete protection of individual rights [4]. Thus, for the requirement of carrying out the processing in the context of the activities of an establishment under Article 4(1)(a) DPD an establishment as stated in Recital 19 DPD entails the effective and real exercise of activity under a stable arrangement, while the legal form of that establishment is not decisive.

As the processing does not have to be carried out by the establishment itself, but only in the context of its activities, this means that even when the establishment of an undertaking in a third State only supports the operation, inter alia by promoting and selling advertising space to make the operation profitable, this is sufficient to link the activities of the establishment and the processing of data. Thus, the national law of the

Member State where that establishment is located is applicable. In another case, the Court held that even the operation of a website in a Member State, using exclusively that State's language, fulfils the criteria of an establishment, if the processor has a representative in that country [5]. However, the nationality of the users of the website is of no relevance for determining the applicable law. Thus, different national implementations of the DPD may apply to the establishment and the main establishment, depending on their location, even though they all concern the same data processing carried out by the main establishment. This interpretation is explicitly regulated in Article 4(1)(a) clause 2 DPD, which states that where a controller is established on the territory of several Member States, he must ensure that each establishment complies with the respective national law.

As each supervisory authority is competent to enforce the national implementation of the DPD on its territory, a supervisory authority may choose to enforce the national law against any processor who is established on its territory. As the Court has held, however, where the main establishment of the controller is in another Member State, it may not enforce its national law against that main establishment, as this lies within the jurisdiction of the supervisory authority of that Member State and would infringe the principles of territorial sovereignty and legality, as well as the rule of law [4]. Nonetheless, it follows from this and Article 4(1)(a) clause 2 DPD that the supervisory authority of a Member State may enforce the national data protection rules against the establishment even when the data processing is carried out by the main establishment located in another Member State.

The provisions on the enforcement of the data protection regime by the supervisory authorities have been left largely untouched by the current reforms. As the relevant rules are now provided by way of a regulation according to Article 288 TFEU they are applicable in the Member States without any implementing measures. Thus the supervisory authorities now enforce EU law directly, rather than EU law in the guise of national implementation measures. However, this differentiation is more of an academic nature and bears little practical consequence.

More importantly, the link to the enforcement in the territory of the supervisory authority's Member State under Articles 55(1) and 57(1)(a) GDPR remains unchanged. Article 3(1) GDPR on the territorial scope, which replaces Article 4(1)(a) DPD, contains the same notion of processing personal data 'in the context of an establishment' as interpreted by the ECJ. Furthermore, the Courts' conclusions have been partially incorporated in the Recitals. Just as Recital 19 DPD, Recital 22 GDPR states that the concept of establishment implies the real and effective exercise of activity through stable arrangements, while the legal form of these arrangements does not prejudice a finding of an establishment. The question of whether a website is aimed at persons in a particular Member State is dealt with in Recital 23 GDPR, which also proposes to consider factors such as the language or currency used on the website. However, this is not done in the context of whether there is an establishment, but rather under the category of offering goods and services while the controller is not established in the EU according to Article 3(2)(a) GDPR.

3.2 Cooperation of Supervisory Authorities

As the 28 Member States set up one or multiple supervisory authorities in accordance with their national law and the DPD according to its Article 1 aims to ensure the free flow of data between these Member States, the supervisory authorities have to cooperate in many cases.

Status Quo. Article 28(6) DPD thus lays down a duty to cooperate. This includes inter alia the exchange of information. In its eponymous Article 29 the DPD set up a Working Party consisting of representatives of the supervisory authorities of each Member State as well as a representative of EU institutions and bodies and one of the Commission. While the latter have no voting rights, the Working Party adopts its decisions by a simple majority under Article 29(3) DPD.

The Article 29 Working Party is charged with examining questions on the application of national implementation measures, issuing opinions to the Commission on the level of protection in the EU and third countries, advising the Commission on safeguards for the rights and freedoms of natural persons and giving opinions on codes of conduct designed on EU level according to Article 30 DPD. Further, it may put forward recommendations on any matter related to the protection of personal data in the EU.

