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

Felix Bieker

Enforcing Data Protection Law – the Role of the Supervisory Authorities in Theory and Practice[1]

Felix Bieker

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD, Independent Centre for Privacy 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.

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

1 Introduction

The raison d'être of data protection law in general is to protect the rights of individuals. Specifically, this is laid down in Article 1(1) of the current Data Protection Directive 95/46/EC (DPD) [1] as well as Article 1(2) of the upcoming General Data Protection Regulation (EU) 2016/679 (GDPR) [2]. The law thereby aims to compensate for the asymmetry in power between organisations (as controllers) and individuals (the data subjects) created by modern means of data processing [3]. However, this does not only affect the secondary law, but is also enshrined on the level of EU primary law: Article 8 of the EU Charter of Fundamental Rights (CFR) [4] guarantees the right to the protection of personal data. Furthermore, Article 7 CFR protects the right to private life, which also includes the protection of personal data relating to the private life of an individual [5]. The enforcement of these rights is entrusted to supervisory authorities in each Member State. According to the Court of Justice of the European Union, which interprets Union law authoritatively, the supervisory authorities protect the rights of the individuals with regard to the protection of personal data and "are therefore the guardians of those fundamental rights" [6].
In order to fulfil this advocacy role, Article 28 DPD requires that the authorities act in complete independence and have effective investigative powers (including access to

[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.

all necessary information), powers of intervention (such as ordering the erasure of data or imposing bans on processing) and the power to engage in legal proceedings when the national provisions implementing the DPD have been violated. Additionally, the data subjects themselves have the right to lodge complaints directly with a supervisory authority, in order to enforce their rights.

Since the coming into force of the DPD, there have been several judgments of the EU's Court of Justice (ECJ or the Court) concerning the interpretation of the supervisory authorities' role. The notion of independence was scrutinized with regard to the implementation in Germany [6], Austria [7], and Hungary [8, 9]. Additionally, the Court ruled on questions concerning the scope of application of the national rules implementing the DPD in the Member States [9, 10] and the competence of the authorities to hear complaints of individuals under Article 28(4) DPD [10, 11]. Furthermore, the supervisory authorities have been [9, 10] and continue to be [12] involved in proceedings before the ECJ in order to obtain an authoritative interpretation of the EU data protection legislation.

The upcoming secondary data protection law, the GDPR – which has already entered into force and will become applicable in the first quarter of 2018 – considerably extends the EU provisions on the supervisory authorities. As the legislator chose the form of a regulation, EU law will prescribe the role of the supervisory authorities in much greater detail.

This paper therefore analyses the jurisprudence of the ECJ to define the status quo of the law on supervisory authorities and examines in how far the forthcoming GDPR advances that status and thereby enables the supervisory authorities to fulfil their role as guardians of the rights to the protection of personal data. 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 in order to honour their role as prescribed by EU law, the supervisory authorities have to be allocated the means and resources to fulfil their role as advocates of fundamental rights.

2 Organization of Supervisory Authorities

Article 28 DPD requires that the supervisory authorities "act with complete independence." As the Court held in its very first judgment concerning the role of supervisory authorities, this notion includes multiple dimensions: being without influence not just by those who are supervised – private sector companies or public authorities, as the case may be – but generally without taking any instructions or being pressured, including direct as well as indirect influence [6].

Due to their advocacy role, as public enforcers of individual rights, the supervisory authorities have a unique position within their Member States. As they oversee both private companies and (other) public authorities, they must be independent from the public sector, i.e. the State they form part of themselves. In practice, this is achieved in different ways, for instance the members of the French Commission Nationale de

l'Informatique et des Libertes are appointed from various institutions, such as the parliament and the courts [13, Article 13]. In Germany, the heads of the supervisory authorities are elected by the respective federal or regional parlament [Cf. inter alia 14, § 35; 15, § 22].

However, as the ECJ found, the State itself may not only be interested in influencing a supervisory authority where its own actions are concerned, but also protect the interests of the private sector. Thus, there is 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 adopt a lenient approach towards economically important companies [6].

The members of the supervisory authorities have to be functionally independent from the government. While Member States are not obliged to grant them a separate budget, there can 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 is seen by the ECJ as not permissible [7].

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 [8]. 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.

