

Internal EDPB Documents



Internal EDPB Document 2/2020 on how to deal with complaints relating to data protection infringements started before the entry into application of GDPR that continue after 25 May 2018

Adopted on 30 June 2020

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

1	INTR	RODUCTION	3	
	1.1	Background	3	
	1.2	Scope	3	
2	LEGA	AL ANALYSIS	6	
	2.1	General context	6	
	2.2	How are cases regarding ongoing infringements dealt with in the Member States?	6	
3	STEP	PS TO FOLLOW IN CASE OF CONTINUING INFRINGEMENTS RELATING TO CROSS-BORDER		
PF	PROCESSING			

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 3 and Article 22 of its Rules of Procedure as amended on 23 November 2018,

HAS ADOPTED THE FOLLOWING INTERNAL GUIDANCE

1 INTRODUCTION

1.1 Background

1. During its meeting on 14 May 2019, the Plenary of the European Data Protection Board (EDPB) gave mandate to the Cooperation Expert Subgroup to provide guidance on the question how to deal with cross-border complaints relating to data protection infringements started before the entry into application of the GDPR that continued after 25 May 2018.

1.2 Scope

- Many Supervisory Authorities (SAs) are dealing with complaints relating to potential/alleged data protection infringements that started before entry into application of GDPR that continue after 25 May 2018. As set out in Opinion 8/2019¹ a continuing infringement is an act (or omission) which lasts over a certain period of time².
- 3. The timelines below illustrate the scope of this paper (what is a continuing infringement) in case when infringement does not relate to data subject rights (case 1) and when infringement relates to data subject rights (case 2 and 3).

¹ Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment.

² See European Court of Human Rights, Grand Chamber, case of Rohlena v. the Czech Republic, application no 59552/08.

Case 1

- Complaint (not related to data subject rights) lodged before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Infringement ends after the entry into application GDPR



Case 2

- · Request for data subject right made before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Complaint lodged before the entry into application GDPR
- Infringement ends after the entry into application GDPR



- 4. Scenario A: An infringement (unlawful processing of personal data) started in February 2018. Data subject lodged a request for erasure of personal data in March 2018. The controller did not comply with the request. In April 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not complied with the data subject's request yet (and proceeding has not been finished) and therefore the infringement continues.
- 5. Scenario B: The data subject made a request for access to personal data in March 2018. The controller did not answer the request made by the data subject. In April 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not answered the data subject's request yet (and proceeding has not been finished) and therefore the infringement continues.

Case 3

- Request for data subject right made before the entry into application GDPR
- Infringement starts before the entry into application GDPR
- Complaint lodged after the entry into application GDPR
- Infringement ends after the entry into application GDPR



- 6. *Scenario A:* An infringement (unlawful processing of personal data) started in January 2018. The data subject lodged a request for erasure of personal data in March 2018. Controller did not comply with the request. In June 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not complied with the data subject's request yet and therefore the infringement continues.
- 7. *Scenario B:* The data subject made a request for access to personal data in March 2018. The controller did not answer the request made by the data subject. In June 2018 the data subject lodged a complaint with the SA. On 25 May 2018 the controller has not answered the data subject's request yet and therefore the infringement continues.
- 8. As shown by the above examples, the key factor is the continuing nature of the infringement, i.e. the fact that the infringement complained against started before 25 May 2018 (the "cut-off date") and continued (was not remedied) thereafter, irrespective of the date when the complaint was lodged with the SA. However, if the processing activity affected by the continuing infringement of the controller/processor qualifies as cross-border processing after the cut-off date, the issue arises of how to arrange for the handling of a complaint regarding such cross-border processing given the distribution of competence envisaged under the GDPR. This applies in particular since competence 'for the cross-border processing carried out by that controller or processor' lies with a LSA under Article 56(1) of the GDPR as from the cut-off date, and that LSA is not necessarily the SA receiving the original complaint.
- 9. It should be noted that in some Member States explicit transitional provisions were put into national law to address such cases of continuing infringement. Problems might arise though on account of conflicting national provisions giving rise in cross-border cases to competence issues.

10. For such situations the guidance should seek to find proposals for practical approaches taking into account the interests of all parties involved. Though looking at how national cases are dealt with in the Member States, this guidance does not intend to give advice how to deal with purely national cases. It only applies to cross-border cases.

2 LEGAL ANALYSIS

2.1 General context

11. The handling of complaints lodged with SAs must be seen in the broader context of the GDPR as well as overarching principles of EU law. The GDPR is meant to strengthen and to set out in detail of the rights of data subjects and gives SAs the powers for monitoring and ensuring compliance with the rules for the protection of personal data (Recital 11). Ensuring consistent monitoring of the processing of personal data by SAs in all Member States is one of the most important aims of the GDPR (Recital 13, 135 GDPR) and the main task of the EDPB (Article 70 (1) s. 1 GDPR).

According to Article 55 (1) GDPR each SA is competent to enforce the GDPR on its national territory. In cross-border cases, according to Article 56 GDPR, the authority of the single or main establishment is competent as LSA.

