Provisional text

OPINION OF ADVOCATE GENERAL
BOBEK
delivered on 13 January 2021(1)

Case C-645/19

Facebook Ireland Limited,
Facebook Inc.,
Facebook Belgium BVBA
v
Gegevensbeschermingsautoriteit

(Request for a preliminary ruling from the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium))

(Reference for a preliminary ruling – Protection of individuals with regard to the processing of personal data – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 47 – Regulation (EU) 2016/679 – Articles 55, 56, 58, 60, 61 and 66 – Supervisory authorities –Cross-border data processing – One-stop-shop – Lead supervisory authority – Supervisory authority concerned – Competence – Powers – Power to commence judicial proceedings)

I. Introduction

1. Does the General Data Protection Regulation (2) ('the GDPR') permit a supervisory authority of a Member State to bring proceedings before a court of that State for an alleged infringement of that regulation with respect to cross-border data processing, where that authority is *not the lead* supervisory authority with regard to that processing?

2. Or does the new 'one-stop-shop' mechanism, heralded as one of the major innovations brought about by the GDPR, prevent such a situation from happening? If a controller were called upon to defend itself against a legal challenge concerning cross-border data processing brought by a supervisory authority in a court outside the place of the controller's main establishment, would that be 'one-stop-too-many' and therefore incompatible with the new GDPR mechanism?

II. Legal framework

A. EU law

3. In the preamble of the GDPR, it is noted, inter alia, that: ‘the objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union [and] legal uncertainty’ (recital 9); a consistent and homogenous application of the data protection rules should be ensured throughout the Union (recital 10); the supervisory authorities should monitor the application of the rules and contribute to its consistent application, in order to protect natural persons and to facilitate the free flow of personal data within the internal market (recital 123); in situations involving cross-border processing ‘the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority’ and that authority has to ‘cooperate with the other authorities concerned’ (recital 124).

4. Pursuant to Article 51(1) of the GDPR, ‘each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (“supervisory authority”)’.

5. Under the terms of Article 55(1) of the GDPR, ‘each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State’.

6. Article 56 of the GDPR concerns the competence of the lead supervisory authority. The first paragraph of that provision states:

‘Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.’

7. Article 56(2) to (5) provides that, by derogation from paragraph 1, ‘each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State’. Those cases may be dealt with by the lead supervisory authorities, acting in accordance with the procedure set out in Article 60 of the GDPR or, ‘where the lead supervisory authority decides not to handle the case’, by the local supervisory authority, acting in accordance with Articles 61 and 62 of the GDPR.

8. Article 56(6) states that ‘the lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor’.

9. Article 58(5) of the GDPR, concerning the powers of the supervisory authorities, provides:

‘Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to initiate or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.’

10. Chapter VII of the GDPR, entitled ‘Cooperation and consistency’, includes Articles 60 to 76. Article 60, entitled ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, lays down the detailed procedure to be followed by the lead supervisory authorities when dealing with the cross-border processing of data.

11. In turn, Article 61(2) of the GDPR, concerning mutual assistance, requires each supervisory authority to take ‘all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request’. Article 61(8) of the GDPR states that where a supervisory authority fails to provide the requested information, the requesting

supervisory authority may adopt a provisional measure on the territory of its Member State, the urgent need to act under Article 66(1) being presumed.

12. Article 65(1)(a) of the GDPR, that article being entitled 'Dispute resolution by the Board', provides that, in order to ensure the correct and consistent application of the regulation in individual cases, the European Data Protection Board ('the Board') is to adopt a binding decision in, inter alia, the cases where a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or where the lead authority has rejected such an objection as being not relevant or reasoned.

13. Article 66(1), concerning the urgency procedure, provides that, in exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the coherence and consistency mechanisms, 'immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months'.

14. Chapter VIII of the GDPR, entitled 'Remedies, liability and penalties', includes Articles 77 to 84. Article 77(1) grants every data subject the right to lodge a complaint with a supervisory authority concerning possible infringements of the regulation vis-à-vis the processing of personal data relating to him or her, 'in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement'. Article 78(1) and (2) of the GDPR grants every natural or legal person the right to an effective judicial remedy against, inter alia, a legally binding decision of a supervisory authority concerning that person, and against a supervisory authority that does not handle a complaint.

B. National law

15. The Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data; 'the WVP'), as amended, transposed 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. (3) That law established, inter alia, the Belgian Privacy Commission. Under Article 32(3) of that law, 'without prejudice to the jurisdiction of the ordinary courts and tribunals for the application of general principles of privacy protection, the president of the [Privacy Commission] may submit to the court of first instance any dispute concerning the application of this law and its implementing measures'.

16. Pursuant to Article 3 of the Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (Law of 3 December 2017 establishing the Belgian Data Protection Authority; 'the DPA Law'), which entered into force on 25 May 2018, a Data Protection Authority ('the DPA') was established to succeed the Privacy Commission. In accordance with Article 6 of that law, the DPA 'has the power to bring any infringement of the fundamental principles of personal data protection, within the framework of this law and laws containing provisions on the protection of the processing of personal data, to the attention of the judicial authorities and, where appropriate, to take legal action to have these fundamental principles applied'.

17. The DPA Law did not include any specific provision with regard to legal proceedings initiated on the basis of Article 32(3) of the WVP, which were still pending on 25 May 2018.

18. The WVP was repealed by the Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Law of 30 July 2018 on the protection of individuals with regard to the processing of personal data). That law implements the provisions of the GDPR which require or allow Member States to adopt more detailed rules in addition to the common rules.

III. Facts, national proceedings and the questions referred

19. On 11 September 2015, the President of Belgium's Privacy Commission, which later became the DPA, commenced proceedings against Facebook Inc., Facebook Ireland Ltd and Facebook Belgium BVBA (collectively, 'Facebook') before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium). Those proceedings concern alleged infringements of data protection laws by Facebook, consisting, inter alia, of the unlawful collection and use of information on the private browsing behaviour of internet users in Belgium by means of technologies such as 'cookies', 'social plugins' and 'pixels'.

20. In essence, the DPA alleges that Facebook uses various technologies to 'monitor and track individuals when they browse from one website to another, and then uses the information collected to profile their browsing behaviour and, on that basis shows them targeted advertising, without properly informing the persons concerned or obtaining their valid consent. The DPA submits that Facebook carries out these practices regardless of whether or not the person concerned has signed up to Facebook's social network.

21. The DPA requested that Facebook be ordered to cease, with respect to any internet user established on the Belgian territory, to place, without their consent, cookies that remain active for two years on the devices used by those individuals when browsing a web page in the Facebook.com domain or the website of a third party, as well as to cease collecting data, in an excessive manner, by means of social plugins and pixels on third-party websites. In addition, it requested the destruction of all personal data obtained by means of cookies and social plugins relating to each internet user established on the Belgian territory.

22. By an interim order of 9 November 2015, the president of the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels) found that it had jurisdiction to hear the case and that the action was admissible with regard to all three defendants. That court also provisionally ordered the defendants to cease certain activities with regard to the internet users situated on the Belgian territory.

23. On 2 March 2016, Facebook filed a notice of appeal against that order with the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium). By judgment of 29 June 2016, that court amended the first-instance order. In particular, that court ruled that it had no jurisdiction with regard to the actions against Facebook Inc. and Facebook Ireland Ltd, whereas it does have jurisdiction in respect of the action brought against Facebook Belgium BVBA. The main proceedings thus became restricted to the actions against Facebook Belgium. That court also declared that there was no urgency.

24. I understand that at present, the case pending before the Hof van beroep te Brussel (Court of Appeal, Brussels) concerns the appeal against a subsequent decision on merits rendered by the first-instance court. Within the appellate proceedings, Facebook Belgium contends, inter alia, that since the new 'one-stop-shop' mechanism of the GDPR has become operational, the DPA lost competence to continue the main proceedings because it is not the lead supervisory authority. With regard to the cross-border processing at issue, the lead supervisory authority would be the Irish Data Protection Commission. The main establishment of the controller in the European Union is in Ireland (Facebook Ireland Ltd).

25. Against that background, the Hof van beroep te Brussel (Court of Appeal, Brussels) decided to stay proceedings and refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Should Articles [55(1)], 56 to 58 and 60 to 66 of the [GDPR], read in conjunction with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, be interpreted as meaning that a supervisory authority which, pursuant to national law adopted in implementation of Article [58(5)] of that regulation, has the power to commence legal proceedings before a court in its Member State against infringements of that regulation cannot exercise that power in connection with cross-border processing if it is not the lead supervisory authority for that cross-border processing?

(2) Does it make a difference if the controller of that cross-border processing does not have its main establishment in that Member State but does have another establishment there?

(3) Does it make a difference whether the national supervisory authority commences the legal proceedings against the controller's main establishment or against the establishment in its own Member State?

(4) Does it make a difference if the national supervisory authority had already commenced the legal proceedings before the date on which the regulation entered into force (25 May 2018)?

(5) If the first question is answered in the affirmative, does Article [58(5)] of the GDPR have direct effect, such that a national supervisory authority can rely on the aforementioned article to commence or continue legal proceedings against private parties even if Article [58(5)] of the GDPR has not been specifically transposed into the legislation of the Member States, notwithstanding the requirement to do so?

(6) If the previous questions are answered in the affirmative, could the outcome of such proceedings prevent the lead supervisory authority from reaching a conclusion to the contrary, in the event that the lead supervisory authority investigates the same or similar cross-border processing activities in accordance with the mechanism laid down in Articles 56 and 60 of the GDPR?'

26. Written observations have been submitted by Facebook, the DPA, the Belgian, Czech, Italian, Polish, Portuguese and Finnish Governments, as well as the European Commission. Facebook, the DPA and the Commission also presented oral argument at the hearing on 5 October 2020.

IV. Analysis

27. In a nutshell, the key issue that arose in the main proceedings is whether the DPA may continue legal proceedings against Facebook Belgium in respect of the cross-border processing of personal data that took place after the GDPR has become applicable, given that the data-processing entity is Facebook Ireland Ltd.