There will be 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

As each of the Member States has its own supervisory authority, their jurisdiction is linked to the applicability of the national law implementing the DPD. Therefore, the determination whether the national law is applicable in a given case is crucial. Ac-

cording to Article 4 DPD this is the case when the controller carries out the processing "in the context of the activities of an establishment". In the *Google Spain* case, this was an issue, as Google argued that its data processing did not take place in its Spanish establishment, but at its corporate headquarters in the USA [10]. However, the ECJ pointed out that the DPD explicitly stated that the processing only had to occur in the context of the establishment's activities. It then ruled that when an establishment promotes and sells advertising space to make the operation profitable, this is sufficient to link the activities of the establishment and the processing of data. The Article 29 Working Party has generalized this requirement as meaning that the "activities and the data processing are 'inextricably linked'" [16, at p. 6].

Further, Recital 19 DPD refers to the effective and real exercise of an activity under a stable arrangement, while the legal form of that establishment is not decisive. Accordingly, in the *Weltimmo* 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 [9]. 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, it 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. The Court found, however, that where the main establishment of the controller is in another Member State, the supervisory authority may not enforce its national law against that main establishment. Rather this rests 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 [11]. 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. Especially 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 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 fac-

tors 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. Although the wide scope of the DPD in the interpretation of the ECJ has been seen critically by some [17, 18], the EU legislator has thus explicitly reiterated the Court's reasoning in the GDPR. This is not necessarily surprising, as the case law is closely linked to the wording of the DPD, which the ECJ interprets in the light of the individual rights of the primary law, in order to ensure effective and complete protection of individual rights.

3.2 Cooperation of Supervisory Authorities

As the 28 Member States set up one or multiple supervisory authorities[2] in accordance with their national law, there is currently a multitude of authorities in the EU which interpret the EU data protection regime, which poses the threat of fragmentation of the application of the law in practice.

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 such as the application of national implementation measures or issuing opinions to the Commission on the level of protection in the EU and third countries. It may further 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. 19]:

Lead Supervisory Authority. In an effort to streamline the jurisdiction of supervisory authorities in cases where the controller or processor is in another Member State than the data subject, the supervisory authority of the (main) establishment acts as lead supervisory authority.[3] Under this one-stop-shop scheme it is the sole interlocutor of the controller or processor according to Article 56(6) GDPR.[4]

---

[2] In the Federal Republic of Germany, for instance, there are 18 different supervisory authorities: one on the federal level and seventeen regional authorities of the *Länder*.

[3] 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.

While the lead authority is in charge of operations, under Article 60(1) GDPR it ultimately has to reach a consensus and therefore cooperate with the other supervisory authorities concerned. To this end, the lead authority may request assistance from other 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.

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 express relevant and reasoned objections as provided by Article 60(4) GDPR.[5] The coordination then proceeds as follows:

- 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 (explained below) 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 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

---

Recital 36 GDPR 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.

4 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, this is defined as cross-border data processing by Article 4(23) GDPR. 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.

5 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.

complaint was lodged has to inform the complainant according to Article 60(7) GDPR.

However, there are exceptions from the one-stop-shop scheme:

- It only applies to private companies; if public authorities or private bodies acting with public authority process data, the supervisory authority of the Member State concerned has the competence to act according to Article 55(2) GDPR.
- Where a complaint concerns a matter which relates only to one specific establishment in one Member State or only substantially affects data subjects in one specific Member State, the supervisory authority of the Member State concerned[6] has to inform the lead supervisory authority. The latter then decides whether it invokes the cooperation procedure of Article 60 GDPR.
  - If it does, the concerned supervisory authority prepares a draft for decision, which has to be taken "into account to the utmost" by the lead authority for its own 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 the assistance of other supervisory authorities according to Article 61 GDPR or as a joint operation under Article 62 GDPR.

The new rules for the cooperation of the supervisory authorities set up a formal system of procedures and strict deadlines of only two to four weeks. 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 deadlines also put a burden on the supervisory authorities. They will have to be able to follow proceedings in other Member States and respond to requests within the deadlines. Aside from the substantive and often very specific questions of EU data protection law, this also requires a timely and appropriate translation of documents. Thus, considerable resources will be required to enable the authorities to actively participate in investigations, supply information to other authorities and process information received within the short prescribed time periods.

