Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements

Version 1.0

Adopted on 2 February 2021

Important note:
This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website.

Table of contents

The European Data Protection Board

Having regard to Article 57(1)(f) and Article 77 and Article 78 of the Regulation 2016/679/EU 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, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1. During the 10th plenary meeting on the 9-10 July 2019, the EDPB granted the Enforcement Expert Subgroup a mandate to:

    a. Develop a common interpretation of Article 57(1)(f) and a common understanding of the minimum requirements to fulfil the obligation to "investigate the complaint to the extent appropriate",
    b. Assess how supervisory authorities deal with information related to a possible infringement of data protection law in order to evaluate the need for developing guidelines or other tools that ensure a consistent approach, in particular in relation to the impact on the cooperation mechanism,
    c. Assess the practice of supervisory authorities on what constitutes a draft decision pursuant to Article 60(3) and reach a common understanding about it as well as on when there is no need to create such a decision,
    d. Assess in the case of cross-border processing, whether and in what way there is an obligation for the competent authority in the event of notification by a supervisory authority concerned of a possible infringement of data protection, to submit a draft decision in accordance with the second sentence of Article 60(3) GDPR even if there is no specific reference to a complaint within the framework of the regulation on the cooperation procedure

2. The present document concerns only question one and two of the mandate. It is in terms of its scope not limited to the handling of complaints and information related to possible infringements that are cross-border in nature. The first section of this paper aims to create a shared understanding of the obligation under 57(1)(f) in general and the second section aims to ensure a consistent approach concerning information related to a possible infringement.

2 LEGAL FRAMEWORK

2.1 Introduction

3. The fundamental right of data protection as enshrined in Article 8 of the Charter of Fundamental Rights ("The Charter") provides *inter alia* that compliance with data protection rules shall be subject to control by an independent authority.

4. In ensuring such control, the GDPR aims at providing a more coherent data protection framework in the European Union backed by strong enforcement.

5. It is thus the task of supervisory authorities to monitor and enforce the GDPR. This is set out in Article 57 that amongst the listed supervisory duties outlines that supervisory authorities shall handle and investigate complaints from data subjects. This key duty of supervisory authorities corresponds with the right of data subjects pursuant to Article 77 to lodge a complaint with a supervisory authority. As "monitoring bodies", supervisory authorities function as complaint handling bodies as well as being empowered to undertake independent supervisory activities necessary for the performance of their supervisory duties.

6. In order to ensure a consistent and high level of protection of natural persons, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data should be equivalent in all Member States. Data subjects shall enjoy equal access to exercise their right to data protection regardless of which supervisory authority would handle a given complaint.

7. With a view to ensuring a consistent and homogenous level of protection, it is important that supervisory authorities share a common understanding of their tasks, including that of handling complaints from data subjects. When applying the provisions of the GDPR, the overarching purpose of ensuring a uniform level of protection of natural persons with regard to the processing of personal data must be taken into account. The enforcement of these rules should contribute to this. Moreover, an interpretation of a given provision must not undermine the effectiveness of EU law and its principle of primacy in an area that has been regulated by the EU (see below regarding the principle of procedural autonomy).

2.2 Legal framework

8. While acknowledging that the previous legal frameworks under the previous Directive 95/46 ("the Directive")[1] have been applied in slightly different contexts, it is relevant to recall the essential predecessor provisions in order to properly assess the application of provisions of the Regulation.

9. The tasks of supervisory authorities were not comprehensively described in Directive 95/46. Article 28(1) merely stated that the authorities were responsible for monitoring the application of the provisions adopted by the Member States pursuant to the Directive. Article 28(4) referred to the task of hearing claims and the right to be informed of the outcome hereof.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

10. On 25 January 2012, the European Commission presented its proposal for the General Data Protection Regulation[2] to replace Directive 95/46. One of the circumstances leading to the new legal framework was, as stated in the Commission Staff Working Paper Impact Assessment[3], that individuals in practice enjoyed different data protection rights, due to fragmentation as well as inconsistent implementation and enforcement in different Member States. To this end, the proposal for a new Regulation *inter alia* focused on ensuring stronger enforcement of the rules.