Upcoming Changes. The system of cooperation between the respective national supervisory authorities is overhauled completely in the forthcoming legislation [on the genesis of these provisions, cf. 9]. According to Article 51(2) GDPR the authorities contribute to the consistent application of the data protection regime throughout the EU and cooperate among each other and with the Commission under rules that are set out in Chapter VII GDPR.

European Data Protection Board. The Article 29 Working Party will be succeeded by the European Data Protection Board, which according to Article 68(1) and (3) GDPR has legal personality and consists of the heads of each supervisory authority of the Member States and the European Data Protection Supervisor. In Member States where there is more than one supervisory authority a joint representative is to be appointed under the national law as a single point of contact for other supervisory authorities, the Board itself and the Commission (Recital 119 GDPR). Articles 73 and 68(2) GDPR provide that the Board elects one of its members as chair, who represents the Board for a maximum of two consecutive terms of five years. Further, the Commission may participate in the Board, but has no voting right according to Article 68(5) GDPR. The Board takes all decisions by a simple majority, unless otherwise provided according to Article 72(1) GDPR. Among its tasks enumerated in Article 70 GDPR is the provision of guidelines concerning the exercise of the national supervisory authorities' powers under Article 58(1), (2) and (3) GDPR. Further, the Board gives the Commission an opinion with regard to the adequacy assessment for the transfer of data to third countries.

Lead Supervisory Authority. In cases of cross-border processing, the supervisory authority of the main establishment or of the single establishment of the controller or processor acts as lead supervisory authority.[2] Under the propagated one-stop-shop scheme it is the sole interlocutor of the controller or processor according to Article 56(6) GDPR. According to the definition of Article 4(23) GDPR cross-border data processing occurs, where the processing takes place within the EU in the context of a controller's or processor's establishments in multiple Member States or where the processing takes place in the sole establishment of a controller or processor in the EU, but which substantially affects or is likely to substantially affect data subjects in more than one Member State. If there are conflicting views on which of the concerned supervisory authorities is competent for the main establishment of a controller or processor, the Board has to adopt a binding decision under the consistency mechanism of Article 65(1)(b) GDPR.

When the processing of data is performed by public authorities or private bodies acting with public authority the supervisory authority of the Member State concerned has the competence to act according to Article 55(2) GDPR and the rules of Article 56 GDPR do not apply.

Also, according to the exception clause of Article 56(2) GDPR, this does not apply, where a complaint concerns a matter which relates only to an establishment in one specific Member State or only substantially affects data subjects in one specific Member State. In such cases the supervisory authority of the Member State concerned[3] has to inform the lead supervisory authority, which has to decide whether it invokes the procedure of Article 60 GDPR or not within three weeks as prescribed by Article 56(2) GDPR. If it does, the supervisory authority which informed the lead authority is tasked with preparing a draft for decision, which has to be taken into account to the utmost by the lead authority for its own draft in preparation for the decision under Article 60(3) GDPR. If the lead supervisory authority decides not to deal with the case, the supervisory authority which informed it handles the case either with

---

[2] The term main establishment is defined in Article 4(16)(a) GDPR with regard to a controller as the place of central administration within the EU, except where another establishment within the EU is tasked with deciding the purposes and means of data processing and has the power to implement such decisions, which then in turn is regarded as main establishment. Recital 36 GDPR employs the wording of the Court and requires the effective and real exercise of activities determining the main decisions regarding the means and purposes of processing through stable arrangements. A processor's main establishment is defined in Article 4(16)(b) as the place of central administration or, in lieu of such a place, the establishment where the main processing activities take place to the extent that the processor is subject to specific obligations under the GDPR. In cases involving both, a controller and processor, the main establishment of the controller should be decisive to determine the lead supervisory authority according to Recital 36 GDPR.