Mutual assistance. The mutual assistance procedure of Article 61 GDPR especially concerns information requests and supervisory measures, for instance requests to carry out prior authorizations and consultations, inspections and investigations. Article 61(3) GDPR introduces the idea of purpose limitation for supervisory authorities: 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 no later than a month after the request and may refuse requests only when it is not competent

[6] 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.

ratione materiae or the measures requested violate provisions of Union or national law. Any refusal to submit information has to be substantiated with reasons.[7]

Joint operations. The joint operations mechanism under Article 62 GDPR extends to investigations and enforcement measures and gives the supervisory authorities of all Member States concerned a right to participate in such operations. They are either invited by the competent supervisory authority or can request to participate. If such a request is not granted within one month, Article 62(7) GDPR provides that the other supervisory authorities may take provisional measures.[8]

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, confer its powers on the seconding supervisory authority 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.

This is an interesting possibility, which has the potential to further European integration. Even though EU law is not a subset of international law, but rather its own, independent and sui generis legal order [20], the principle of the sovereignty of Member States is still paramount. In its *Schrems* judgment, the ECJ heavily emphasized that supervisory authorities could only exercise their jurisdiction within their own Member State and invoked this general principle [11]. In this regard, the GDPR goes beyond the status quo in allowing for joint operations and exercise of jurisdiction in another Member State, albeit subject to consent and supervision of the Member State concerned. However, as the Member States are reluctant to give up sovereignty with regard to other Member States, it will have to be determined in the future, whether these provisions found any practical application.

European Data Protection Board. The Article 29 Working Party will be succeeded by the European Data Protection Board, which consists of the heads of each supervisory authority of the Member States and the European Data Protection Supervisor.[9]

The Board generally takes all decisions by a simple majority. Its tasks are similar to those of the Article 29 Working Party: according to Article 70 GDPR, it advises the

---

[7] 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.

[8] In that case, as under Article 60(8) GDPR for the mutual assistance procedure, the urgency mechanism of Article 66 GDPR is then triggered.

[9] 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 members of the Board (Recital 119 GDPR), which facilitates coordination.

Commission, for instance by providing it with an opinion on the adequacy assessment for the transfer of data to third countries or examines any matter of general application or affecting more than one Member State, at the request of a Board member. 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 (as described above). The opinions of the Board have to be issued within eight weeks and are non-binding.[10]

Consistency Mechanism. A major change in the working of the supervisory authorities on the EU level is the consistency mechanism. It allows the Board to issue binding decisions according to Article 65(1) GDPR. This particularly concerns instances when the lead supervisory authority does not follow the objections of a supervisory authorities concerned or when the competent supervisory authority decides not to follow an opinion of the Board under Article 64 GDPR.

All binding decisions are adopted with a two-thirds majority and generally within one month.[11] 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. As the binding decisions of the Board can be seen as an interference with the independence of the individual authorities, the possibility to bring a decision before the Court is a mitigating factor.

For cases with an urgent need to protect the rights and freedoms of data subjects there is also an urgency procedure provided by Article 66(1) GDPR, which allows the supervisory authority concerned to circumvent the consistency mechanism under exceptional circumstances and adopt immediate provisional measures in its Member State. However, these measures have to specify a period of validity, which may not exceed three months. In order to adopt final measures, the supervisory authority concerned may request an urgent opinion or decision of the Board.[12]

In the opposite case, where a 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.

---

[10] However, when a supervisory authority requests an opinion, for adoption of one of the measures listed in Article 64(1) GDPR it has to "take utmost account" of the opinion. If it deviates from the opinion, another supervisory authority or the Commission may request the adoption of a binding decision. Article 64(1) GDPR includes 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, and the approval of binding corporate rules according to Article 47 GDPR.

[11] 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.

[12] According to Article 66(4) GDPR urgent opinions and decisions have to be adopted within two weeks by a simple majority.

Even though the Board is mainly based on cooperative action, certain elements such as the possibility to take a supervisory authority refusing to grant mutual assistance or refusing to let another supervisory authority join investigations before the Board or to invoke the urgency procedure where a supervisory authority fails to take action 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. However, these concerns may in practice well be outweighed by a coherent enforcement strategy of 28 Member States.