28. In order to address that issue, it is necessary to assess the scope and functioning of what the GDPR itself, in recital 127, refers to as the 'one-stop-shop' mechanism. That mechanism consists in a set of rules giving rise, in the case of cross-border data processing, to a central point of enforcement through a *lead supervisory authority* ('the LSA'), which sits within the system of cooperation and consistency procedures along with the *supervisory authorities concerned* ('the SACs'), designed to ensure the involvement of all interested supervisory authorities.

29. Pursuant to Article 56(1) of the GDPR, a supervisory authority acts as the LSA with regard to the cross-border processing carried out by controllers and processors that have their main establishment or the single establishment in its territory. Under Article 4(22) of the GDPR, a supervisory authority acts as the SAC if one of the following alternative conditions is satisfied: '(a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority'.

30. Before dealing with the substance of the questions referred, some preliminary remarks are called for (A). I shall then turn to the examination of the legal issues raised by the referring court. I shall focus, in particular, on the first question referred since that question is at the heart of the dispute before the referring court (B). Next, I shall deal with the other questions referred only briefly, given that if the answer to the first question is the one proposed in this Opinion, an answer to those other questions becomes either unnecessary or rather straightforward (C).

A. Preliminary remarks

31. At the outset, I note that there are certain elements of the main proceedings that I have difficulty in fully understanding.

32. First, I must admit that the relevance of the questions posed in the course of the main proceedings is not entirely obvious to me given the fact that, of the parties against which the DPA has taken action, it appears that only Facebook Belgium is still the defendant in the main proceedings. (4) It would appear from the file before this Court that that company is neither the 'main establishment' of the controller for the purposes of Article 4(16) of the GDPR, nor, since it appears to be an establishment of the same undertaking, a possible 'joint controller' within the meaning of Article 26 of the GDPR. (5)

33. However, questions that are referred for a preliminary ruling enjoy a presumption of relevance. As such, the Court refuses to give a ruling only in limited circumstances, in particular, where the requirements of Article 94 of the Rules of Procedure of the Court of Justice are not satisfied or where it is obvious that the interpretation of EU law concerned bears no relation to the facts, or where the questions are (entirely) hypothetical. (6) The present case is, in my view, not such a case. 'Who is who' and 'who may be pursued for what exactly' is not only a factual assessment which ultimately falls to the national court, but is also, in a way, one of the aspects of the questions referred to the Court.

34. Second, the temporal aspect of the main proceedings is also not entirely easy to grasp. The action was initiated while Directive 95/46 was in force. It has then been maintained when the GDPR entered into force. However, the proceedings now apparently concern only conduct taking place *after* the new legal framework has become applicable. There is indeed the issue of whether the continuation of the procedure by the DPA is in line with the provisions of the GDPR, an element raised by the fourth question. However, those questions would be relevant in the main proceedings only if a national authority sought to see ongoing proceedings to their completion with regard to alleged infringements pre-dating the moment when the new legal framework became applicable. If, however, the ongoing proceedings were at this point to concern only alleged unlawfulness arising after the date in which the GDPR has become applicable, possibly coupled with seeking the (necessarily prospective) judicial prohibition of such practices, it is not easy to understand why the DPA, in so far as it considers itself competent to intervene, did not terminate the current proceedings and did not proceed pursuant to the relevant provisions of the GDPR.

35. Third, at the hearing the DPA referred to an exchange it had with the Irish supervisory authority and the Board concerning one of the technologies used by Facebook to collect data (cookies). It has been stated that the two supervisory authorities disagreed on whether that technology actually fell within the scope *ratione materiae* of the GDPR.

36. In that connection, and as far as the present case is concerned, it may be worth pointing out that certain data processing activities may indeed fall within the material scope of more than one EU legislative instrument, in which case all of those instruments are, save where otherwise provided, applicable at the same time. (7) In other cases however, for example where the processing activities do not involve *personal* data within the meaning of Article 4(1) of the GDPR, the GDPR obviously does not apply.

37. Accordingly, where the alleged unlawfulness of some types of data processing stems from other provisions of (EU or national) law, the procedures and mechanisms set out in the GDPR do not come into play. The GDPR cannot be used as a gateway to bring into the 'one-stop-shop' mechanism forms of conduct that, although involving some data flows or even processing, do not fall foul of any of the obligations laid down therein.

38. In order to decide whether or not a case does in fact fall within the scope of the GDPR *ratione materiae*, a national court, including any referring court, ought to enquire about the *exact source of the legal obligation* incumbent on an economic operator that is said to have been infringed by the latter. If the source of that obligation is not the GDPR, then the procedures set out by that instrument, related to the substantive scope of that instrument, are logically not applicable either.

B. First question

39. By its first question, the referring court asks essentially whether the provisions of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter'), permit the supervisory authority of a Member State to bring proceedings before a court of that State for an alleged infringement of the GDPR with respect to cross-border data processing, even if that authority is not the 'lead supervisory authority'.

40. In that regard the DPA and the Belgian, Italian, Polish and Portuguese Governments suggest that the Court should answer in the affirmative, whereas Facebook, and the Czech and Finnish Governments, as well as the Commission take the opposite stance.

41. In the following section, I shall explain why I do not find convincing the interpretation of the GDPR proposed by the DPA and the Belgian, Italian, Polish and Portuguese Governments: both, a literal and systematic (1), as well as a teleological and historical (2) interpretation of the GDPR go clearly in the opposite direction. Moreover, neither a Charter-oriented interpretation of the regulation (3), nor alleged risks of possible under-enforcement of the GDPR (4) are such as to call into question what, in my view, is the proper interpretation of the GDPR, certainly not at present.

42. That said, the consequences from that particular reading of the regulation are, in my view, not as extreme as those suggested by Facebook, the Czech and Finnish Governments, and by the Commission. Accordingly, I shall explain why the answer to be given to the referring court should lie in the middle-ground between the two positions put forward in these proceedings: the supervisory authority of a Member State *is* entitled to bring proceedings before a court of that State for an alleged infringement of the GDPR with respect to cross-border data processing, despite not being the LSA, *provided* that it does so in the situations and according to the procedures set out in the GDPR (5).

1. A literal and systematic interpretation of the GDPR

43. In the first place, it seems to me that the wording of the relevant provisions, especially when read in their context, lends support to the interpretation of the GDPR according to which the LSA has a general competence over cross-border processing and, by implication, the SACs enjoy a limited power to act in that regard.

44. Article 56(1) of the GDPR states that 'the supervisory authority of the main establishment or of the single establishment of the controller or processor *shall be competent to act as lead supervisory authority for the cross-border processing* carried out by that controller or processor in accordance with the procedure provided in Article 60'. (8) According to Article 56(6) of the GDPR, 'the lead supervisory authority *shall be the sole interlocutor* of the controller or processor for the cross-border processing carried out by that controller or processor'. (9) Recital 124 echoes those provisions, essentially stating that, in the case of cross-border processing, 'the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor *should act as lead authority*'. (10)

45. The LSA's general competence over cross-border data processing is further confirmed by the fact that the situations in which the competence with regard to cross-border processing is given to other supervisory authorities are described as *exceptions* to the general rule. In particular, Article 55(2) of the GDPR excludes the competence of the LSA over certain data processing 'carried out by public authorities'. In addition, Article 56(2) of the GDPR states that, by derogation from the principle that the competence belongs to the LSA, 'each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'.

46. Furthermore, Article 66 of the GDPR, which concerns the 'urgency procedure', empowers each SAC 'in exceptional circumstances', where there is an urgent need to act in order to protect the rights and freedoms of data subjects, to immediately adopt provisional measures intended to produce legal effects on its own territory, with a specified period of validity which shall not exceed three months, 'by way of

derogation' from the cooperation and consistency mechanisms referred to in Articles 60, 63, 64 and 65 of the GDPR.

47. Therefore, it seems rather clear to me from the text of the GDPR that, vis-à-vis cross-border processing, the competence of the LSA is the rule, and the competence of other supervisory authorities is the exception. (11)

48. However, the DPA and certain governments contest that reading of the GDPR. In their view, the text of the relevant provisions suggests an (almost unfettered) right of any supervisory authority to initiate judicial proceedings against possible infringements which affect their territories, regardless of whether the processing is cross-border in nature. They rely mainly on two arguments.

49. In the first place, they argue that the expression 'without prejudice to Article 55', with which Article 56(1) begins, means that the competence given to the LSA by the latter provision cannot impinge or limit the powers attributed by the former provision to *each* supervisory authority, including that of initiating judicial proceedings.

50. I am not persuaded by this argument.

51. Article 55(1) lays down the principle that each supervisory authority 'shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State'. Those tasks are then listed in Article 57 of the GDPR. The powers are listed in Article 58 thereof. Among the tasks assigned is notably that of monitoring and enforcing the application of the GDPR (Article 57(1)(a)). Under Article 58, the supervisory authorities are granted various investigative (paragraph 1), corrective (paragraph 2), authorisation and advisory (paragraph 3) powers, as well as the power to engage in legal proceedings (paragraph 5).

52. In essence, those provisions – to which Article 55 impliedly refers – encompass *all* the tasks and powers conferred on supervisory authorities by virtue of the GDPR. If one were to follow the interpretation put forward by the DPA and certain governments, virtually nothing would be left for the general competence of the LSA, thereby depriving Article 56 of any meaning. The LSA would neither be the 'sole' interlocutor, nor would it 'lead' the other supervisory authorities in any way. Its role would, arguably, be reduced to that of an 'information point', without a clearly defined mission.

53. The importance of the role given to the LSA, and by implication of the one-stop-shop mechanism, becomes even clearer when those provisions are read together and in context.

54. The prominence given to Article 56 within the scheme of the GDPR is a first indication of this. Article 56 is the second provision appearing in the relevant section of the GDPR (Chapter VI, 'Independent supervisory authorities', Section 2, 'Competence, tasks and powers'), and comes immediately after the general provision on 'competence' and before the other general provisions on 'tasks' and 'powers'. Therefore, the EU legislature has decided to emphasise the centrality of the LSA's competence even before detailing the specific tasks and powers of *all* supervisory authorities.