- 12. According to Article 57 (1) (a) GDPR it is the SA's duty to monitor and enforce the application of the GDPR (Recital 117 GDPR). The SA has to handle complaints lodged by a data subject and investigate, to the extent appropriate, the subject matter of the complaint (Article 57 (1) (f) GDPR. Moreover, according to Article 57 (1) (h) GDPR it is the SA's duty to conduct investigations on the application of the GDPR on their own initiative (*ex officio*).
- 13. It has to be kept in mind that the GDPR is of immediate effect and has priority to national Acts. Moreover, according to Recital 171³ processing already begun before 25 May 2018 should comply with the GDPR by 25 May 2018.

2.2 How are cases regarding ongoing infringements dealt with in the Member States?

14. There are different provisions in national Acts on the application of the GDPR on complaints relating to infringements that started before the entry into application of GDPR and continued after 25 May 2018.

National transitional provisions

In most Member States⁴, no transitional provisions apply or these provisions require the SA to apply the GDPR globally to complaints lodged before 25 May 2018 and regarding ongoing infringements. This would mean that these Member States find the one-stop-shop (OSS) mechanism to be applicable to the cross-border cases arising from pre-GDPR complaints.

³ Recital 171 s. 2 ["]Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force". ⁴ Such as Austria, Czech Republic, France, Germany, Italy, Luxembourg, Norway, Romania, Spain, Sweden.

- 2. However, there also exists, in some Member States, a 'mixed' approach in the transition provisions, where the GDPR will be applied as a substantive law to complaints lodged before 25 May 2018 with ongoing infringements, but the administrative proceeding will be governed by the previous procedural regime (Poland). Thus, the OSS mechanism would not be found to be applicable to these pre-GDPR proceedings.
- 3. In other Member States the transition provisions require that in case a complaint is lodged before 25 May 2018 and the investigation is initiated before this date (Hungary, Slovakia), or in cases where either the request to the controller was made, the contravention occurred or the complaint has been lodged before this date (Ireland, Slovenia), the previous legal regime would apply. Consequently, for SAs of these Member States the cooperation (and consistency) mechanism does not apply.
- 4. Regarding sanctions to an infringement that started before 25 May 2018, in many Member States according to the principle of non-retroactivity either the provisions of the previous legal regime or, in other Member States, those of the more lenient legal regime would apply.
- 15. In cases under 2. and 3., the receiving SA would not upload the case into the IMI system, as the OSS mechanism did not exist in previous data protection regime. On the other hand, the assumed LSA may be obliged to reject such complaint from the CSA that uploaded the case into the IMI system as it is precluded from acting as Lead Supervisory Authority (LSA). This paper focuses on the LSA's role in this context, especially on the application of the GDPR OSS mechanism to the complaint.

National approach to data subject's pre-GDPR and post-GDPR rights

16. SAs have different approaches to give effect to the GDPR provisions in cases where the application of the GDPR might not seem clear. When considering if there is a continuing data protection infringement, in some cases SAs take also account of the scope of the request lodged by a data subject; in particular, they consider if the right had already (similarly) existed under the previous national legal system or if it has been newly created by the GDPR.

Example 1: GDPR applied to continuing infringements that started pre-GDPR

In case of a request for access, expressly based on Article 15 (1) GDPR and subsequent complaint, both lodged before 25 May 2018, and dealt with by the SA after 25 May 2018, the complaint might be considered under GDPR if the infringement continued after that date. However, it would be taken into account that the request at the time it was lodged would not have been founded according to Article 15 (1) GDPR but according to the law previously applicable.

Counter-Example 1: Previous legal regime applied to continuing infringements that started pre-GDPR

A request for access according to Article 15 (1) GDPR lodged before 25 May 2018 and a complaint lodged before or even after this date would be treated by some SAs according to the substantive law applicable at the time of the request. However, in case the controller does not answer the request

before 25 May 2018, the SA might apply the GDPR and consider the lack of providing access an infringement of the GDPR.

17. While requests under Article 15 (1), Article 20 (1) and 21 (1) GDPR lead only to an infringement in case the request is not reacted upon properly, in other cases, e.g. in case of requests under Articles 16, 17 (1), 18 GDPR, processing of data may be without a legal basis. A controller's duty to rectification and erasure of personal data exists irrespective of the existence of a data subject's request, e.g. in case the personal data are no longer necessary to fulfil the purpose of the processing or if the retention periods have expired.

Example 2: *Ex officio* action taken in response to continuing infringements that started pre-GDPR A request under Article 17 (1) GDPR⁵ and a complaint are lodged before 25 May 2018. In the view of some SAs a request by a data subject under Article 17 (1) GDPR, lodged before 25 May 2018 would lead to a GDPR infringement as of 25 May 2018 if it is established that the infringement continues after 25 May 2018 and the SA might, if it is not legally precluded from, consider to handle the complaint *ex officio*.

3 STEPS TO FOLLOW IN CASE OF CONTINUING INFRINGEMENTS RELATING TO CROSS-BORDER PROCESSING

18. This guidance is aimed at putting forward proposals for those cases where

- the complaint fulfils the formal conditions laid down by the Member State of the SA which received the complaint
- the receiving SA has introduced the case into the IMI system and
- the assumed LSA is precluded from declaring itself as LSA. According to its national procedural rules, the assumed LSA would either not apply the GDPR to the case at all, or not apply the procedural rules laid down in the GDPR (Articles 60 et seq. GDPR).