4 Power to Hear Individual Complaints

Individuals have the right to file a complaint with the supervisory authority, which is enshrined in EU primary law as a fundamental right in Article 8(1) and (3) CFR [cf. 11]. Correspondingly, the supervisory authorities under Article 28(4) DPD/Articles 77 and 52(1)(b) and (4) GDPR have the power to hear these complaints. These powers therefore are not merely an end in themselves, but rather serve to implement these individual rights.

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 [9]. 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 from the search results of an internet search engine, when the interest of the data subject outweighs the interest of the public to this information [10].

Further, the Court has ruled that when a claim 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 [9]. However, the territorial restriction of the rules it enforces according to Article 28(1) and (3) DPD still applies. Thus, a 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. This means that, generally, any supervisory authority may investigate the practice of controllers in 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 [9]. 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, i.e. the establishment's activities are inextricably linked to the activities of the main establishment.

Upcoming Changes. Under Article 77 GDPR, individuals may now choose the supervisory authority where they want to lodge their complaints: they may select the authority of their 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.[13]

Individuals may also challenge any legally binding decision of a supervisory authority addressing them, as they have the right to an effective judicial remedy according to Article 47 CFR. 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. This clarifies that the notion of independence of the supervisory authorities, as introduced above (2), only extends to the organisations it supervises. However, as the executive has thus only limited influence and control, this must be compensated by adequate judicial supervision.

If the supervisory authority competent under Articles 55 et seq 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. 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, data subjects under Article 80(1) GDPR have the right to mandate a non-profit organization active in the field of data protection to exercise them on their behalf. Taking this point even further, Article 80(2) GDPR contains an opening 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.

4.2 Complaints and 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 supervisory 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 [11]. 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.

[13] As laid down by Article 56(2) GDPR with regard to actions taken by the lead supervisory authorities, Article 60(7)-(9) GDPR concerning cooperation between supervisory authorities and Article 65(6) GDPR for decisions of the Board

The ECJ explicitly held that adequacy decisions of the Commission under Article 25(1) and (6) DPD do not curtail the power of the supervisory authorities to examine the actual level of protection in that third country.[14] The Commission decision does not prejudice the examination of an individual complaint put before the supervisory authority, which must assess these with due diligence [11]. 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 complaints 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) third indent 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.

The process for the adoption of adequacy decision is now set out in more detail in Article 45 GDPR: 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. Further, it must assess whether there are effective and enforceable data subject rights as well as effective administrative and judicial remedies for data subjects. The existence of an effective, independent supervisory authority is also required. With these provisions the legislator anticipated the requirements laid down by the Court in the *Schrems* judgment.

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. 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.

[14] 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.

It thus becomes clear, that in the view of the EU legislator as well as the judiciary, the entire EU data protection regime must be read in the light of the fundamental rights of the individuals it aims to protect. Therefore, the protection standard established within the EU may not be undermined by a transfer to a third country which does not provide at least a level of protection that is 'essentially equivalent' to these safeguards, as the Court put it in *Schrems* [11]. Furthermore, the ECJ has emphasised the crucial role of the supervisory authorities, which must act not only independently of their Member States, but also the Commission where it acts within the framework of the data protection law. The authorities may not defer to an assessment provided by Brussels, but must examine the merits of each complaint, especially where it concerns a violation of individual rights on a massive scale. Furthermore, the Court empowers individuals to use the instrument of complaints in order to enforce their rights in a meaningful way.

5 Outlook

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 thus 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.

The Court itself as well as the upcoming legislation emphasize the importance of lodging proceedings before the ECJ in order to ensure coherent interpretation. Yet, 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 before the Court. Under Article 267 TFEU only national courts of last instance are obliged to refer their questions on EU law to the ECJ. So far, national courts of lower instance have been reluctant to forward questions on EU law and there might be a considerable amount of proceedings which ended before they reached the court of last resort. Remarkably, the Court, twenty years after the coming into force of the DPD, has been concerned with fundamental questions such as the application of the DPD or the concept of the controller only in recent years.

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 reference 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 [23]. Furthermore, the supervisory authorities in these proceedings are dependent on the questions submitted by national courts, which enjoy discretion as to how to phrase them and which questions to put forward.