55. More fundamentally, the significance of the LSA's role is also borne out by the provisions included in Chapter VII of the GDPR (entitled 'Cooperation and consistency'), which sets out the various procedures and mechanisms that supervisory authorities are to follow in order to ensure the consistent application of the GDPR. In particular, Article 60, which starts off the chapter and to which Article 56(1) refers, lays down the procedure of 'cooperation between the lead supervisory authority and the other supervisory authorities concerned'.

56. It is clear that that is meant to be *the* procedure to be followed when enforcement action against cross-border processing is necessary. That procedure, just like the other procedures provided for in Chapter VII of the GDPR, is not optional. The imperative terms included, particularly in Article 51(2) and

Article 63 of the GDPR, unequivocally indicate that supervisory authorities must cooperate and must do so through the (compulsory) use of the procedures and mechanisms established for that purpose.

57. Therefore, the expression 'without prejudice to Article 55', contained in Article 56(1), has a different meaning to that suggested by the DPA. In my view, that turn of phrase, in the context where it is placed, simply means that even if in an individual case, it is the LSA that is *competent* for that case involving cross-border processing pursuant to Article 56 of the GDPR, all supervisory authorities naturally retain the general *powers* assigned to them by virtue of Article 55 (and Article 58) of the GDPR.

58. Pursuant to Article 55(1) of the GDPR, Member States must enable the supervisory authority to carry out the tasks and exercise the powers provided for in the regulation. That provision thus assigns to any supervisory authority a general power (or competence) to act with regard to its territory, and that remains true regardless ('*without prejudice*') of whether the processing is cross-border in nature or not and, if the former, the authority in question acts as the LSA or the SAC. (12) Nevertheless, Article 55 of the GDPR does not govern the situations and manner in which that power to act will be exercised in an individual case. Indeed, those aspects are regulated by other provisions of the GDPR, especially those included in Chapter VII thereof. According to those provisions, whether a supervisory authority can exercise the general power to act, and the manner in which it does so, depends, inter alia, on whether, in respect of a given controller or processor, that authority is the LSA or the SAC. (13)

59. In this regard and as to the outcome, I therefore share the view of the Board which, in a recent Opinion, referred to Article 56(1) of the GDPR as an 'overriding rule' and as '*lex specialis*': that provision 'takes priority [over the general rule of Article 55 of the GDPR] whenever any processing situation arises that fulfils the conditions specified therein'. (14)

60. Accordingly, I believe that the DPA and certain governments misinterpret Article 55 and Article 56(1) of the GDPR. Those interveners take the first part of the sentence in Article 56(1) out of its context, in order to reverse the relationship between the rule and the exception. To do so results in watering down the prescriptive content of several provisions of the GDPR, and frustrates the objective, emphasised inter alia in recital 10 thereof, of ensuring a more consistent and homogenous application of the data protection rules. It would essentially amount to a return to the previous regime of Directive 95/46.

61. In the second place, the DPA and some governments contend that it follows from the very wording of Article 58(5) of the GDPR that *all* supervisory authorities must be able to start judicial proceedings against *any* potential infringement of the data protection rules affecting their territory, irrespective of the (local or cross-border) nature of the processing. The consequence is – in their view – that even if one were to interpret the one-stop-shop mechanism as limiting the powers of other supervisory authorities with regard to cross-border processing, those limits concern solely administrative action and not judicial proceedings.

62. This second argument too is, in my view, untenable. It falls into the same 'sin' of the previous argument: reading a specific provision of the GDPR in 'clinical isolation' from the rest of the regulation while, at the same time, reading too much into it.

63. Article 58(5) of the GDPR states: 'each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation'.

64. That provision requires Member States, on the one hand, to permit supervisory authorities to maintain close ties with judicial authorities (including potentially criminal authorities) and, on the other hand, to grant supervisory authorities (not only passive but also active) standing to bring proceedings before their national courts and tribunals. In other words, supervisory authorities should, in principle, be able to liaise with judicial authorities and, if necessary, start judicial proceedings. I understand that such an express provision was considered necessary by the EU legislature since, despite the text of Article 28(3) of

Directive 95/46, (15) significant differences between Member States' laws on this matter existed, which in turn created issues of under enforcement. (16) The present case, initiated while that directive was still in force, offers an example in point: the case raised, under national law, issues of standing of the Privacy Commission and of the appropriateness of the legal basis for the action brought by the President thereof.

65. However, similar to what was already stated above, (17) Article 58(5) of the GDPR sets out *powers* that are to be given to all supervisory authorities without exception at that stage, irrespective of (or before) the determination, in an individual case, of whether that authority would be the *competent* LSA, or the SAC or potentially not concerned at all. Article 58(5) of the GDPR does not regulate the situations and manner in which that power to bring proceedings is to be exercised. This is presumably also why that provision includes the terms 'where appropriate'. That is the object of other provisions of the GDPR.

66. In addition, neither the text nor the structure of Article 58 of the GDPR suggest that a distinction can be made – as the DPA contends – between the *administrative powers* of the authorities (which would be subject to the constraints stemming from the one-stop-shop mechanism) and the *power to bring judicial proceedings* (which would not be subject to those constraints). That provision lists, paragraph after paragraph, the various powers to be conferred on the supervisory authorities, grouping them according to purpose (investigative, corrective, advisory, and so on). The wording of those paragraphs is rather similar, stating, in essence, that *each* supervisory authority shall have the powers set out therein.

67. Therefore, I see no basis for interpreting paragraph 5 of Article 58 any differently from paragraphs 1 to 3 of the same provision. Of the two, only one can be true: either each and every supervisory authority enjoys all those powers unconstrained by the one-stop-shop mechanism, or all those powers have to be exercised according to the procedures and within the limits set out in the regulation.

68. For the reasons explained in points 51 and 52 above, the former hypothesis cannot be upheld. In fact, when Article 58 of the GDPR is read in its context, it becomes clear that, if anything, the opposite of what the DPA and some governments contend is actually true.

69. Indeed, each supervisory authority is to contribute to the correct and consistent application of the regulation. To that end, each supervisory authority – irrespective of its role as the LSA or as the SAC in a specific case – must, for example, examine the complaints lodged before it and do so with due diligence. (18) In fact, even where the alleged infringements concern cross-border processing and an authority is not the LSA, other supervisory authorities should be able to examine the matter in order to provide a meaningful input when called upon to do so within the framework of the cooperation and consistency mechanisms, (19) or to adopt urgent measures. However, it is then for the LSA to, generally, adopt binding decisions to enforce the GDPR vis-à-vis the processor or controller. (20) In particular, as it emerges from the recent judgment in *Facebook Ireland and Schrems*, it is for the '*competent* national supervisory authority … where relevant, to bring an action before the national courts'. (21) Therefore, the suggestion that supervisory authorities could disregard the consistency and cooperation mechanisms when they wish to bring proceedings cannot be reconciled with the text of the GDPR and the Court's case-law.

70. Furthermore, from a more practical perspective, it would be illogical to prevent an authority from opening an administrative procedure, in order to discuss the presumed breach of the data protection rules with the operators concerned, but to permit that same authority to immediately start legal proceedings in a court on the same matter. Litigation is often an instrument of last resort, to which an authority is likely to turn when an issue cannot be effectively dealt with through (formal or informal) discussions and decision making at the administrative level.

71. The distinction suggested by the DPA, which would *not allow* a supervisory authority to (*administratively*) investigate, prepare, process, and decide, but would *allow* it instead immediately to *bring judicial proceedings* before a court, comes dangerously close to turning administrative authorities into rather questionable Western characters, who shoot first, and (perhaps) talk later, if at all ('when you have to shoot, shoot; don't talk' (22)). I am not sure that that would be either a reasonable or an appropriate way for administrative authorities to deal with presumed infringements of data protection rules.

72. Furthermore, and more importantly, permitting supervisory authorities freely to go before their national courts, when they cannot use their administrative powers without going through the cooperation and consistency mechanisms set out in the regulation, would pave the way for an easy circumvention of those mechanisms. In particular, in the event of disagreement on a draft decision, both the LSA and (each of) the SACs could 'take the situation in their own hands' and start proceedings before national courts, thus bypassing the procedure provided for in Article 60(4) and Article 65 of the GDPR.

73. That would, in turn, also render meaningless one of the main functions of the Board – a body established by the GDPR – composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. (23) One of the Board's task is precisely that of monitoring and ensuring the correct application of the GDPR where disagreement between different supervisory authorities arises. (24) In those cases, the Board acts as a dispute settlement forum and decision-making body. Were the interpretation defended by the DPA and some governments to be followed, the mechanism set out in Article 65 of the GDPR could be entirely sidelined: each authority could go its own way, bypassing the Board.

74. The ensuing situation would appear to be the opposite of what the EU legislature intended to achieve with the new system, as will be explained in the next section.

2. A teleological and historical interpretation of the GDPR

75. As follows from recital 9 of the GDPR, the EU legislature considered that, whereas 'the objectives and principles of Directive 95/46/EC [remained] sound', that instrument had 'not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons'.