11. Chapter VI (Independent supervisory authorities) of the GDPR reinforces *inter alia* the role and powers of supervisory authorities. Article 57(1) lists the tasks of supervisory authorities, whereas Article 58(1) of the GDPR lists the investigative powers that the supervisory authorities shall have. When comparing the tasks of supervisory authorities as held in Article 57 of the GDPR with the tasks of supervisory authorities under the previous legal framework, it appears that the number of tasks have been expanded or strengthened.

12. Chapter VIII (Remedies, liability and penalties) includes provisions that strengthen the legal position of data subjects *vis-a-vis* supervisory authorities in providing the data subject with a right to lodge a complaint and to an effective judicial remedy against a supervisory authority.

2.2.1 Article 57(1): Tasks of supervisory authorities

13. Article 57 enumerates several tasks of supervisory authorities.

14. Article 57(1) provides *inter alia* that:

1. Without prejudice to other tasks asset out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

[…]

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

[…]

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

[2] 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/2012/011 final - 2012/0011 (COD) */

[3] COMMISSION STAFF WORKING PAPER Impact Assessment /* SEC/2012/0072 final */https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

[…]

15. This Article should be read in conjunction with Recital 129, which provides that: "*In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings.*

[…]The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision."

2.2.2 Article 58(1): Investigative powers of supervisory authorities

16. In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority.

Article 58(1) provides that:

Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2.2.3 Article 77: The right to lodge a complaint with a supervisory authority

17. Article 77 stipulates the right of data subjects to file a complaint with a supervisory authority regarding an alleged infringement of his or her personal data. The provision also sets out a duty to inform the complainant on the progress and outcome of the complaint.

18. Article 77 provides that:

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

19. In the context of the right to lodge a complaint should be read in conjunction with Recital 141: "*Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority 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.*

The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject […]."

2.2.4 Article 78: Right to an effective judicial remedy against a supervisory authority

20. Article 78 sets out the right to an effective judicial remedy against a legally binding decision of a supervisory authority and against an 'inactive' supervisory authority.

Article 78 provides that:

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. 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.

21. This Article should be read in conjunction with Recital 143, which provides that:

"Each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority."

2.3 EU Case law

22. The importance of consistent and homogeneous EU data protection rules - in particular as regards the independency and the powers of the supervisory authorities in light of Article 8(3) of the Charter and Article 16 TFEU - has been underlined by the Court of Justice of the European Union ("Court of Justice" or "the Court"). The Court of Justice has consistently emphasized that control by an independent authority is an essential component of the right to protection of personal data.

23. In its judgment of 6 October 2015, *Schrems* (C 362/14, EU:C:2015:650), the Court underlines that "*As regards the powers available to the national supervisory authorities (...) Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU. In order to guarantee that protection [of individuals with regard to the processing of personal data], the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings*."[4]

24. Moreover, the Court noted – in the context of a Commission decision pursuant to Article 25(6) of Directive 95/46 – that it is incumbent upon a supervisory authority to examine the claim from the data subject regarding the protection of his or her privacy with "all due diligence": "*Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings,*

[4] Para. 40, 42 and 43.

the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence"[5].

25. The Court stressed in its judgement of 16 July 2020, Facebook Ireland and *Schrems* (Case C-311/18, EU:C:2020:559) that the primary responsibility of supervisory authorities is to monitor the application of the GDPR and to ensure its enforcement: "*In accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data.[….][6]. It follows from those provisions that the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement*. [….]"[7].

