Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints

Adopted on 15 December 2020

Table of contents

The European Data Protection Board

Having regard to Article 70 (1) (e) and 56.2 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 of 25 May 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 PART 1 – KEY CONCEPTS

1. The definitions given below are related to concepts that have not already been defined in other guidelines. The terms "*cross-border processing*"[1] and "*substantially affects*"[2] are therefore not defined in this section since a definition has been given in the Guidelines for identifying a controller or processor's lead supervisory authority (WP244).

1.1 Complaint

2. The GDPR does not explicitly define what constitutes a complaint but Article 77 gives a first understanding 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*".
3. Furthermore, the most relevant ordinary 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).
4. Consequently, 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[3] - who considers that "*the processing of personal data relating to him or her infringes this Regulation*".
5. It follows from the above that the definition of a complaint is not restricted to a breach of the rights of the data subject under chapter III of the GDPR[4] but is, more generally, an infringement of the Regulation by a processing of the complainant's personal data.

[1] Article 4(23) of the GDPR.

[2] Article 4(23) and Article 56.2.

[3] Article 57.1(f): « *each supervisory authority shall on its territory handle complaints lodged by a data subject, or by a body, organization or association in accordance with Article 80* ».

[4] Even if Recitals 141 and 142 emphasis on the possibility for a data subject to lodge a complaint within a supervisory authority where he "*considers that his or her rights under this Regulation are infringed*".

Example 1

A complaint is a request from a data subject about:
- a controller's refusal to give him or her a copy of his or her personal data undergoing processing (Article 15 of the GDPR);

- the absence of an answer from a controller or processor to the natural person who exercised his or her right to rectification (Article 16 of the GDPR);

- the alleged absence or insufficiency of measures implemented by the controller or processor to ensure a level of appropriate security for the processing of his or her personal data;

- the unauthorized disclosure of his or her personal data;

- the alleged unlawfulness of the processing of his or her personal data.

Example 2

On the contrary, a complaint should not be about:

- a request for advice from a controller or a processor on an envisaged or implemented processing of personal data;

- a controller or processor's general request about the GDPR, such as an inquiry about the data protection impact assessment;

- a natural person's general request about the GDPR, such as an enquiry for advice about how to exercise his or her rights mentioned in Article 57.1(e)[5];
- a suggestion made by a natural person that he or she thinks that a particular company is not compliant with the GDPR as long as he or she is not among the data subjects.

- cases without any reference to the processing of personal data such as disputes concerning exclusively commercial- or consumer protection matters such as a violation of the controllers general terms and conditions or violation of contracts

1.2 Infringement

6. The GDPR does not define the term "infringement" either. The most relevant ordinary English meaning of "infringement" is "The action of breaking the terms of a law, an agreement" (Oxford English Dictionary).

7. Therefore, an infringement is 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.

8. There are the following possibilities for the supervisory authority to determine an infringement:

[5] Article 57.1(e): "*each supervisory authority shall on its territory upon request, provide information to any data subject concerning the exercises of their rights under this Regulation*".

- The supervisory authority may determine that there is an infringement of the GDPR when acting upon a complaint, whether the complainant explicitly states that such infringement exists, or that he or she does not ;

The supervisory authority may act upon its own motion (ex officio), e.g., after being "informed otherwise of situations that entail possible infringements"[6] (e.g. by the press, another administration, a court, or another private company, a hint by a natural person which is however not a complaint within the meaning of Article 77).

Example 3

A supervisory authority may, during an investigation carried out on its own initiative, discover that a controller does not give the data subjects all the information provided by Article 13 of the GDPR at the time where personal data are obtained.

Example 4

A supervisory authority may be informed, through a press article, of the existence of a data breach that led to an unauthorized disclosure of personal data on Internet.

1.3 Amicable settlement

9. The GDPR does not define the meaning of the term "amicable settlement". This expression is mentioned only by Recital 131[7] which provides that "*the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers*". The most relevant meanings of "settlement" are "an arrangement" and "an official agreement intended to resolve a dispute or conflict". The adjective "amicable" means "characterized by friendliness and absence of discord" (Oxford English Dictionary).

10. Since Recital 131 refers to the "full range of powers" of the supervisory authorities, we could consider that the "amicable settlement" means the use of some of these powers which do not imply the use of corrective powers provided by Article 58.2.

Example 5

A controller or processor accepts to provide any information requested by a supervisory authority to resolve a complaint, such as clear proof that it has complied with Articles 33 and 34 of the GDPR in case of a personal data breach.

Example 6

A controller abides by the request of the data subject after the supervisory authority asks it to do so (for example with a telephone call or letter).

[6] Recital 131 of the Regulation.

[7] Even if Recital 131 concerns cases with only local impacts, seeking for an amicable settlement may also be a good practice when a SA is handling a case that does not fulfill the conditions laid down by article 56.2, depending on the national procedural legislation.