76. The need to ensure consistency thus became the 'name of the game' of the legal instrument destined to replace Directive 95/46. That objective was considered important from a dual perspective: on the one hand, to ensure an homogenous and high level of protection of natural persons, and on the other, to remove the obstacles to flows of personal data within the Union, providing legal certainty and transparency for economic operators. (25)

77. The latter aspect should be emphasised. Under Directive 95/46, economic operators active throughout the European Union were required to comply with the various sets of national rules implementing the directive, and to liaise, at the same time, with all the national data protection authorities. That situation was not only costly, burdensome and time-consuming for the economic operators, but also an inevitable source of uncertainty and conflicts for those operators and their customers. (26)

78. The limits of the system set up under Directive 95/46 also became evident in a number of judgments of the Court. In *Weltimmo*, the Court held that the powers of data protection authorities were strictly limited by the principle of territoriality: those authorities could act against breaches taking place only within their own territory, having in all other cases to ask the authorities of the other Member States to intervene. (27) In *Wirtschaftsakademie Schleswig-Holstein*, the Court ruled that, in the case of cross-border processing, each data protection authority could exercise its powers with respect to an entity established in its territory, independently of the views and actions of the data protection authority of the Member State where the entity responsible for that processing has its seat. (28)

79. However, in the virtual world of data processing, splitting the competence of the various authorities along territorial lines is often problematic. (29) In addition, the lack of clear mechanisms of coordination between the national authorities was a source of inconsistencies and uncertainty.

80. The introduction of the one-stop-shop mechanism, with the significant role given to the LSA and the cooperation mechanisms set up to involve other supervisory authorities, was thus meant to tackle those very problems. (30) In *Google (Territorial scope of de-referencing)*, the Court stressed the importance of the mechanisms of cooperation and consistency, for the correct and coherent application of the GDPR, and

their obligatory character. (31) More recently, in *Facebook Ireland and Schrems*, Advocate General Saugmandsgaard Øe equally emphasised that the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR are designed to avoid the risk that various supervisory authorities take different approaches with regard to cross-border processing. (32)

81. It is true that – as the DPA points out – during the legislative process, both the Council and the Parliament sought to limit the competence of the LSA, as originally envisaged by the Commission. However, the changes eventually introduced in the final text of the GDPR do not cast doubts over the interpretation of the regulation illustrated above, but rather confirm it.

82. According to the Commission's original proposal, the one-stop-shop mechanism implied that, in respect of cross-border processing, one single supervisory authority (the LSA) had to be responsible for monitoring the activities of the controller or the processor throughout the European Union and for taking the related decisions. (33) That proposal gave rise, however, to discussions within the Council and the Parliament.

83. The Council ultimately agreed on a text on the basis of a proposal tabled by the Presidency. (34) That proposal by no means called into question the one-stop-shop mechanism as such, which the Council referred to as being 'one of the central pillars' of the new legal framework. (35) The Presidency's proposal ultimately led to two sets of rather specific amendments.

84. First, the Council wished to introduce certain *exceptions* to the general competence of the LSA: with regard to the processing carried out by public authorities, and with regard to local situations. The Council thus proposed to introduce two provisions which did not feature in the Commission's Proposal, (36) and which are now Article 55(2) and Article 56(2) of the GDPR. (37)

85. Second, the Council intended to *mitigate* the role and competence of the LSA, by making the procedure more inclusive. The text of the Commission's Proposal was considered to be somewhat ambiguous on the point, and possibly giving rise to an exclusive competence of the LSA over cross-border data processing. A number of corrections were made to the text in order to enhance the 'proximity' between data subjects and the supervisory authorities. (38) Inter alia, the involvement of other supervisory authorities in the decision-making process was significantly increased.

86. For its part, the European Parliament also supported the creation of the one-stop-shop mechanism, with an enhanced role for the LSA, but proposed to strengthen the system of cooperation among the supervisory authorities. Both the Explanatory Statement to the Draft Report of the Parliament (39) and the European Parliament legislative resolution of 12 March 2014 (40) are rather clear in that regard.

87. In essence, with the Council's and the Parliament's intervention, the one-stop-shop mechanism, previously heavily leaning towards the LSA, was turned into a more balanced two-pillar mechanism: the leading role of the LSA with regard to cross-border processing is preserved, but it is now accompanied by an enhanced role for the other supervisory authorities which actively participate in the process through the cooperation and consistency mechanisms, with the Board given the role of referee and guide in the event of disagreement.

88. Therefore, a teleological and historical interpretation of the GDPR confirms the importance of the one-stop-shop mechanism and, as a consequence, the general competence of the LSA with regard to cross-border data processing. The interpretation of the provisions of the GDPR put forward by the DPA and certain governments cannot be reconciled with the intention of the EU legislature, as it can be inferred from the preamble and provisions of the regulation, as well as from the preparatory works.

89. I thus conclude that a textual, contextual, teleological, and historical approach to the interpretation of the relevant provisions of the GDPR confirm that supervisory authorities are bound to follow the rules on competence, and on the mechanisms and procedures of cooperation and consistency set out in the

regulation. When faced with cross-border processing, those authorities must act within the framework established by the GDPR.

90. However, the DPA and certain governments put forward two additional sets of arguments that, in their view, plead in favour of strengthening the powers of all supervisory authorities to act unilaterally, even in respect of cross-border processing. In the following sections, I will explain why those arguments should not call into question the interpretation of the GDPR that I have suggested above, certainly not at present.

3. A Charter-oriented interpretation of the GDPR

91. The DPA maintains the view that an unfettered power of supervisory authorities to bring proceedings against processors and controllers, including where the processing is cross-border in nature, is necessary to ensure compliance with Articles 7, 8 and 47 of the Charter. There seems to be two main concerns underpinning the DPA's arguments on this matter, although neither concern has been fully articulated in its observations. (41)

92. The *first* concern of the DPA seems to relate to the reduction in the number of authorities that can take action in respect of specific conduct. There appears to be a silent assumption in that proposition, namely that a high level of protection requires a multiplicity of authorities that may enforce compliance with the GDPR, even by acting in parallel. Put simply, the more authorities involved, the greater level of protection.

93. I do not think that this is necessarily be the case, at least as far as the level of protection is concerned.

94. It is true that, as the Court has stated, the EU legislation on data protection, read in the light of Articles 7 and 8 of the Charter, seeks to ensure a *high level* of protection of, inter alia, the fundamental right to respect for private life with regard to the processing of personal data. (42)

95. Nevertheless, the EU legislature has taken the view that, in order to ensure a '*high* level of protection of natural persons', a 'strong and *more coherent* data protection framework' is needed. (43) To that end, the framework established by the GDPR is intended to ensure consistency at all levels: for natural persons, for economic operators, for controllers and processors, and for supervisory authorities alike. (44) With regard to the latter, the GDPR seeks, as confirmed in recital 116, to promote '*closer* cooperation' among them. (45)

96. Consequently, unlike what was argued by the DPA, the pursuit of a *high* level of protection of the rights and freedoms of data subjects is – in the eyes of the EU legislature – fully in line with the operation of the one-stop-shop mechanism illustrated above. By permitting a more coherent, effective and transparent approach on the matter, the mechanisms of cooperation and consistency set out in the GDPR should contribute towards a stronger emphasis on the promotion and safeguarding of the rights enshrined, inter alia, in Articles 7 and 8 of the Charter.

97. Put differently, a coherent and uniform level of protection certainly does not preclude that protection from being placed at a high level. It is simply a question of where that uniform yardstick should be set. After all, it is doubtful that the coexistence of several unrelated, and possibly contradictory, actions by the supervisory authorities would truly further the aim of ensuring a *high* level of protection of individuals' rights. Consistency and clarity, ensured by the supervisory authorities acting in concert, could be said to better serve that aim.

98. The *second* concern expressed by the DPA raises issues of proximity between the individuals submitting a complaint and the authorities that will ultimately take action in response to that complaint. The question is, in substance, whether individuals can effectively bring proceedings against the action or inaction of the supervisory authorities vis-à-vis their complaints.

99. Indeed, Article 78 of the GDPR confirms the right of natural or legal persons to an effective judicial remedy against a supervisory authority. Moreover, in order to be consistent with Article 47 of the Charter, the remedies provided for in the GDPR cannot require data subjects to comply with detailed rules that, having regard to their status as natural persons, may disproportionately affect their right to a judicial remedy (for example, by increasing costs or delaying action). (46)

100. Yet, none of the (rather vague) arguments put forward by each party on this point clearly explains why the interpretation of the GDPR put forward by Facebook, the Czech and Finnish Governments and the Commission would clash with Article 47 of the Charter.

101. To begin with, the GDPR expressly provides for the right of data subjects to bring proceedings both against controllers and processors, and against supervisory authorities. In structural terms, therefore, it is not apparent why the GDPR would not comply with Article 47 of the Charter.

102. As regards the right of data subjects to bring proceedings *against controllers and processors*, they are given the choice to start proceedings before the courts of the Member States where the controller or processor has an establishment or where the data subjects reside. (47) This rule seems rather favourable to, or at least unproblematic for, data subjects. (48)

103. As far as the right of data subjects to start proceedings *against supervisory authorities* is concerned, the situation is more complex. To begin with, data subjects are given the right to challenge both the actions and the inaction of supervisory authorities. In particular, they can act against any supervisory authority that 'does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject'. (49)

104. However, actions against the supervisory authorities must, unlike in the case of actions against controllers and processors, be brought before the courts of the Member State where the supervisory authority is established. (50) Although this rule may appear to be less favourable to individuals, it must be borne in mind that, pursuant to Article 60(8) and (9) of the GDPR, where a complaint lodged by a data subject is wholly or partly rejected or dismissed, the relevant decision is adopted and notified to the data subject *by the supervisory authority with which he or she had lodged the complaint*. That is so regardless of whether or not that authority is the LSA, thereby permitting (where appropriate) the data subject to initiate proceedings in his or her own Member State.

105. These mechanisms of shifting the competence to adopt the decisions and, where necessary, of potentially adopting two-tier decisions (the LSA vis-à-vis the controller or processor, and the local authority vis-à-vis the complainant) seem specifically intended to avoid data subjects having to 'tour' the courtrooms of the European Union in order to bring proceedings against inactive supervisory authorities.