[3] Article 4(22) GDPR defines the supervisory authority concerned as the one which is concerned by the processing, due to the controller's or processor's establishment on the territory of its Member State, the data subjects residing in its Member State are substantially affected or likely to be affected, or a complaint according to Article 77 GDPR has been lodged with that supervisory authority.

the assistance of other supervisory authorities according to Article 61 GDPR or as a joint operation under Article 62 GDPR.

While the lead authority is in charge of operations, under Article 60(1) GDPR it has to cooperate with the other supervisory authorities concerned in order to reach a consensus on actions to be taken. It may request assistance by other concerned supervisory authorities under Article 61 GDPR, and especially for purposes of carrying out investigations or monitoring the implementation of measures taken, may conduct joint operations in accordance with Article 62 GDPR. All supervisory authorities concerned exchange relevant information (Article 60(1) cl. 2 and (3) GDPR).

Concerning a decision, it is for the lead supervisory authority to submit a draft to the other concerned supervisory authorities. According to Article 60(3) GDPR, their views have to be taken duly into account. Further, the other concerned supervisory authorities may, within four weeks, express relevant and reasoned objections as provided by Article 60(4) GDPR. This term is defined in Article 4(24) GDPR as stating whether there is an infringement of the GDPR, whether the envisaged action is in accordance with the GDPR and clearly demonstrate the significance of risks incurred by the draft decision with data subjects' fundamental rights and freedoms or the free flow of personal data.

- If the lead supervisory authority does not follow the objection or regards it as not relevant and reasoned, it has to apply the consistency mechanism and the Board has to adopt a binding decision according to Article 65(1)(a) GDPR.
- If the lead supervisory authority agrees with the objection, it has to submit a revised draft to the other concerned supervisory authorities, who then have to submit any objections within two weeks according to Article 60(5) GDPR.
- If no objections are submitted within the prescribed period, a consensus is deemed to exist by Article 60(6) GDPR and all supervisory authorities concerned are bound by the decision.

When the decision is adopted, it is for the lead supervisory authority to take action with regard to the controller or processor, while the supervisory authority to which a complaint was lodged has to inform the complainant according to Article 60(7) GDPR.

Any of the supervisory authorities concerned may exceptionally invoke the urgency procedure of Article 66 GDPR when it finds an urgent need to act to protect the interests of data subjects.

The new rules for the cooperation of the supervisory authorities set up a formal system of procedures and deadlines. This can be attributed to the complexity of a one-stop-shop approach for the enforcement of common rules across 28 Member States. While this is intended to allow effective cooperation, the strict deadlines also put a burden on the supervisory authorities. It will take considerable resources to enable them to actively participate in investigations and supply information to other authorities and process information received.

Mutual assistance. The mutual assistance procedure of Article 61 GDPR is supposed to contribute to consistent implementation and application of the GDPR. It especially concerns information requests and supervisory measures, for instance requests to carry out prior authorizations and consultations, inspections and investigations. Under Article 61(3) GDPR the use of information exchanged is expressly limited to the purpose for which it was requested.

The requested supervisory authority has to submit the information without undue delay, but no later than a month after the request according to Article 61(2) GDPR. The requested supervisory authority may refuse requests only under Article 61(4) GDPR when it is not competent ratione materiae or the measures requested violate provisions of the GDPR, Union or national law which binds the requested supervisory authority. Any refusal to submit information has to be substantiated with reasons according to Article 61(5) GDPR. If the requested supervisory authority fails to act within the prescribed period, Article 60(8) GDPR authorizes the requesting supervisory authority to take provisional measures in its Member State. However, the urgency procedure of Article 66 GDPR is triggered: While the urgent need to act is presumed, an urgent binding decision by the Board prescribed by Article 66(2) GDPR is required.

Joint operations. The joint operations mechanism under Article 62 GDPR extends to investigations and enforcement measures and gives the supervisory authority of any Member State concerned a right to participate in such operations. Supervisory authorities are either invited by the competent supervisory authority or can request to participate according to Article 62(2) GDPR. If such a request is not granted within one month Article 62(7) GDPR provides that the other supervisory authorities may take provisional measures. In that case, as under Article 60(8) GDPR for the mutual assistance procedure, the urgency mechanism of Article 66 GDPR is then triggered.