11. On the contrary, if the controller or processor refuses to give this information, the supervisory authority will have to order the latter to provide it. In this case the supervisory authority action cannot be viewed as an amicable settlement.

12. Other supervisory authority powers such as: carrying out investigations in the form of data protection audits, obtaining access to all personal data, or obtaining access to any premises of the controller and the processing, cannot be viewed as an amicable settlement either.

13. Although the GDPR encourages 'amicable settlement' by mentioning it explicitly in recital 131, it should be kept in mind that national procedural legislation may further specify how amicable settlements can be implemented in practice.

2 PART 2 – COMMON PRELIMINARY STEPS TO HANDLE A COMPLAINT OR AN INFRINGEMENT

14. This section aims to set out common preliminary handling procedures when a supervisory authority receives a complaint or detects a possible infringement. The first step is to ensure that the complaint is admissible (2.1). The second step is to verify the relevant facts of the case before introducing it in the IMI system, if necessary (2.2).

2.1 Step 1 - admissibility of the complaint

15. It will occur that a supervisory authority receives a complaint that has to be rejected on admissibility grounds. It can happen mainly in three situations:

- the subject matter of the complaint is clearly not related to the protection of personal data. This is the case when the GDPR does not apply, for example, because no personal data are processed. Consequently, the SA is not competent to handle such complaints.

- the claim is manifestly unfounded or excessive pursuant to Article 57.4 of the GDPR**.** A complaint is unfounded when its subject matter falls within the scope of the GDPR but obviously does not justify an action from a supervisory authority. In the same vein, a repetitive complaint can be considered as manifestly excessive and will consequently not be handled by the SA.

Example 7

The individual has submitted its request for exercising its rights to the controller less than one month ago and did not receive a reply. Even if the controller has to reply without delay, the maximum period laid down by Article 12.4 of the GDPR has not yet expired. Consequently the complaint is not admissible.

- the claim does not fulfill the formal conditions laid down by the Member State of the SA which received the complaint. These conditions could result from a legal obligation (for example the constitutional obligation to contact any administration in one of the official languages), from other applicable legal requirements e.g. administrative procedure requirements of the relevant Member State, or from the internal rule of the supervisory authority based upon respective legal provisions (such as, in some Member States, the obligation for the complainant to supply a proof of identity).

16. The complaint has to fulfill formal conditions of the Member State where it was lodged. Consequently, if the complaint is deemed admissible by the supervisory authority which received the complaint, the LSA shall not re-examine the admissibility of the complaint, due to formal aspects. In other words, the LSA cannot reject, due to formal aspects, to handle the complaint when the formal requirements of the receiving authority have been fulfilled.

17. According to Article 56.3, *"the supervisory authority shall inform the lead supervisory authority without delay*" when it receives a case about a cross-border processing which it deems has only local impacts. Nevertheless, when a supervisory authority receives a complaint that falls within one of the first two cases (the SA is not competent or the claim is manifestly unfounded), it may reject the complaint without first informing the LSA.

18. If the complaint is rejected by the SA because it does not fulfil the formal conditions (either laid down by a legal obligation in the Member State or by the internal rule of the supervisory authority), the supervisory authority which received the complaint *shall*, as a good practice and in alignment with its national law, first inform the complainant of the missing conditions in order to enable him or her to fulfil these conditions.

19. If the complainant still does not provide these elements, the supervisory authority *may* inform the LSA which can decide to handle the case or launch an ex-officio investigation if the circumstances justify that. Informing the lead supervisory authority may be particularly important when a complaint that is otherwise unsatisfactory for formal requirements reveals a serious infringement.

20. The notification of the LSA after the case has been rejected could be done on a monthly basis about the cases that have been directly rejected by the supervisory authority.

2.2 Step 2 – Preliminary vetting

21. This subsection describes a common approach on the preliminary checks to be carried out by all SAs before introducing a case in IMI ('due diligence').

22. The first sub-step mentioned below should be carried out by the receiving SA in order to obtain the information that is necessary to make a preliminary assessment of the cross-border and possible local nature of the case. The second sub-step is only to be applied for cases relating to exercise of data subject rights mentioned in Articles 12 – 22 of the GDPR ("DSR-cases").

23. Preliminary vetting of a complaint will be beneficial regardless of the route or pathway that the particular case takes afterwards (potential amicable resolution by the receiving SA, imposing corrective measures when the case is handled locally, the cooperation procedure according to Article 60 of the GDPR ….), as the relevant elements shall be included in the file from an early date. The preliminary vetting procedure should be completed by all receiving SAs but the specific approach may depend on whether the controller has an establishment on the territory of that receiving SA or not.