106. I acknowledge nonetheless that such a solution may lead to a number of practical questions. What will be the exact content of each of those decisions? Would that content be identical, (51) or different? Would a data subject be allowed to challenge all the issues that he or she believes to pertain to his or her case, even those that are effectively part of the decision of the LSA? Or would the decision of the supervisory authority with which the data subject lodged a complaint largely be an 'empty shell', simply dealing with the individual complaint in a formal manner, while the actual content is contained in the decision of the LSA? In that case, would the data subject, in order to have access to an indeed 'effective judicial remedy' within the meaning of Article 78 of the GDPR and Article 47 of the Charter, have to bring judicial proceedings before the courts of the Member State where the LSA is established in any case? How would the rules for access to an effective judicial remedy operate with regard to the review of any underlying decisions, be it at the *horizontal* level (amongst the supervisory authorities acting jointly) or the *vertical* level (as regards the review of an opinion or a decision of the Board in the consistency mechanism preceding and effectively likely determining the final decision of a supervisory authority)? (52)

107. There is no shortage of potential thorny issues. Practical experience might, one day, reveal genuine problems with the quality or even the level of legal protection inherent in the new system. However, at

present, any such issues remain at the level of conjecture. At this stage, and certainly in these proceedings, no elements have been submitted to the Court which point to any actual issues in that regard.

4. A possible under-enforcement of the GDPR

108. The DPA argues essentially that the enforcement of the GDPR in cross-border situations cannot be left almost solely to the LSA and to the data subjects that may be affected by the processing. It is the very role of each and every supervisory authority to act in order to protect the rights of individuals that may be affected by data processing. In particular, a supervisory authority cannot properly fulfil its mission if in every instance the decision of whether to take action against a suspected infringement, and the manner in which to do so, is left to the discretion of another authority.

109. In my view, this argument essentially represents a direct challenge to the new cooperation mechanism introduced by the GDPR. My answer in response to it is formulated in two layers: on the one hand, as far as the layer of the *extant law* is concerned, the GDPR could be said to contain mechanisms aimed at avoiding such scenarios. On the other hand, as far as the *genuine operation and effects* of the new systems are concerned, such fears are, at this stage, premature and hypothetical.

110. First, it ought to be clarified at the outset that the fact that a supervisory authority is not the LSA in respect of a given controller or processor by no means implies – as claimed by the DPA – that infringements of the GDPR which give rise to a criminal offence cannot properly be prosecuted. The power to 'bring infringements of this Regulation to the attention of the judicial authorities', set out in Article 58(5), obviously includes the power to liaise with criminal authorities such as the public prosecutor's office. That power is consistent with the supervisory authorities' task to monitor and enforce the application of the GDPR on their territory and does not impair the effective operation of the mechanisms of cooperation and consistency set out in Chapter VII of the GDPR. In that connection, it hardly needs to be pointed out that while those mechanisms are obligatory for the supervisory authorities, they *do not apply* to *other* Member States' authorities, in particular those charged with the task of prosecuting criminal offences.

111. Second and more importantly, when the system set up by the GDPR is observed in its entirety, it is rather clear that the LSA is not the sole enforcer of the GDPR in cross-border situations. The LSA is more of a *primus inter pares*. Generally, an LSA will only be able to act (administratively or judicially) with the consent of the SACs. Within the procedure laid down in Article 60 of the GDPR, the LSA is required to seek consensus. (53) It cannot ignore the views of the SACs. Not only is the LSA obliged to 'take due account' of those views, but any formal objection expressed by an SAC has the effect of temporarily blocking the adoption of the LSA's draft decision. Ultimately, any persistent divergence of views between the authorities is settled by a specific body (the Board) which is composed of the representatives of all EU supervisory authorities. Therefore, the LSA's position in that regard is no stronger than that of any other authority. (54)

112. As stated by the former European Data Protection Supervisor, Mr P. Hustinx, within the scheme of the GDPR, the role of an LSA 'should not be seen as an *exclusive* competence, but as a structured way of cooperating with other locally competent supervisory authorities'. (55) The GDPR provides for a shared responsibility to monitor the application of the GDPR and ensure its consistent application. To that end, the supervisory authorities are assigned tasks and endowed with certain powers; they are granted some rights but also burdened with some duties. Among those duties is, notably, the obligation to follow certain procedures and mechanisms designed to ensure consistency. An authority's wish to adopt a 'go-it-alone' approach (56) with regard to the (judicial) enforcement of the GDPR, without cooperating with the other authorities, cannot be reconciled with either the letter or the spirit of that regulation.

113. As mentioned in points 76 and 77 above, the GDPR is built on a delicate equilibrium between the need to ensure a high level of protection of natural persons and the need to remove the obstacles to flows of personal data within the Union. Those two objectives are, as evidenced in particular by recital 10 and Article 1(1) of the GDPR, inextricably linked. National supervisory authorities must therefore ensure a fair

balance between them, as the Court has consistently emphasised from its first judgments in the field of data protection. (57) Article 51(1) of the GDPR, in defining the supervisory authorities' mission, reflects that approach. (58)

114. Third, the GDPR not only provides mechanisms to sort out divergences with regard to the manner in which the enforcement is to be carried out, that is to say arbitrating on the conflicting views and opinions expressed by the supervisory authorities. It also includes mechanisms to overcome situations of administrative *inertia*. Those are, in particular, the situations in which an LSA – for lack of expertise and/or staff, or for whatever other reason – fails to take any meaningful action in order to investigate possible breaches of the GDPR and, where appropriate, enforce its rules.

115. As a matter of principle, the GDPR requires, in cases concerning cross-border processing, the LSA to act promptly. In particular, under Article 60(3) of the GDPR, an LSA must '*without delay*, communicate the relevant information on the matter to the other supervisory authorities concerned [and] *without delay* submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views'. (59)

116. Should an LSA fail to comply with that obligation, or more generally fail to act when required, one wonders whether there is any legal remedy for the SACs that are willing to proceed with an investigation and, possibly, enforcement actions? (60) I think there are at least two different routes that those authorities may follow, with those routes not being mutually exclusive.

117. On the one hand, under Article 61(1) and (2) of the GDPR, a supervisory authority may request another supervisory authority to provide 'information *and* mutual assistance in order to implement and apply [the GDPR]'. (61) That request may take the form of a request for information, including 'on the conduct of an investigation', or of other measures of assistance (such as the carrying out of inspections and investigations, or the putting in place of measures for effective cooperation). Any such request must be answered by the requested authority 'without undue delay and no later than one month after receiving the request'.

118. According to Article 61(5) and (8) of the GDPR, a failure to reply within the given time frame, or a refusal to comply with the request, enables the requesting authority to 'adopt a provisional measure on the territory of its Member State in accordance with Article 55(1)'. In such cases, 'the urgent need to act under Article 66(1) shall be *presumed* to be met and require an urgent binding decision from the Board pursuant to Article 66(2)'. (62)

119. It seems to me that that mechanism may also be used (and is probably meant to be used (63)) by an SAC vis-à-vis an LSA. A failure to act in a specific case of cross-border processing by the LSA, despite a request to that effect by an SAC, may thus enable the latter to adopt the urgent measures considered necessary to protect the interests of data subjects. Indeed, the existence of exceptional circumstances justifying the urgent need to act is presumed and need not be proven.

120. On the other hand, Article 64(2) of the GDPR allows any supervisory authority (or the Chair of the Board, or the Commission) to 'request that any matter of general application *or producing effects in more than one Member State* be examined by the Board with a view to obtaining an opinion, *in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 …*'. (64)

121. It is not entirely clear whether the Board's decision would be *legally* binding upon the LSA concerned. (65) However, according to Article 65(1)(c) of the GDPR, where a competent supervisory authority does not follow the opinion of the Board issued under Article 64, any SAC (or the Commission) may communicate the matter to the Board and thus initiate the dispute resolution procedure provided to that end. The latter procedure would, eventually, produce a binding decision. (66)

122. Having said that, it must be acknowledged that the two mechanisms illustrated above (Articles 61 and 66 of the GDPR on the one hand, and Articles 64 and 65 of the GDPR on the other hand), are somewhat cumbersome. Their actual functioning is not always crystal clear. Therefore, if on paper the abovementioned provisions seem apt to avoid those problems, only the future application of those provisions will tell whether, in practice, those provisions may turn out to be 'paper tigers'.

123. This brings me back to the second layer of the argument advanced in connection with under-enforcement, and its rather hypothetical and unsubstantiated nature, certainly at present. I must admit that, in my view, if the dangers concerning under-enforcement of the GDPR suggested by the DPA and some other interveners were to materialise, the entire system would be ripe for a major revision.

124. From a structural point of view, that could indeed be the case if the new structure were to lead to regulatory 'nests' for certain operators who, after having effectively chosen their national regulator themselves by accordingly placing their main establishment within the Union, rather than being monitored, they would in fact be shielded from other regulators by a specific LSA. Few would disagree that regulatory competition in the form of a race to the bottom amongst the Member States would be just as unhealthy and dangerous as regulatory inconsistency – the type of lack of coordination and consistency which was characteristic of the previous design. Network regulatory regimes might be able to prevent inconsistency and divergence by fostering consensus and cooperation. Yet, the price for consensus tends to be to block the active authorities, especially in a system where enhanced concertation is required in order to reach any decision. Within such systems, collective responsibility may lead to collective irresponsibility and, ultimately, inertia.

125. However, with regard to any such dangers, the legal framework set up by the GDPR is still in its infancy. It is not easy to predict – especially for a court, in the context of a single, or indeed rather singular, procedure – how the mechanisms set up by that regulation will work in practice, and how effective they will be. Within such a framework, similar to the potential issues under relating to the protection of fundamental rights and the Charter-conform interpretation, (67) caution is advised.

126. In my view, it would be a bad idea for the Court to significantly alter that framework – which is the (delicate and carefully crafted) product of a lengthy and intense legislative process – by way of interpretation of individual sentences taken out of their context and, at this point, based on assumptions and speculation. That is all the more so if the interpretation proposed by some parties is simply that of essentially reading out from the regulation some key parts and thereby, de facto, returning to the old system under Directive 95/46, which, as regards its institutional dimension, has been expressly and clearly discarded by the EU legislature.