In a joint operation a supervisory authority may, in accordance with national law, grant investigative powers on a seconding supervisory authority or, if allowed by national law, authorize the seconding supervisory authority to exercise its powers as provided by Article 62(3) GDPR. Both modi are subject to the guidance and presence of members or staff of the host supervisory authority and subjects the supervisory authorities own members or staff to the national law of the host Member State. In turn, the host supervisory authority assumes responsibility for the actions of the supervisory authority acting in its Member State under Article 62(4) GDPR.

Consistency Mechanism. The Board is at the heart of the consistency mechanism set out in Articles 63 et seq. GDPR. In order to ensure consistent interpretation and application of the GDPR, the Board may issue non-binding opinions under Article 64 GDPR and binding decisions in accordance with Article 65 GDPR.

While Article 64(1) GDPR provides a list of activities of the supervisory authorities where the Board gives an opinion[4] – such as the list defining when a Data Protection Impact Assessments has to be carried out under Article 35(4) GDPR, standard protection clauses under Articles 46(2)(d) and 28(8) GDPR among others – it may also be approached by supervisory authorities, the chair of the Board or the Commission to examine any matter of general application or affecting more than one Member State under its second paragraph. This particularly concerns cases where a supervisory authority does not comply with its obligation to provide mutual assistance under Article 61 GDPR or engage in joint operations as prescribed in Article 62 GDPR and detailed above. The opinions of the Board have to be issued within eight weeks, which may be extended by another six weeks depending on the complexity of the issues according to Article 64(3)

As described above the Board adopts decisions according to Article 65(1) GDPR, when the lead supervisory authority does not follow objections of supervisory authorities concerned, regards them as irrelevant or unreasoned, when there are conflicting views on the main establishment of a controller or processor, or when the competent supervisory authority either fails to request an opinion of the Board or decides not to follow an opinion of the Board under Article 64 GDPR.

Article 65(2)-(4) GDPR prescribes that all decisions are adopted with a two-thirds majority and generally within one month, which may be extended by six weeks. If the Board fails to adopt a decision by that time the quorum is lowered to a simple majority for an additional two weeks. In the case of a split vote, the chair decides. During the time of deliberation, the competent supervisory authority is barred from adopting its draft decision. As pointed out in Recital 142 GDPR decisions of the Board can be brought before the ECJ in an annulment action under Article 263 TFEU by supervisory authorities, as they are addressees of these decisions.

Lastly, there is an urgency procedure provided by Article 66(1) GDPR, which allows the supervisory authority concerned to circumvent the consistency mechanism of Articles 63-65 GDPR under exceptional circumstances in cases with an urgent need to protect the rights and freedoms of data subjects and to adopt immediate provisional measures for its Member State. These measures have to specify a period of validity, which may not exceed three months. In order to have final measures adopted, the supervisory authority concerned may request an urgent opinion or decision of the Board. According to paragraph 4 urgent opinions and decisions have to be adopted within two weeks by a simple majority.

In the opposite case, where the supervisory authority concerned does not take measures although there is an urgent need to act in order to protect the rights and freedoms of data subject, any supervisory authority may request an urgent opinion or decision of the Board according to Article 66(3) GDPR.

---

[4] The requesting supervisory authority has to "take utmost account" of the opinion in cases of Article 64(1) GDPR, yet according to Article 64(7) GDPR it also has the option to maintain its draft decision. However, as provided by Article 65(1)(c) GDPR the Board may be approached by other supervisory authorities or the Commission to adopt a binding decision on the matter if the competent supervisory authority does not conform to an opinion issued by the Board or fails to approach the Board in the cases of Article 64(1) GDPR.