26. Furthermore, the Court underlined with reference to Article 57(1)(f) and Article 77(1) that supervisory authorities must handle a complaint with all due diligence and examine the nature of the complaint as necessary: "*In addition, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must handle such a complaint with all due diligence (see, by analogy, as regards Article 25(6) of Directive 95/46, judgment of 6 October 2015, Schrems, C 362/14, EU:C:2015:650, paragraph 63)*" [8].

27. As to the means of investigation and its outcome the Court highlights the supervisory authority's investigative powers in Article 58(1) and its corrective powers in Article 58(2) GDPR: "*In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt*."[9] Even though the judgment of the Court references actions related to unlawful transfer of personal data to third countries, the EDPB recognizes that the duty to take appropriate action in relation is a general obligation of SAs and is not limited to investigative and corrective powers applied in the field of data transfers.

28. In this context, the Court acknowledged the discretion of the supervisory authority to choose among adequate measures, but also clarified that the supervisory authority can be required by EU law to enforce the GDPR with all due diligence, especially where the controller or processor does not take remedial action on its own: "*Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances (…), the supervisory*

5 Para. 63.
6 Para. 107.
7 Para. 108.
8 Para. 109.
9 Para. 111.

authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence. In that regard, (…), the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."[10] Even though the judgment relates to complaints in the context of transfer of personal data to a third country, the EDPB infers that the duty to review complaints with due diligence extends to all complaints, regardless of their subject matter.

29. The Court also noted that the right of each person to an effective judicial remedy under the GDPR applies in particular where the supervisory authority fails to deal with a complaint: "*Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that 'right to an effective judicial remedy in accordance with Article 47 of the Charter' in circumstances where that supervisory authority 'does not act where such action is necessary to protect the rights of the data subject"*[11].

30. In view of the relevance of national administrative laws as regards the handling of complaints, reference should be made to the jurisprudence of the Court of Justice concerning the interpretation of both national and secondary legislation including the principle of national procedural autonomy.

31. The principle of national procedural autonomy[12] implies that unless the procedural issues are directly regulated in the EU primary or secondary law, the Member States retain their competence to independently legislate on procedural issues. This autonomy has its limits as procedural solutions adopted by the Member State must be in line with principles of effectiveness and equivalence[13]. In terms of the GDPR, this means that national procedural law may not lead to fragmentation and hinder the consistent handling of complaints throughout the Union. In particular, the enforcement of the GDPR must comply with the principles of equivalence and effectiveness.

32. In C-78/98 Preston and Others[14] ruling, the Court stated that: *"(...) according to settled case-law, in the absence of relevant Community rules, it is for the national legal order of each Member State to designate the competent courts and to lay down the procedural rules for proceedings designed to ensure the protection of the rights which individuals acquire through the direct effect of Community law, provided that such rules are not less favourable than those governing similar domestic actions (principle of equivalence) and are not framed in such a way as to render impossible in practice the exercise of rights conferred by Community law (principle of effectiveness) (see, to that effect, Case 33/76 Rewe [1976] ECR 1989, paragraphs 5 and 6, Case 45/76 Comet [1976] ECR 2043, paragraph 13, Fisscher cited above, paragraph 39, Case C-410/92 Johnson*

[10] Para. 112 and 113.
[11] Para. 110.
[12] The term 'procedural autonomy' was used in the Court jurisprudence in Delena Wells case C-201/02, para. 65, 67, 70.
[13] See also C-201/02, para. 70.
[14] C-78/98, para. 57.

[1994] ECR I-5483, paragraph 21, and Case C-246/96 Magorrian and Cunningham v Eastern Health and Social Services Board [1997] ECR I-7153, paragraph 37)".

33. Moreover, in N.S. and Others[15] case, the Court ruled that: "*According to settled case-law, the Member States must not only interpret their national law in a manner consistent with European Union law but also make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the European Union legal order or with the other general principles of European Union law (see, to that effect, Case C-101/01 Lindqvist [2003] ECR I-12971, paragraph 87, and Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-5305, paragraph 28)*."[16]

34. The extensive case law quoted by the Court reiterates that the Court has consistently ruled that Member States must interpret and apply secondary European Union legislation in a manner consistent with fundamental rights and interpret national law in consistence with European Union law.