127. That abundantly clear legislative design, as evidenced, as it follows from the previous sections of this Opinion, both in the text and structure of the GDPR, as well as in the documented legislative intent, also provides an answer to other potential structural concerns, such as those relating to the proper balance between public and private enforcement of the data protection rules and the GDPR. Does it make sense to limit *public* enforcement to one single authority and hence to one single Member State, the implementation of which will come about only after a lengthy and cumbersome administrative procedure, whereas *private* enforcement of the same rules is likely to happen faster in practice and before the (civil) courts of all the Member States? Should national supervisory authorities have less access to courts than an individual private consumer? Will most of the data protection cases not end up in national courts (and possibly before the Court of Justice by way of a preliminary ruling) brought directly by private litigants, completely bypassing national regulators established for that purpose, because those national regulators are still in the process of cooperating and coordinating their positions? Within such a regime, is there not a danger that private enforcement will entirely supersede the public one?

128. Be that as it may, the EU legislature made a clear institutional and structural choice and there is, to my mind, no doubt about what it intended to achieve. Under such circumstances, metaphorically speaking, one should give the infant the benefit of doubt, at least for the time being. If, however, that child would turn out bad – which fact would have to be evidenced by facts and robust arguments – then I do not believe that the

Court would turn a blind eye to any gap which might thereby emerge in the protection of fundamental rights guaranteed by the Charter and their effective enforcement by the competent regulators. Whether that would then still be an issue for a Charter-conform interpretation of provisions of secondary law, or an issue of validity of the relevant provisions, or even sections of a secondary law instrument, is a question for another case.

5. Interim conclusion

129. All the outlined elements of interpretation thus point to one and the same outcome: the LSA has a general competence over cross-border processing. All supervisory authorities (irrespective of their role as LSA or as SAC) are to act, especially in the case of cross-border processing, according to the procedures and mechanisms set out in the GDPR.

130. That said, does it follow that a supervisory authority which is not the LSA is always precluded, as a matter of principle, from acting before the domestic courts against a controller or processor when the processing is cross-border in nature?

131. No, it does not.

132. First, supervisory authorities may naturally go before a national court when they act outside the material scope of the GDPR, provided that that is allowed under national law and not precluded by EU law, for instance because the processing does not involve personal data or because the processing of personal data is carried out in the context of the activities referred to in Article 2(2) of the GDPR. (68)

133. Second, despite the cross-border nature of the processing, in situations set out in Article 55(2) of the GDPR (processing carried out by public authorities, but also any processing carried out in the public interest or in the exercise of official authority), the regulatory competence remains vested in local supervisory authority, which naturally also includes, if the need arises, the ability to bring judicial proceedings before a court.

134. Third, there are cases where, despite there being cross-border processing of personal data that falls within the scope of the GDPR, no supervisory authority is to act as LSA. Since the cooperation and consistency mechanism set out in the GDPR only applies to controllers with one or more establishments in the European Union, there is no LSA with regard to cross-border processing by controllers that have no establishment in the European Union. This means that controllers without any establishment in the Union must deal with local supervisory authorities in every Member State they are active in. (69)

135. Fourth, any supervisory authority may adopt urgent measures where the appropriate conditions are fulfilled. There are, furthermore, situations in which the urgency of the measures is presumed. That may be so, for example, in cases where an SAC is potentially faced with persistent inertia from the LSA in charge. Since Article 66(1) of the GDPR provides for a wholesale setting aside of the consistency mechanism, it is fair to assume that in such an exceptional situation, the entire range of powers vested in a supervisory authority (which under normal circumstances is not to be exercised because it is blocked by the special rules on the competence of an LSA for cross-border processing) is revived and may be temporarily exercised. This, therefore, naturally includes the power to commence legal proceedings pursuant to Article 58(5) of the GDPR.

136. Finally, fifth, for the sake of completeness, it may be pointed out that it is also possible that a supervisory authority which notified the LSA may also gain (or rather retain) the power to go to court in a case where the LSA ‘decides not to handle the case’ pursuant to Article 56(5) of the GDPR. On the face of it, the latter provision might very well accommodate an actual agreement between both supervisory authorities on which of them is better placed to handle the case.

137. In sum, the provisions on the GDPR do not include any *general bar* for other supervisory authorities, especially SACs, to start proceedings against potential infringements of data protection rules. On the

contrary, various situations in which they are empowered to do so are expressly envisaged in the GDPR, or follow impliedly from it. (70)

138. In general, however, it is of the utmost importance that, where the procedures and mechanisms provided for in the GDRP (especially those found in Chapters VI and VII thereof) apply, both the LSA and the SACs duly follow them. The rules of the GDPR are very clear in that none of those authorities must act outside, or in disregard, of that legal framework.

139. That said, whether or not the DPA has complied with those procedures and mechanisms in the case at hand – an issue which gave rise to some debate at the hearing, but remains somewhat blurry in view of the peculiar procedural background of the present case (71) – is, however, for the referring court to check.

140. Accordingly, the answer to the first question should be that the provisions of the GDPR *permit* the supervisory authority of a Member State to bring proceedings before a court of that State for an alleged infringement of the GDPR with respect to cross-border data processing, despite not being the LSA, *provided* that it does so in the situations and according to the procedures set out in the GDPR.

C. The other questions referred

1. Second question

141. By its second question, the referring court inquires as to whether the answer to the first question would be different if the controller of that cross-border processing does not have its main establishment in that Member State but it does have another establishment there.

142. In the light of the answer proposed for the first question, the answer to be given to the second question is rather clear: in principle, *no*, provided that the 'main establishment' in the sense of Article 4(16) of the GDPR is indeed located in another Member State.

143. The fact that a controller has a *secondary* establishment in a Member State, in principle, does not affect the local supervisory authority's capacity to start judicial proceedings, in accordance with Article 58(5) of the GDPR, in relation to a given cross-border processing situation. In other words, in the case of cross-border data processing, the scope of the powers granted to a supervisory authority and the manner in which those powers should be exercised do not generally depend on whether the controller or processor, which has its main establishment in another Member State, *also* has an establishment in the Member State of that authority.

144. However, similar to what has already been stated above, (72) as a preliminary element to that conclusion, a national court needs first to ascertain which establishment is in fact the main establishment *for the purposes of a given processing operation*. In that regard, Article 4(16)(a) of the GDPR embraces a dynamic understanding (73) of what is considered to be the main establishment, which need not necessarily coincide with the static corporate structure of an undertaking.

145. Furthermore, the fact that the controller or processor has a (secondary) establishment in the territory of the supervisory authority means that that authority is an SAC within the meaning of Article 4(22) of the GDPR. SACs are given significant powers in the context of the procedures laid down in Chapter VII of the GDPR. (74)

146. In addition, Article 56(2) of the GDPR provides for an exception to the general competence of the LSA as regards cross-border processing: 'each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of [the GDPR], if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'. That competence must, in turn, be exercised in conformity with the procedure set out in paragraphs 3 to 5 of the same provision. (75)

2. Third question

147. By its third question, the referring court inquires as to whether the answer to the first question would be different if the national supervisory authority commences the legal proceedings against the controller's main establishment or against the establishment situated in its own Member State.

148. In the light of the answer proposed to the first question, and as far as the third question does not in fact overlap with the second question, the third question also calls for a negative answer.

149. Again, provided that it has indeed been clarified on the facts of a case that the main establishment for a given processing operation pursuant to Article 4(16) of the GDPR is actually located in another Member State, the national supervisory authority of the Member State in which an establishment of the controller is located is not the LSA, but might become an SAC. Within that assessment, however, the supervisory authority's competence to act does not depend on whether the legal proceedings are brought against the controller's main establishment or against the establishment in its own Member State. (76)

150. For the sake of completeness, it might be added that Article 58(5) of the GDPR is formulated in a broad manner and does not specify the entities against which the supervisory authorities should or could act. That led to an intriguing discussion in the submissions of some of the parties on an issue which, in my view, although not unimportant, does not need to be addressed by the Court in the present case. The issue is: whether supervisory authorities, provided that they are indeed competent to do so under the rules of the GDPR, may take action only against the controller's or processor's establishment(s) located in their territory, or whether they may also take action *against establishments located abroad*?

151. On the one hand, the Belgian, Italian and Polish Governments stress that Article 55(1) of the GDPR limits the territorial competence of each supervisory authority to its territory. They deduce from that that the supervisory authorities can only act against local establishments.

152. Nevertheless, the text is in my view not that clear: it refers to exercising the powers conferred by the regulation 'on the territory of its own Member State'. I do not read that provision as necessarily precluding an action against an establishment located in another Member State. The territorial element included in Article 55(1) of the GDPR, read in the light of the overall scope of the GDPR in its Article 1(1) and Article 3 thereof, triggering the competence of a supervisory authority in a given case, relates to *the effects of the data processing* on the territory of a Member State. That element does not operate as a limit to actions against controllers or processors based outside the national boundaries.

153. On the other hand, the DPA suggests that each authority has the power to act against all infringements of the GDPR taking place in its territory, regardless of whether the controller or processor has an establishment in its territory. That means that an authority should also be able to start proceedings against establishments located abroad. In that connection, the DPA refers to the judgment of the Court in *Wirtschaftsakademie Schleswig-Holstein*. (77) *In that decision, the Court found that* Articles 4 and 28 of Directive 95/46 permitted the supervisory authority of a Member State to exercise the power to engage in legal proceedings with respect to an establishment of that undertaking situated in the territory of that Member State. That was the case even if that establishment was responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State, while exclusive responsibility for collecting and processing personal data belonged, for the entire territory of the Union, to an establishment situated in another Member State.

154. The DPA is correct in arguing that, in so far as the GDPR includes, on this matter, provisions similar to those of Directive 95/46, (78) the principles established by the Court in *Wirtschaftsakademie Schleswig-Holstein should*, *mutatis mutandis*, also be valid with regard to the GDPR. However, that judgment only explained when a local establishment can be sued by the authority, despite the (main part of the) processing being carried out by an establishment located elsewhere in the European Union. That judgment, at least expressly, neither confirmed nor excluded that the supervisory authority could also act against the latter establishment.