Even though the Board is mainly based on cooperative action, certain elements such as the possibility of the lead authority to dismiss reasons of another supervisory authority as unfounded under Article 60(4) GDPR, to take a supervisory authority refusing to grant mutual assistance according to Article 60(8) GDPR or refusing to let another supervisory authority join investigations according to Article 62(7) GDPR before the Board, or to invoke the urgency procedure where a supervisory authority fails to take action as provided by Article 66(3) GDPR introduce an adversarial mode to the Board. In practice, these instruments will have to be handled carefully in order to allow productive cooperation between all of the supervisory authorities.

4 Power to Hear Individual Complaints

The supervisory authorities under Article 28(4) DPD have the power to hear claims brought by any person concerning the protection of his or her rights in regard to data processing, which is provided correspondingly, albeit relabelled as complaints, in Articles 77 and 52(1)(b) and (4) GDPR. For the individual this remedy is also enshrined in EU primary law as a fundamental right in Articles 8(1) and (3) CFR [cf. 6]. These rights are relevant for the interpretation of the powers of Article 28 DPD/Article 77 GDPR, as the supervisory authorities' powers are not merely an end in themselves, but rather serve to implement individual rights.

In order to process claims, the supervisory authorities have a range of competences granted by Article 28(3) DPD: they have investigative powers, powers of intervention, such as ordering a ban on processing, may engage in legal proceedings and, in turn, their decisions must be subject to appeals before the national courts. While the general scope of the competences has been preserved in the forthcoming legislation, the supervisory authorities' powers are described in more detail in Article 58(1)(a), (e), (f), (2), (4) and (5) GDPR.

4.1 Complaints Concerning Processing within the EU

Status Quo. According to the ECJ individuals may bring a claim to the supervisory authority when they are not successful in the exercise of their rights as data subjects, for instance under Articles 12 or 14 DPD [4]. If the competent supervisory authority finds a violation of fundamental rights, it may order the controller to take certain action. In the infamous case of Google Spain, this included the order to remove certain links form the search results of an internet search engine.

Further, the Court has ruled that when a complaint is lodged with an authority and it is unclear which national legislation applies, this does not change that authority's competence to hear that claim under Article 28(4) DPD [4]. However, the territorial application of the rules it enforces according to Article 28(1) and (3) DPD still applies. Thus the supervisory authority which is confronted with such a claim may exercise its investigative powers even if the law applicable is that of another Member State. Yet, its powers may be limited, especially regarding the imposition of penalties, as that would violate the territorial sovereignty of the other Member State and raise

issues regarding the principle of legality and the rule of law. In such cases, the supervisory authority can only rely on the duty of cooperation under Article 28(6) DPD for the enforcement of its actions on the territory of another Member State. If, however, there is an establishment on the territory of the supervisory authority's own Member State, it may take action against that establishment, where the required nexus to the processing as detailed above (3.1) exists.

Upcoming Changes. Article 77 GDPR gives individuals the right to lodge complaints with supervisory authorities if they consider that data processing relating to them violates the rules of the GDPR. The individual concerned may lodge his or her complaint inter alia with the supervisory authority of his or her habitual residence, place of work or the place of the alleged violation. Just like the lead supervisory authority provides a one-stop-shop for controllers and processors, the supervisory authority where the complaint is lodged is responsible to inform the individual on the progress and outcome of the complaint, as laid down by Article 56(2) GDPR with regard to lead supervisory authorities, Article 60(7)-(9) GDPR concerning cooperation between supervisory authorities and Article 65(6) GDPR for decisions of the Board.

Individuals further have the right to a judicial remedy, in accordance with Article 47 CFR, against legally binding decisions of the supervisory authority concerning them. Recital 142 GDPR states that the proceedings following national law should give the courts full jurisdiction including the examination of all questions of fact and law. Where the latter concern EU law it points to the preliminary reference procedure before the ECJ provided by Article 267 TFEU. If the supervisory authority competent under Articles 55 or 56 GDPR does not deal with a complaint or even when it fails to inform the individual of the progress or outcome of a complaint lodged under Article 77 GDPR within three months, individuals must have a judicial remedy against the supervisory authority, as further detailed in Recital 140 GDPR. Additionally Article 79 GDPR introduces a right for individuals to an effective judicial remedy against a controller or processor, including public authorities, before the courts of the Member State.