2.2.1 Sub-step 1 – to be applied for every cross-border incoming cases

24. Upon opening a case file, the receiving SA should consult the relevant publicly available information (e.g. companies' websites, national commercial register, etc.) to obtain possible information that is necessary to make a preliminary assessment of the cross-border and, if so, local nature of a case according to the criteria set out in Internal EDPB document on handling cases with only local impacts under Article 56.2 GDPR. The receiving SA could reach out to the assumed controller, the complainant, and/or the processor to obtain the necessary information if it cannot be ascertained through public

sources. When reaching out the receiving SA can either contact the assumed controller/processor directly or contact its local establishment within the territory of the receiving SA (if existing).

25. The receiving SA could ask for example the following questions:

- Who is the relevant controller or processor for the processing in question?
- Is there more than one establishment of the controller or processor in the EEA?
- If so, where is the main establishment? In other words, where is the place of the central administration or the place of the other establishment that takes decisions on the purposes and means of the processing?
- Is the processing cross-border in nature because it is being carried out in the context of the activities of establishments in more than one Member State?
- Is the processing cross-border in nature because it substantially affects or is likely to substantially affect data subjects in more than one Member State?

26. As the receiving SA cannot be certain at this stage whether it is a case concerning cross-border processing and whether or not the case has only local impacts, a disclaimer should be included in communications with the controller/processor stating for example that:

"*We need the requested information to assess whether the processing is cross-border in nature and to determine whether the subject matter of this case has only local impacts or not. The requested information shall be used in view of preparing the case-file for a handover to the Lead Supervisory Authority if such would be necessary. This letter is without any prejudice to any later decision which could be taken by the Lead Supervisory Authority in this matter*."

27. The receiving SA should then assess the response received:

- If the controller/processor provides evidence that the processing at stake is cross-border, the receiving SA must transfer the relevant information to the LSA through IMI, regardless whether it considers that the case has only local impacts or not;
- If the controller/processor provides evidence that the processing at stake is not cross-border, the receiving SA is fully competent to handle the case according to Article 55 of the GDPR; except if the SA receives a complaint about a non-cross-border processing that is carried out in another Member State than the SA's. In such case, the receiving SA request mutual assistance to the SA in the Member State where the processing is carried out. The latter handles the case but the receiving SA remains the interlocutor of the complainant (according to Article 77.2 of the GDPR).

Example 8
An online shop has its sole establishment in Member State A. It sells products via an internet website to only customers in Member State B. In the definition of the GDPR this is not a cross border case: Art. 4 (23) (a) does not apply because we have only one establishment. Article 4 (23) (b) does not apply because the processing does not affect data subjects in more than one Member State.

- If the controller/processor does not respond and the receiving SA has reason to believe that the processing activity may be cross-border, the receiving SA should inform the presumed LSA of the case through IMI.

- If the receiving SA already has sufficient information to assume with reasonable certainty the cross-border nature of the processing (cross-border or not) and the nature of the case (local or not) it can immediately proceed to upload to IMI.

2.2.2 Sub-step 2 – to be applied only for DSR-complaints

28. The application of this sub-step is limited to complaints relating to exercise of data subject rights (DSR-complaints) within the meaning of chapter III of the GDPR.

29. Upon receipt of a DSR complaint, the receiving SA may – in alignment with national administrative law – request more information from the complainant and/or the assumed controller/processor (or from its local establishment) in order to establish the facts of the case. As indicated in paragraph 26 of this guidance, a disclaimer should be included in the communications with the controller / processor. For example, the following questions could be asked (in addition to those mentioned under sub-step 1 above):

- Has the data subject already exercised his rights vis-à-vis the controller/processor, and if so, with what results?

- Does the controller/processor acknowledge having received the data subject request?

- Does the controller/processor have already taken (or envisages to take) certain steps to carry out the request, and if so, which steps and in which timeframe?

30. The receiving SA should then assess the response of the controller/processor:

- When the answer indicates that the controller has in the meantime already complied with the DSR or envisages to do so in a short timeframe, the receiving SA will request appropriate supporting evidence (if not provided already). If the controller complied with the DSR to the satisfaction of both the data subject and the receiving SA, the receiving SA should no longer inform the LSA of the DSR-case through an article 56 IMI notification, as the object of the complaint is no longer present. The receiving SA should nevertheless communicate the case and outcome to the LSA at an appropriate time for instance, on a quarterly basis (i.e.: trough the voluntary mutual assistance) ;

- When the controller refuses for whatever reason to collaborate with the receiving SA, the latter should inform the presumed LSA of the DSR-case through IMI.

31. This second sub-step of the preliminary vetting procedure may in practice give effect to data subject rights before a case ever needs to be notified to the LSA via the IMI. This may offer a potentially quick resolution to data subjects, but even if it cannot be resolved in that manner, the preliminary vetting steps already carried out should expedite the case handling once the lead supervisory authority has been seized. If the receiving SA already has sufficient information to assume with reasonable certainty the cross-border nature of the processing and the nature of the case (local or not) it can immediately proceed to upload the case to IMI.

For the European Data Protection Board

The Chair

(Andrea Jelinek)