155. Nevertheless, it seems to me that the new one-stop-shop mechanism, by creating a central point of enforcement, necessarily implies that a supervisory authority can also act against establishments located abroad. I am not sure the new system could work properly if it were to preclude the possibility that the authorities, and in particular the LSA, could take action against establishments located elsewhere. (79)

3. Fourth question

156. By its fourth question, the referring court asks whether the answer to the first question would be different if the national supervisory authority had already initiated the legal proceedings before the date on which the GDPR entered into force.

157. At the outset, it must be pointed out that, in the GDPR, there are no transitional rules or other rules which govern the status of judicial proceedings pending at the time the new framework enters into force.

158. In the light of above, the answer to the question should be, in my view, 'it depends'.

159. On the one hand, as regards infringements by controllers or processors of the data protection rules that took place *prior* to the date in which the GDPR became applicable, I believe that those proceedings may continue. I cannot see any good reason to force the authorities to terminate enforcement actions which relate to *past conduct* that was (allegedly) unlawful when committed, and against which they were (at the time) competent to take action. A different solution would lead to a sort of amnesty with regard to certain breaches of data protection laws.

160. On the other hand, a different situation arises with regard to actions initiated against breaches that have not yet materialised, since they occur *after* the date in which the GDPR became applicable. (80) In that regard, as in any other situation of new rules being applicable to situations arising under the new legal regime, the new substantive rules will only be applicable to facts occurring after the new instrument has become applicable. (81)

161. It is for the referring court to ascertain which of the two scenarios in fact reflects the current state of the main proceedings. (82) In the case of the first scenario, I would suggest that the ongoing proceedings may be continued, certainly from the point of view of EU law, provided that they are limited to a possible finding of past infringements. In the case of the second scenario, the national proceedings ought to be discontinued. Indeed, the new framework set up a different system of competences and powers, with the consequence being that an SAC cannot take action against infringements stemming from cross-border processing outside the specific situations, and unless following the procedures and mechanisms, provided to that end.

162. The opposite solution would imply a de facto prorogation of the system established by Directive 95/46, despite the fact that both EU and national law have expressly repealed and replaced it with a new one. After all, if the DPA were indeed to obtain an injunction barring Facebook from adopting in the future (and, by the way, for how long?) the practices at issue in the main proceedings, would that not interfere with the competence over (the same) conduct that the GDPR gave, as from 25 May 2018, to the LSA and the SACs, potentially coupled with conflicting decisions (or judicial orders) emerging from different Member States?

4. Fifth question

163. By its fifth question – posed in the event that the first question is answered in the affirmative – the referring court seeks to clarify whether Article 58(5) of the GDPR has direct effect, such that a national supervisory authority can rely on it in order to commence or continue legal proceedings against private parties, even if that provision has not been specifically transposed into national law.

164. To reiterate, Article 58(5) reads: 'Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial

authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.'

165. Facebook, and the Czech and Portuguese Governments point out that that provision clearly requires Member States to do something: to put in place provisions enabling the authorities to bring proceedings. To be fully operational, the power to bring proceedings may also require some national rules to determine, inter alia, the courts having jurisdiction, the conditions for initiating an action, and the procedures to be followed.

166. In view of my proposed answer to the first question, there is indeed no need to answer the fifth one. However, for the sake of completeness, for my part, I see no problem in agreeing with the DPA that the prescriptive content of that particular EU law provision is rather unequivocal and self-executing. In that regard, it must be borne in mind that, generally, an EU law provision has direct effect whenever, as far as its subject matter is concerned, it is sufficiently clear, precise and unconditional to be relied on against a conflicting national measure, or in so far as the provision defines rights which individuals are able to assert against the State. (83)

167. Quite apart from the fact that the provision is included in a regulation (an instrument that, under Article 288 TFEU is 'binding in its entirety and directly applicable in all Member States' (84)), it seems to me that a specific and immediately applicable rule can indeed be extracted from Article 58(5) of the GDPR. That rule is very simple: supervisory authorities must have standing before national courts, they are given the capacity to start judicial proceedings in national law. The action brought before a national court cannot be declared inadmissible for lack of legal personality.

168. Whilst I agree with Facebook and the Czech and Portuguese Governments that Member States may provide for special rules, conditions, or jurisdiction for actions brought by supervisory authorities, such rules are by no means necessary for the directly effective rule under Article 58(5) of the GDPR to operate. Failing any ad hoc rules introduced by the national legislature, the *default* rules in the appropriate national procedural codes (be it codes of administrative justice or even by default codes of civil procedure) will naturally be applicable to any actions initiated by the supervisory authorities. Thus, for example, if there were no specific implementing rules on jurisdiction, it is safe to assume that the general default rule likely to be found in any code of (civil) procedure, whereby the default court is the court of the place of establishment of the defendant unless provided otherwise, would be applicable.

5. Sixth question

169. By its sixth and final question, the referring court asks if, in the case where the national supervisory authority is empowered to take action, the outcome of such proceedings prevent the lead supervisory authority from reaching a conclusion to the contrary, in the event that the lead supervisory authority investigates the same or similar cross-border processing activities in accordance with the mechanism laid down in Articles 56 and 60 of the GDPR.

170. In the light of the answer proposed to the first question, this question need not be answered.

171. However, the issue raised by this question shows once again why the first question should be answered as proposed above. If the compulsory nature of the consistency and cooperation mechanisms set out in the GDPR were to be eliminated, thereby making the one-stop-shop mechanism 'optional', or in reality rather non-existent, the coherence of the whole system would be severely affected. Rules on competence currently contained in the GDPR would, in essence, be replaced by a parallel 'race-to-the-first-judgment' by all supervisory authorities. In the end, whoever is 'first past the post' of a final judgment within their jurisdiction would then become the effective LSA for the rest of the European Union, as implied by the sixth question.

V. Conclusions

172. I propose that the Court answer the questions referred for a preliminary ruling by the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium) as follows:

– The provisions of 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) permit the supervisory authority of a Member State to bring proceedings before a court of that State for an alleged infringement of that regulation with respect to cross-border data processing, despite not being the lead supervisory authority, provided that it does so in the situations and according to the procedures set out in the same regulation;

– The General Data Protection Regulation precludes a supervisory authority from continuing legal proceedings started before the date in which it has become applicable, but which concerns conduct that occurs after that date;

– Article 58(5) of the General Data Protection Regulation has direct effect, to the extent that a national supervisory authority can rely on it in order to commence or continue legal proceedings before national courts, even if that provision has not been specifically transposed into national law.

---

1 Original language: English.

---

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 2016 L 119, p. 1).

---

3 OJ 1995 L 281, p. 31.

---

4 For the reasons set out above, see point 23 of this Opinion.

---

5 In that regard, the Court has consistently stated that, under Directive 95/46, the concept of ‘controller’ had to be construed broadly – see, for example, the recent judgments of 29 July 2019, *Fashion ID* (C−40/17, EU:C:2019:629, paragraphs 65, 66 and 70), and of 10 July 2018, *Jehovan todistajat* (C−25/17, EU:C:2018:551, paragraph 66). I see no reason why the same should not equally be true with regard to the GDPR.

---

6 See, for example, judgment of 25 July 2018, *Confédération paysanne and Others* (C−528/16, EU:C:2018:583, paragraphs 72 and 73 and the case-law cited), or of 1 October 2019, *Blaise and Others* (C−616/17, EU:C:2019:800, paragraph 35).

---

7 For example, in my Opinion in *Fashion ID*, I have explained the reasons for which both the rules of then in force Directive 95/46 and of the so-called ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37)) could be potentially applicable in a case involving the placement of cookies (C−40/17, EU:C:2018:1039, points 111 to 115). On this matter, more generally, see European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, of 12 March 2019. See also Article 29 of the Data Protection Working Party, Document 02/2013 providing guidance on obtaining consent for cookies, 1676/13/EN WP 208, of 2 October 2013.

---

8 My emphasis.

9 My emphasis.

10 My emphasis.

11 In legal scholarship, see Bensoussan, A. (ed.), *Règlement européen sur la protection des données – Textes, commentaires et orientations pratiques*, 2nd ed., Bruylant, Bruxelles, 2017, p. 363.

12 Similarly, Hijmans, H., 'Comment to Article 56 of the GDPR', in Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, Oxford, 2020, p. 921.

13 By an analogy with general administrative law (or codes of judicial procedure), a body might have the (general) *power* to act in certain ways, but may not necessarily have the *competence* (*rationae materiae, personae, temporis, loci …*) to exercise that power and to decide on an individual case. Thus, for example, the fact that a criminal court has the power to give judgment in criminal proceedings does not necessarily mean that it will also be competent to do so in the case of a given crime committed by a specific person (as that might fall within the jurisdiction of a different court).

14 European Data Protection Board, Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment, of 9 July 2019, points 19 and 20.

15 That provision, in the relevant part, read: 'each authority shall in particular be endowed with … the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities'.

16 See European Commission, First report on the implementation of the Data Protection Directive (95/46/EC) of 15 May 2003, COM(2003) 265 final, pp. 12 and 13, and its Annex 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States', p. 40. See also European Union Agency for Fundamental Rights, Access to data protection remedies in EU Member States – Report, 2012, especially pp. 20 to 22.

17 See above, points 51, 57 and 58 of this Opinion.

18 Judgments of 6 October 2015, *Schrems* (C−362/14, EU:C:2015:650, paragraph 63), and of 16 July 2020, *Facebook Ireland and Schrems* (C−311/18, EU:C:2020:559, paragraph 109).

19 In some cases, an SAC is entitled (and thus should be able to) submit to the LSA a draft for a decision: see Article 56(2) to (4) of the GDPR.