3 INVESTIGATING COMPLAINTS

3.1 Introduction

35. Supervisory authorities are independent public administrative authorities with specific supervisory tasks. It is an inherent feature of a supervisory authority that it has a certain margin of discretion to set its priorities in its enforcement activity while cooperating with other supervisory authorities with a view to ensuring the consistency of application and enforcement of the Regulation.

36. Complaints are one of a number of sources of information for detecting infringements of data protection rules and the handling of complaints is for that reason naturally an important task for supervisory authorities.

37. As mentioned above, the right of the individual to the protection of personal data is a fundamental right. In order to ensure the fulfilment of this right, it is of crucial importance that supervisory authorities cooperate effectively. To this end, supervisory authorities must reach a common understanding of the obligations entrusted to them by the GDPR.

38. Supervisory authorities have thus pursuant to Article 57(1)(f) a duty to handle each and every complaint submitted to them and to investigate the subject matter of the complaint to the extent appropriate. It is crucial that supervisory authorities have a shared understanding of this obligation and have efficient procedures for handling complaints.

3.1.1 The role of national procedural law

39. The current regulatory system of EU law does not aim to unify procedural law. EU legal instruments may include procedural provisions (such as the GDPR Articles conferring certain powers on supervisory authorities), but insofar EU law does not provide for specific procedural rules, national procedural law

[15] C-411/10.
[16] Ibid, para. 77.

applies. This is known as the principle of national procedural autonomy, which is a general principle of EU law. This general principle is limited, as is outlined extensively in the case law of the CJEU, by the EU principles of equivalence and effectiveness. These principles entail that EU law should be treated the same as national law (equivalence) and the exercise of rights conferred by EU law should not be rendered excessively difficult or practically impossible (effectiveness).

40. Since the GDPR does not further regulate the handling of complaints, the tasks entrusted to supervisory authorities by Article 57 of the GDPR should be fulfilled by relying on national procedural law, which must include – at the very least – the powers provided for by Article 58 of the GDPR. However, these national procedural rules should apply to national - and EU law alike, and must not make it excessively difficult or impossible to exercise the rights conferred by the GDPR. This applies also to the handling of complaints.

41. Different national administrative rules exist. Such differences may partly be the reason why supervisory authorities handle complaints in different ways and investigate them to different extents. Nevertheless, these differences in national procedural law can never lead to situations in which the principles of equivalence and effectiveness are undermined.

42. The GDPR creates two types of rights that it is important to distinguish between: (i) the procedural rights for complainants that a supervisory authority must respect, and (ii) the substantive rights that the GDPR creates for data subjects vis-à-vis the controller/processor. The application of national procedural law should not make it impossible or excessively difficult for a complainant to exercise its procedural rights vis-à-vis the supervisory authorities (e.g. lodging a complaint), and should also not make it impossible or excessively difficult for a data subject to exercise its rights vis-à-vis the controller/processor.

3.1.2 Procedurals rights of the complainant under the GDPR and general principles of law

43. The duty of supervisory authorities to handle and investigate complaints in Article 57(1)(f) corresponds with the right of data subjects to submit a complaint pursuant to Article 77.

44. Article 77 establishes a right for every data subject to lodge a complaint with a supervisory authority and to be informed on the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78. It should be noted that Article 77 does not establish a right for a complainant to necessarily become party to the supervisory authorities' administrative proceedings against the controller. Nevertheless, national procedural law can provide such a right.