In order to pursue these rights, the data subject under Article 80(1) GDPR has the right to mandate a non-profit organization active in the field of data protection to exercise them on his or her behalf. Taking this point even further, Article 80(2) GDPR contains a flexibility clause allowing Member States to introduce a right of non-profit organizations to initiate proceedings under Articles 77-79 GDPR independent of a mandate by a data subject.

Additionally, as required by Article 53(5) and recital 128 GDPR national law has to enable the supervisory authority where a complaint is lodged, to engage in legal proceedings to enforce the rules of the GDPR.

4.2 Complaints Concerning the Transfer to Third Countries

The competence of the supervisory authority is not limited to actions concerning controllers within the EU. In the Schrems case, the ECJ dealt with the powers of the su-

pervisory authorities with regard to the processing of personal data in third countries. The Court argued that while the supervisory authorities could carry out their powers within the territory of their own Member State under Article 28(1) and (6) DPD, the transfer of data from a Member State to a third country under Articles 25 and 26 DPD was a processing of data within the meaning of Article 2(b) DPD, which was carried out in a certain Member State [6]. Consequently, the national supervisory authorities under Article 28 DPD read in conjunction with Article 8(3) CFR were also responsible to monitor compliance with the DPD in the case of data transfers to a third country.

When an individual lodges a claim, the supervisory authority has to examine it under Article 28(4) DPD regardless of whether the Commission has adopted a decision under Article 25(1) and (6) DPD as to the adequacy of the level of protection in that third country.[5] The ECJ clearly stated that the Commission decision does not prejudice the examination of an individual claim put before the supervisory authority, which must assess these with due diligence [6]. However, the supervisory authority itself cannot declare the Commission decision invalid. In EU law, it is within the exclusive jurisdiction of the Court to declare any acts of EU organs or institutions invalid. For the claims before the supervisory authority there are thus two possibilities:

- If the authority rejects the claim, the individual must have the possibility of judicial remedies according to Article 28(3) subparagraph 2 DPD.
- If the supervisory authority upholds the claim, it must, in turn, be able to instigate legal proceedings in compliance with Article 28(3) subparagraph 2 DPD.

In either case, the competent national court seized of the matter has to submit questions concerning the validity of the decision to the ECJ by way of a preliminary reference under Article 267 TFEU.

While the GDPR brings some changes to the system of transfer of personal data to third countries in Articles 44 et seq. GDPR – mostly in the form of more detailed provisions – the general concept remains the same. Thus, the finding of the ECJ that any transfer of personal data begins with a processing within the EU still stands. The supervisory authorities further retain the power to suspend data flows to recipients in third countries according to Article 58(2)(j) GDPR and must thus be able to investigate complaints concerning an alleged violation of provisions set out in the GDPR.

Article 45 GDPR now sets out the process for the adoption of adequacy decisions by the Commission in more detail: According to its second paragraph, the Commission has to take into account factors such as whether the country in question respects the rule of law, human rights and fundamental freedoms, the relevant national legislation concerning public and national security and access rights of public authorities as well as whether there are effective and enforceable data subject rights and effective

[5] The fact that the Commission's Safe Harbor Decision curtailed the supervisory authorities' powers with regard to self-certified organizations under Article 28 DPD was, as the ECJ held in Schrems, actually one of the reasons for its invalidity.

administrative and judicial remedies for data subjects. Further, the existence of an effective, independent supervisory authority is required.

If the Commission concludes that the level of protection is adequate in a third country or a specific sector in that country, the implementing act has to provide a mechanism for periodic review, as required by the ECJ in the Schrems case, which has to be carried out at least every four years according to Article 45(3) GDPR. When information reveals that the relevant country no longer meets the adequacy threshold, Article 45(5) GDPR demands that the Commission repeals, amends or even suspends its decision.