20 See, to that effect, recital 125 of the GDPR.

21 Judgment of 16 July 2020 (C−311/18, EU:C:2020:559, paragraph 120) (my emphasis). Similarly, making it clear that it is for the *competent* supervisory authority to react to an infringement of the GDPR and to choose the most appropriate means to do that, see Opinion of Advocate General Saugmandsgaard Øe in *Facebook Ireland and Schrems* (C−311/18, EU:C:2019:1145, points 147 and 148). Compare those statements with the judgment of 6 October 2015, *Schrems* (C−362/14, EU:C:2015:650, paragraph 65) in which the Court stated that, under Directive 95/46, (any) national supervisory authority had to be able to engage in legal proceedings.

---

22 As the famous line in '*The Good, the Bad and the Ugly*' had it (A 1966 film directed by Sergio Leone, starring Clint Eastwood, Lee Van Cleef and Eli Wallach, produced by Produzioni Europee Associate and United Artists).

---

23 Article 68 of the GDPR.

---

24 See, in particular, Article 70(1)(a) of the GDPR.

---

25 See the Explanatory Memorandum to the Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. See also recitals 10, 13 and 123 of the GDPR.

---

26 On this issue, see generally Giurgiu, A. and Larsen, T., 'Roles and Powers of National Data Protection Authorities – Moving from Directive 95/46/EC to the GDPR: Stronger and More "European" DPAs as Guardians of Consistency?' *European Data Protection Law Review*, 2016, pp. 342-352, at 349; and Voigt, P., von dem Bussche, A., *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Springer, 2017, pp. 190-192.

---

27 Judgment of 1 October 2015 (C−230/14, EU:C:2015:639, paragraphs 42 to 60).

---

28 Judgment of 5 June 2018 (C−210/16, EU:C:2018:388, paragraphs 65 to 74).

---

29 See, for example, Miglio, A., 'The Competence of Supervisory Authorities and the One-stop-shop Mechanism', in EU Law Live – Weekend edition, No. 28, 2020, pp. 10 to 14, at 11.

---

30 See Opinion of Advocate General Bot in *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2017:796, point 103).

---

31 Judgment of 24 September 2019 (C−507/17, EU:C:2019:772, paragraph 68).

---

32 C−311/18, EU:C:2019:1145, point 155.

---

33 See recitals 97 and 98 of the Commission's Proposal (see above footnote 25).

---

34 See Council documents 15656/1/14 REV 1, of 28 November 2014, and 16526/14, of 4 and 5 December 2014, pp. 2, 8 and 9.

35 Ibid., p. 1.

36 See Council Document 5419/1/16 REV 1 of 8 April 2016, pp. 203 to 205.

37 See above, point 45 of this Opinion.

38 Council document 15656/1/14 REV 1, of 28 November 2014, p. 2.

39 See Document A7-0402/2013 of 22 November 2013, which referred to the one-stop-shop mechanism as a 'huge step towards a coherent application of data protection legislation across the EU'.

40 Document EP-PE_TC1-COD(2012)0011 of 12 March 2014 (see especially amendments 148, 149, 158, 159 and 167).

41 In a similar vein, I simply assume that those Charter provisions and rights invoked are those of the data subjects, which a supervisory authority is called on to protect, not that a supervisory authority itself would be the bearer of those rights. The idea that administrative authorities, that is to say, emanations of State, would be endowed with fundamental (human) rights on which they could rely against the State (or rather against each other or, in cases of horizontal direct effect, even against individuals) is indeed rather singular. To my mind, the answer should be clearly in the negative, but I acknowledge that there different approaches exist in the Member States. Be that as it may, in the context of the present case, that issue can be safely left unexplored.

42 See, to that effect, judgment of 6 October 2015, *Schrems* (C−362/14, EU:C:2015:650, paragraph 39).

43 See recitals 7, 9 and 10 of the GDPR (my emphasis).

44 See, to that effect, recitals 10, 11 and 13 of the GDPR

45 My emphasis.

46 See, to that effect, judgment of 27 September 2017, *Puškár* (C−73/16, EU:C:2017:725, paragraphs 54 to 76 and the case-law cited).

47 See Article 79 and also recital 145 of the GDPR.

48 Bearing in mind also that in practical terms, that solution coincides with what would typically be the (indeed protective) forum (*actoris*) in consumer contracts under the Brussels Regulation regime – see, in general, judgment of 25 January 2018, *Schrems* (C−498/16, EU:C:2018:37).

49 See recitals 141 and 143 of the GDPR, and judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 110).

50 See recital 143 and Article 78 of the GDPR.

51 For such an approach in another (decentralised) regulatory context, see my Opinion in *Astellas Pharma* (C-557/16, EU:C:2017:957).

52 On the latter issue, Article 78(4) notes that 'where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that Opinion or decision to the court'. In practical terms, this is likely to be the only avenue for a judicial review of Board decisions, since as recital 143 of the GDPR ominously confirms, 'any natural or legal person' (hence including data subjects) can, when the conditions provided for in Article 263 TFEU are satisfied, challenge a legally binding decision of the Board before the EU Courts. However, in view of the Court's restrictive interpretation of the conditions for standing of individuals set out in the fourth paragraph of Article 263 TFEU, it is not easy to identify situations in which individuals could be deemed to be *directly* concerned by decisions of the Board, since the latter decisions will in any event have to be 'applied' to the situation of a specific data subject by a subsequent decision of the LSA or an SAC. In such a situation, as in many others areas of EU law (critically on this issue, see my Opinion in *Région de Bruxelles-Capitale* v *Commission* (C-352/19 P, EU:C:2020:588, points 137 to 147)), the only way to challenge a decision of the Board would ultimately be through a preliminary ruling under Article 267 TFEU, limited to instances in which a more inquisitive national court wished to 'lift the veil' of its own judicial review, placed over it by the national supervisory authority in the form of the 'forwarded' opinion of the Board pursuant to Article 78(4) of the GDPR.

53 See especially Article 60(1) of the GDPR.

54 Hijmans, H., 'Comment to Article 56 of the GDPR', in Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, Oxford, 2020, p. 918

55 Hustinx, P., 'EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation', in Cremona, M. (ed.), *New Technologies and EU Law*, 2017, Oxford University Press, Oxford, p. 123.

56 For that expression, see Council, 'Orientation debate on one-stop-shop mechanism', 10139/14 of 26 May 2014, p. 4.

57 See, for example, judgment of 9 March 2010, *Commission* v *Germany* (C-518/07, EU:C:2010:125, paragraph 24). More recently, see judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 42).

58 See above, point 4 of this Opinion.

59 My emphasis.

60 In this context, I would merely add that the supervisory authorities that receive a complaint – irrespective of their position as LSA or SAC – are not only required to *examine* that complaint with due diligence (see above at point 69 of this Opinion), but they are also required to ensure that 'the GDPR is fully *enforced* with all due diligence' (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems* (C−311/18, EU:C:2020:559, paragraph 112) (my emphasis).

61 My emphasis.

62 My emphasis.

63 See Tosoni, L., 'Comment to Article 60 of GDPR', in Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, Oxford, 2020, p. 969.

64 My emphasis.

65 Depending on, as clarified by recital 138 of the GDPR, the type of measure concerned. However, in realistic terms, it would be rather surprising if, even if not formally binding under the GDPR, an LSA would choose to ignore a decision of the Board (in particular since what is not binding in the first round might become very much so in the next).

66 Similarly, in more detail, Van Eecke, P., Šimkus, A., 'Comment to Article 64', in Kuner, C., Bygrave, L., Docksey, C. (eds), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, Oxford, 2020, p. 1011.

67 See above, points 106 and 107 of this Opinion.

68 See above, points 35 to 38 of this Opinion.

69 See also Article 29 of the Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 rev.01, of 5 April 2017, p. 10.

70 Moreover, I do not claim that the examples mentioned above are an exhaustive list. Could there not be a further situation in which the final decision taken in a given case of cross-border processing – whether by agreement between the LSA and the SACs, or following a dispute resolution by the Board – might entrust one or more SACs with the task of carrying out certain *acts of enforcement* in their respective territories including, for example, the commencement of legal proceedings?

71 As set out above, in points 31 to 38 of this Opinion.

72 Above, points 32 to 33 of this Opinion.

73 As it ought to be, in general the case for any processing as such, and the definition of the (joint) controller thereof. The effective control over *the purposes and means* of processing is to be assessed with regard *to a given processing operation*, and not in abstract, static terms, with regard to undefined 'processing' – see judgment of 29 July 2019, *Fashion ID* (C−40/17, EU:C:2019:629, paragraphs 71 to 74).

74 See above, points 111 and 112 of this Opinion.

75 See above points 45 and 84 of this Opinion.

76 Thereby indirectly circling back to the initial issue of what exactly is such an establishment in fact being prosecuted for in that Member State *after the* the GDPR has become applicable, as discussed above in points 32 to 34 of this Opinion.

77 Judgment of 5 June 2018 (C−210/16, EU:C:2018:388).

78 Compare, in particular, the new Article 3(1) with the old Article 4(1)(a), and the new Article 58(6) with the old Article 28(3), third indent.

79 However, as suggested above in footnote 70, it is equally conceivable that coordinated decision-making might result in coordinated enforcement measures.

80 See, by analogy, judgment of 14 February 2012, *Toshiba Corporation and Others* (C−17/10, EU:C:2012:72, especially paragraph 60).

81 For a detailed discussion with examples, see my Opinion in *Nemec* (C−256/15, EU:C:2016:619, points 27 to 44).

82 See also above, point 34 of this Opinion.

83 In more detail, see my Opinion in *Klohn* (C−167/17, EU:C:2018:387, points 36 to 46).

84 While of course direct applicability is not direct effect, and the same conditions for direct effect apply with regard to provisions of regulations foreseeing or necessitating their implementation – see, for example, judgments of 11 January 2001, *Monte Arcosu* (C−403/98, EU:C:2001:6, paragraphs 26 to 28); of 28 October 2010, *SGS Belgium and Others* (C−367/09, EU:C:2010:648, paragraphs 33 et seq.); or of 14 April 2011, *Vlaamse Dierenartsenvereniging and Janssens* (C−42/10, C−45/10 and C−57/10, EU:C:2011:253, paragraphs 48 to 50).