45. Article 78(1) provides the affected person (natural or legal) with a right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. The dismissal or rejection of a complaint is such a legally binding decision affecting the complainant, cf. recital 143 GDPR. Article 78(2) provides data subjects with a right to an effective judicial remedy against a supervisory authority if it does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged. This indicates a duty of a supervisory authority to inform the complainant within 3 months after the submission of the complaint about the process of handling the case unless the result of the proceeding is established. It does not, however, require the case to be closed in this tight timeframe nor to inform the complainant repeatedly every three months of the

status of the case. The complainant should, however, as indicated by Recital 141 be informed that the matter requires further investigation.

46. The Regulation strengthened the position of data subjects vis-à-vis supervisory authorities by formulating a "rights-based approach" in regard to complaints. These procedural rights would be devoid of purpose if there were not a corresponding duty of supervisory authorities to handle complaints and inform complainants of the progress and outcome of the complaint. Article 57(1)(f) must therefore be read in light of Articles 77 and 78.

47. Legally binding decisions taken by supervisory authorities should fulfill the requirements set out in Recital 129, i.e. be in writing, clear and unambiguous, giving the reasons for the measure etc.

48. Taken as a whole, the provisions in question imply that every admitted complaint that is not granted must result in an outcome specifying the reasons for the decision to enable the complainant to understand the result of his or her complaint and enabling a given competent authority to exercise its power of review.

49. For every admitted complaint - which is not withdrawn –SAs must thus provide an outcome specifying the facts and legal considerations for e.g. rejecting the complaint or dismissing the complaint i.e. not investigating it further, with a view to make it a legally attackable act.

3.2 Definition of a complaint

50. Initially, the definition of a complaint needs to be explored to ensure a common understanding hereof as a basis for the interpretation of Article 57(1)(f). The definition is also crucial as it relates to when the claim may be rejected on the basis of formally not constituting a complaint.

51. The GDPR does not explicitly define what constitutes a complaint, but Article 77 provides a first understanding in providing that "*every data subject shall have the right to lodge a complaint (…) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*".

52. Furthermore, the most relevant English meanings of "complaint" include: "*A statement that something is unsatisfactory or unacceptable"; "The plaintiff's reasons for proceeding in an action*" (Oxford English Dictionary).

53. The Internal Guidance on Local Cases offers additional guidance on the definition of a complaint. It specifies that a complaint may be defined as: *a submission to a supervisory authority by an identified natural person – or a not-for-profit body, organization or association that fulfils the conditions provided by Article 80 of the GDPR – who considers that "the processing of personal data relating to him or her infringes this Regulation*".

54. Thus, the Guidance further underlines that a complaint is not restricted to a breach of the rights of the data subject under Chapter III of the GDPR but is, more generally, an infringement of the Regulation by a processing of the complainant's personal data.

55. On the contrary, enquiries and "tips" are not complaints. An enquiry could be e.g. a request for advice from a controller or processor on the implementation of data protection law or a request from a natural person for advice about how to exercise his or her rights. Moreover, a suggestion made by a natural person that he or she thinks that a particular controller or processor is not compliant with the GDPR would not either be considered a complaint provided he or she is not among the concerned data subjects.

56. A complaint has to fulfil the formal conditions of the Member State where it was lodged. National requirements for filing a complaint (admissibility criteria) should not undermine the right of the data subject to lodge a complaint under Article 77, with a supervisory authority of his or her choice.

57. As regards the level of proof required to admit a complaint, it is necessary and sufficient that the complainant provides a substantiated complaint. This means that the circumstances that allegedly constitute an infringement of the GDPR must be presented in a way that the supervisory authority will be able to investigate the case. If the complainant presents circumstances that state a reason, why he or she considers that the processing of personal data relating to him or her infringes the Regulation, the complaint is substantiated. In contrast, this would for instance not be the case if the subject matter is not related to personal data. The SA should however take steps, if appropriate, to clarify the unsubstantiated issues before dismissing the complaint.