If binding decisions of the Board would, in practice, be brought before the Court this would allow the supervisory authorities to have a greater influence in the proceedings. However, such proceedings would also be adversarial in nature and thus might lead to conflicts between the supervisory authorities, which also depend on each other in order to properly enforce data protection law across the EU.

6 Conclusions

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 of engaging in the protection of the individual's rights and effectively counter interests and ambitions of multi-national companies processing personal data. Ideally, due to their complete independence, the supervisory authorities are also capable of discursive interaction with other State actors, especially in the executive. This is the justification for awarding a public authority far-reaching independence from the executive. Where the authorities do not live up to this vision, individuals can request them to engage on their behalf by submitting complaints and, if an authority is unwilling, take them to court. A strong judicial oversight in the conception of the Court is the key to ensuring that the supervisory authorities do not take their independence as a purpose of itself – they must use it in order to fulfil their advocacy role (cf. section 2).

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. This has two dimensions: the supervisory authorities must be outfitted with personnel competent to assess specific substantive issues of EU law and also to be able to engage in the actual communication with 27 other Member States, which requires considerable translation efforts (cf. section 3.2).

While the new means of cooperation offer great opportunities, it will have to be seen whether the Member States, for instance, will opt for an extra-territorial enforcement of data protection among the Member States in practice. Among the supervisory authorities at least, there will be much more interaction and dependence with the introduction of the Board, which provides a powerful tool in the form of the consistency mechanism that will have to be used carefully. The Board's modus operandi has to keep a balance between cooperative and adversarial action (cf. section 3.2).

The Court on the other hand has made it clear that it will not allow for a lowering of standards with regard of transfer to third countries in particular and the enforce-

ment of EU data protection law in general (cf. section 4). It has consistently strengthened the role of the authorities in its jurisprudence and in turn expects them to use their independence to fulfil their role as guardians of individual rights with regard to privacy and data protection. Furthermore, the ECJ has empowered individuals to ensure that their rights are properly enforced and thus added an additional measure of control.

References

1. Directive 95/46/EC of the European Parliament 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, OJ L 281 of 23 November 1995, 31-50, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML
2. 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
3. Rost, M.: Was meint eigentlich "Datenschutz"? Der Landkreis, 445-448 (2014)
4. Charter of Fundamental Rights of the European Union, OJ C 326 of 26 October 2012, 391-407, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
5. ECJ, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, ECLI:EU:C:2003:294
6. ECJ, Case C-518/07 *Commission v Germany*, EU:C:2010:125
7. ECJ, Case C-614/10 *Commission v Austria*, EU:C:2012:631
8. ECJ, Case C-288/12 *Commission v Hungary*, EU:C:2014:237
9. ECJ, Case C-230/14 *Weltimmo*, EU:C:2015:639
10. ECJ, Case C-131/12 *Google and Google Spain*, EU:C:2014:317
11. ECJ, Case C-362/14 *Schrems*, EU:C:2015:650
12. ECJ, Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, pending
13. Act No. 78-17 of January 1978 on Information Technology, Data Files and Civil Liberties, https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf
14. Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) vom 9. Februar 2000, https://datenschutzzentrum.de/gesetze/ldsg/
15. Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html
16. Article 29 Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, adopted on 16 December 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf

17. Revolidis, I.: The Long Arm of the European Data Protection Law. Zeitschrift für Datenschutz-aktuell, 04756 (2015)
18. Nwankwo, I. S.: Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság and the Concept of "Establishment" under Art. 4 (1)(a) Directive 95/46/EC, Zeitschrift für Datenschutz-aktuell, 04879 (2015)
19. Nguyen, A. M.: Die zukünftige Datenschutzaufsicht in Europa. Zeitschrift für Datenschutz, 265-270 (2015)
20. ECJ, Case Case 26-62 *van Gend en Loos*, ECLI:EU:C:1963:1
21. Kühling, J., Heberlein, J.: EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU. Neue Zeitschrift für Verwaltungsrecht, 7-12 (2016)
22. Jotzo, F.: Anmerkung. Juristenzeitung, 366-370 (2016)
23. Schwartmann, R.: Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Konsequenzen der Safe-Harbor-Entscheidung des EuGH. Europäische Zeitschrift für Wirtschaftsrecht, 864-868 (2015)
24. 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