Example 3: OSS mechanism initiated by the receiving SA to continuing infringements that started pre-GDPR

A request according to Article 17 (1) GDPR and a corresponding complaint are lodged before 25 May 2018, and dealt with by the SA after 25 May 2018. The infringement is ongoing after 25 May 2018.

Most SAs would apply the GDPR. The controller's refusal to rectify or erase personal data would be considered an ongoing infringement after 25 May 2018. In a cross-border case the receiving SAs would start a cooperation procedure in accordance with Article 60 GDPR if the case is not a local one according to Article 56 (2) GDPR.⁶ In the latter case, the SAs would inform the assumed LSA according to Article 56 (3) GDPR.

⁵ See Art. 12 (b) of the Directive 95/46.

⁶ See in this respect also Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR and related issues such as the preliminary vetting of complaints.

Counter-Example 3: OSS mechanism not found applicable to continuing infringements started pre-GDPR

A request according to Article 17 (1) GDPR and a corresponding complaint are lodged before 25 May 2018, and dealt with by the SA after 25 May 2018. The infringement continues after 25 May 2018. SAs which, according to national law provisions, are precluded from applying the GDPR in case the request, or both, the request and the complaint were lodged before 25 May 2018, or are precluded from applying the GDPR procedural rules to complaints lodged before this date, would not initiate a procedure according to Article 60 et seq. GDPR and would not declare themselves as LSA.

- 19. The guidance is not giving advice on how the assumed infringement is supposed to be assessed and sanctioned by the LSA. The LSA might come to the conclusion that the complaint is unfounded or the infringement (in accordance with national procedural rules or the principle of non-retroactivity), is not to be sanctioned under GDPR. Nevertheless, the question arises of how a complaint in a cross-border case, that is found admissible by the receiving SA and introduced into the IMI system, should be dealt with.
- 20. It is assumed that prior to initiation of an OSS procedure, it has already been established that the infringement complained against is a continuing one. Which means that, in the meantime, there has been no reply to the request made by the data subject to the controller or there has been only a partial reply, and that the complaint lodged with the SA prior to 25 May 2018 is admissible under the receiving SA's legislation in this respect. Such an analysis is in line with best practice as outlined in the Article 56.2 internal guidance, where the receiving SA should carry out preliminary vetting of a complaint which might also include contacting the data controller or its establishment situated in the receiving SA's Member State. It might also be preferable to contact the data subject and verify whether his request had not been answered upon.
- 21. If the abovementioned situation takes place and it is established that the infringement is continuing, different scenarios can be envisaged depending on the national legislation the assumed LSA is required to abide by (which should be made known clearly to the receiving SA in the reply to the cooperation request):
 - a) Firstly, one should recall that Article 60 (1) GDPR obliges the LSA and the CSAs to cooperate with each other in an endeavor to reach consensus within the cooperation procedures without involving the EDPB (Recital 138 s. 2). Informal cooperation procedures should be triggered, thus, before initiating formal procedures. The receiving SA may consider contacting the data subject or the data controller in line with the preliminary vetting procedures as outlined in Article 56.2 internal guidelines.
 - b) If the assumed LSA's national legislation provides that either the request with the controller or the complaint must have been lodged with the SA after 25 May 2018, the receiving SA (CSA) should contact the complainant and invite him or her to withdraw the existing complaint and lodge a new (possibly identical) complaint with the SA and to lodge a new request to the controller. In both cases the CSA should explain the underlying reasons (related to assumed LSA's national legislation constraints) and the consequences that may occur if the data subject refuses to do so

(including the possibility of a dispute between the involved SAs to be settled by the EDPB under Article 65 (1) (b), see below). If the data subject accepts that proposal, the LSA will then act on the new complaint pursuant to the GDPR (Article 60). If the data subject does not accept the above proposal, the available options are outlined in paragraphs c) and d) below.

- c) If the data subject does not accept the proposal by the SA to lodge a new (post 25 May 2018) complaint and request in respect of a continuing infringement, it should be considered if there can be reached a consensus between the assumed LSA and the receiving SA as to whether the complaint can be dealt with by the assumed LSA *ex officio*. If the *ex officio* action cannot be followed, the assumed LSA will resolve the case in accordance with its national provisions⁷.
- d) In case the assumed LSA, according to its national procedural rules, would refuse to handle the case as a competent authority, the receiving SA can ask the EDPB for a binding decision. Pursuant to Article 65 (1) (b) GDPR where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment, the binding decision of the Board shall be adopted. This article applies to all individual cases, even those pre-GDPR with ongoing infringements, as this competence of the Board arises from 25 May 2018 onwards.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁷ For instance Section 8(2) of the Irish Data Protection Act provides: "The Act of 1988 shall apply to (a) a complaint by an individual under section 10 of that Act made before the commencement of this section, and (b) a contravention of that Act that occurred before such commencement".