3.3 "Investigate" the subject matter of the complaint

58. The GDPR does not specifically define what constitutes an "investigation" in the sense of Article 57(1)(f). The most relevant ordinary English meaning of "investigate" is to carefully examine the facts of a situation, an event, a crime, etc. to find out the truth (Oxford Dictionary). It should further be noted that the term "investigation" has a specific definition in some Member States' national legislation which may go further than the common understanding of what constitutes an investigation.

59. The change in wording from 'hear claims' in Directive 95/46 to 'handle and investigate' in the GDPR implies a change in the tasks of supervisory authorities. An actual investigation requires the authority to take specific actions as opposed to hearing claims that has a more passive connotation.

60. The term "to handle" should, according to an ordinary meaning of the term be understood as "to deal with" (Oxford Dictionary). This understanding is underpinned by the wording proposal of the Council to Article 57(1)(f). The change in wording from "deal with" to "handle" is presumably merely a matter of semantics. The term therefore refers to the whole procedure for dealing with or handling complaints and thus covers all stages.

61. The term "investigate" entails taking all necessary and appropriate steps with a view to resolving an issue or establishing whether an infringement has been committed and if so under what circumstances. For this purpose, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority.[17] Resolving an issue could include sending a letter to the

[17] CJEU, C-311/18, para. 111.

controller/processor reminding it of its duties to prompt some remedial action or settling the case amicably following action by either party to the complaint to resolve the case.

62. As stated in paragraph 54 above, for all admitted complaints that are not withdrawn, SAs must provide an outcome specifying the facts and legal considerations for e.g. rejecting the complaint or dismissing the complaint i.e. not investigating it further, with a view to make it a legally attackable act.

63. Necessary and appropriate steps encompass the measures (investigative powers) mentioned in Article 58, which include requesting information from the controller or processor, notifying the controller or the processor of an alleged infringement etc., or carrying out an audit or on-site inspection.

3.4 Investigate "to the extent appropriate"

64. Article 57(1)(f) read in conjunction with Article 77 and 78 implies an individual right to have every complaint (if admissible) handled and investigated to the extent necessary to reach an outcome appropriate to the nature and circumstances of that complaint. However, it falls within the discretion of each competent supervisory authority to decide the extent to which a complaint should be investigated. An outcome could e.g. be an establishment of an infringement, that the parties to the complaint through the intervention of the SA have settled the case amicably or, that the SA has sent a letter to the controller reminding it of its duties. It also falls within the discretion of the SA to assess and decide with all due diligence the extent to which specific investigative and corrective measures are appropriate, necessary and proportionate.[18]

If the supervisory authority decides not to investigate a complaint further, the complainant must be informed hereof and be provided with the rationale for concluding the investigation.

65. The term "to the extent appropriate" provides the competent supervisory authority with a margin of discretion as regards the extent or depth of the investigation needed. Which investigatory steps are to be taken, depends on both the circumstances of the specific case and the requirements under national procedural law. It is therefore not possible to formulate standardized minimum requirements regarding the duty to investigate but some degree of investigation must take place if the complainant is deemed admissible. A simple data subject rights breach may entail a very brief analysis of the documentation presented to verify the validity of the complaint. On the other hand a complex, technologically sophisticated or systemic failure could prompt a supervisory authority to deepen its investigation, namely to inspect the means and/or facilities used by the controller or processor, to ask for other public authorities to cooperate, to conduct hearings, etc. In any case, an investigation normally requires taking active steps to establish the facts and legal issues. Active steps could, but should not be limited to, in minor cases be to check whether similar complaints have been received regarding the same subject matter and same controller.

66. This discretionary power must be exercised in line with the other provisions of the Regulation and in accordance with appropriate procedural safeguards set out in Union and Member State Law, impartially, fairly and within a reasonable time. In case measures are taken, these should be appropriate, necessary and proportionate, taking into account the circumstances of the case, respect

[18] CJEU, C-311/18, para. 112 and 113.

the right to be heard before a measure (that may have adverse consequences), and superfluous costs and excessive inconveniences for the persons concerned should be avoided (cf. Recital 129).