5 Conclusion

While the ECJ's judgments in the cases of inter alia Google Spain or Schrems attracted praise [10, 11], but also considerable criticism [12], it has been demonstrated that the GDPR incorporates many of the principles laid out by the Court. It is not to be expected that the ECJ will change its approach to enforce data protection law from a fundamental rights perspective under the new legislation.

However, as the joint enforcement of a harmonized data protection regime has to be coordinated appropriately, considerable resources will have to be mobilized. The supervisory authorities will need the appropriate budgetary furnishings to exercise their powers in their own Member State, communicate to individuals lodging complaints in a timely manner and be able to engage in meaningful cooperation beyond the national sphere.

The Court itself as well as the upcoming legislation emphasize the importance of lodging proceedings before the ECJ in order to ensure coherent interpretation. While the supervisory authorities already find themselves in a position where they have to engage in proceedings before the ECJ, a development which is likely to continue and even expand in frequency with the GDPR, as it will be more obvious that EU law is at issue in a case – a fact that may currently be overlooked in practice, as the parties before national courts focus on the national implementation legislation. The Court, in the few cases that reached it, has definitely played an important role in advancing the level of data protection in the EU. However, it has to be borne in mind that in most instances, i.e. the preliminary reference procedure, it takes considerable time before a case comes to the Court. Under Article 267 TFEU only national courts of last instance are obliged to refer their questions on EU law to the ECJ. As the proceedings before the Court differ from those before national courts, they require representation of the supervisory authorities by lawyers familiar with the intricacies of EU procedural law, which incurs substantial costs for the supervisory authorities in order to resolve contentious cases. And even though in the preliminary rulings procedure, which is of concern here, the language of the case is that of the referring national court according to Article 37 of the Rules of Procedure of the Court of Justice, translations of the questions submitted by the national court and its own written submissions are required in order to allow meaningful cooperation of the national supervisory authorities among each other and with the European Data Protection Supervisor, who may

also submit observations to the ECJ according to Article 47(1)(i) Data Protection Regulation (EC) No 45/2001 [13]. In order to enable the supervisory authorities to engage in meaningful cooperation, the Member States, in executing the provisions of the GDPR, are called upon to take these fiscal concerns duly into account.

The new mechanisms for consistency, including the establishment of the Board, are welcome, as the procedural rules allow it to work efficiently with the adoption of measures by a simple majority. However, its modus operandi has to keep a balance between cooperative and adversarial action.

From the case-law and the new legislation, the picture of the supervisory authorities as agents of individuals and their rights emerges. With this conception, based on the provisions of EU law, there is an agency capable to engage in the protection of the individual's rights and effectively counter interests and ambitions of multi-national companies engaging in the processing of personal data. However, due to their complete independence, the supervisory authorities ideally are also capable of engaging in controversies with other State actors, especially in the executive. Taking this concept of supervisory authorities as envisioned in the current and future EU law seriously in practice, will require awarding them the appropriate means and funds to exercise these powers.

References

1. *Commission v Germany*, C-518/07, EU:C:2010:125
2. *Commission v Austria*, C-614/10, EU:C:2012:631
3. *Commission v Hungary*, C-288/12, EU:C:2014:237
4. *Weltimmo*, C-230/14, EU:C:2015:639
5. *Google and Google Spain*, C-131/12, EU:C:2014:317
6. *Schrems*, C-362/14, EU:C:2015:650
7. Wirtschaftsakademie Schleswig-Holstein, C-210/16, pending
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 of 4 May 2016, 1-88, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1
9. Nguyen, A. M.: Die zukünftige Datenschutzaufsicht in Europa. Zeitschrift für Datenschutz, 265-270 (2015)
10. Kühling, J., Heberlein, J.: EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU. Neue Zeitschrift für Verwaltungsrecht, 7-12 (2016)
11. Jotzo, F.: Anmerkung. Juristenzeitung, 366-370 (2016)
12. Schwartmann, R.: Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Konsequenzen der Safe-Harbor-Entscheidung des EuGH. Europäische Zeitschrift für Wirtschaftsrecht, 864-868 (2015)
13. 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, OJ L 8 of

12 January 2001, 1-22, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=1