3.5 Conclusion

67. The duty to handle and investigate complaints "to the extent appropriate" entails a duty for the competent supervisory authority to investigate every complaint to the extent that is appropriate in that specific case. There are certain situations where a full-fledged investigation is not required. In the absence of further Union law on the subject, this obligation can be effectuated based on national procedural law – provided that such national rules do not render virtually impossible or excessively difficult the exercise of the rights provided for in the Regulation. Moreover, SAs should always fulfill their other procedural obligations under the Regulation, as well as adhere to other applicable rules and principles of EU law.

68. The competent supervisory authority has a discretionary power to decide upon the necessary investigatory steps to be taken, including the extent and kind of information needed in order to provide a reply to the data subject and to decide on the necessity of enforcement action. This discretionary power must be exercised with all due diligence and in accordance with the relevant provisions of the Regulation. In all cases, the competent supervisory authority must examine the factual and legal issues raised by the complainant and provide a clear and reasoned reply to the complainant as well as an outcome of the complaint. Regardless of the outcome of the complaint process, sufficient reasoning must always be provided, also in cases where the complaint is rejected and no action is taken. Such reasoning may – depending on the type and complexity of the case – be kept rather short.

4 INFORMATION RELATED TO A POSSIBLE INFRINGEMENT OF DATA PROTECTION LAW

4.1 Introduction

69. A supervisory authority may determine an infringement of data protection law either when acting upon a complaint or when acting upon its own initiative, e.g. after being "informed otherwise of situations that entail possible infringements", as stated in Recital 131.
70. The GDPR does not define the term "infringement". In the Guidance on Local Cases, an infringement is defined as "a violation, a non-respect of the GDPR's provisions including both the failure to accommodate the data *subject* as well as non-compliance with other controller or processor obligations".

71. A supervisory authority may be informed of the existence of a potential infringement of data protection law through various means. The infringement could for instance come to its attention through information received through tips from natural persons (Article 54(2)), from another supervisory authority or a public authority (Article 57(1)(h)), a body association or organization not fulfilling the conditions set out in Article 80 or from press coverage.

72. Article 57(1)(f) regulates the handling and investigation of complaints as defined in Article 77. By contrast, the Regulation does not offer comparable guidance on how supervisory authorities shall handle information received otherwise related to possible infringements of data protection law. There

are, however, provisions that suggest that supervisory authorities may also launch investigations or open enforcement actions on the basis of information not originating from complaints.

4.2 Legal Framework

73. A supervisory authority has an obligation to monitor and enforce the application of the Regulation on its territory, cf. Article 57(1)(a). Spelling out the tasks of supervisory authorities in a more detailed manner, Article 57(1)(h) provides that each supervisory authority shall on its territory "*conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority*".

74. Additionally, Article 57(1)(g) entails a task to "*cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation*."

4.3 Conclusion

75. Since the Regulation does not entail a specific obligation to act upon information related to a possible infringement of data protection law similar to the obligation in Article 57(1)(f) regarding complaints, supervisory authorities seem to enjoy wide discretionary powers to decide when to initiate an investigation ex officio based on information received on potential infringements.[19]

76. When deciding whether to take action and launch an investigation based on information received, supervisory authorities should take into consideration whether there is evidence of the alleged infringement and evaluate the nature, gravity and duration of the possible infringement. If the alleged infringement is very severe, supervisory authorities would be encouraged to take action even if they have not received complaints regarding the same issue.

77. Should a supervisory authority never act on any information, no matter the seriousness of the possible infringement, it would likely not fulfil the general obligation in Article 57(1)(a). Moreover, it stems from the role as a supervisory authority and the supervisory tasks and powers that supervisory authorities should, and are expected to, assess information received on potential infringements, at least at a basic level.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[19] It should be noted that national legislation may oblige a supervisory authority to assess further information received regarding a possible infringement of data protection law.