Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR

Adopted on 09 November 2020

Table of contents

The European Data Protection Board

Having regard to Article 63 and Article 65(1)(a) 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 (General Data Protection Regulation) (hereinafter "**GDPR**")[1],

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[2],

Having regard to Article 11 and Article 22 of its Rules of Procedure[3],

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "**EDPB**" or the "**Board**") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 60 GDPR that the lead supervisory authority (hereinafter "**LSA**") shall cooperate with the other supervisory authorities concerned (hereinafter "**CSAs**") in an endeavour to reach consensus, that the LSA and CSAs shall exchange all relevant information with each other, and that the LSA shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. The LSA shall without delay submit a draft decision to the other CSAs for their opinion and take due account of their views.

(2) Where any of the CSAs expressed a reasoned and relevant objection ("**RRO**") on the draft decision in accordance with Article 4(24) and Article 60(4) GDPR and the LSA does not intend to follow the RRO or considers that the objection is not reasoned and relevant, the LSA shall submit this matter to the consistency mechanism referred to in Article 63 GDPR.

(3) Pursuant to Article 65(1)(a) GDPR, the EDPB shall issue a binding decision concerning all the matters which are the subject of the RROs, in particular whether there is an infringement of the GDPR.

(4) The binding decision of the EDPB shall be adopted by a two-thirds majority of the members of the EDPB, pursuant to Article 65(2) GDPR in conjunction with Article 11(4) of the EDPB Rules of Procedure, within one month after the Chair and the competent supervisory authority have decided that the file is complete. The deadline may be extended by a further month, taking into account the complexity of the subject-matter upon decision of the Chair on its own initiative or at the request of at least one third of the members of the EDPB.

(5) In accordance with Article 65(3) GDPR, if, in spite of such an extension, the EDPB has not been able to adopt a decision within the timeframe, it shall do so within two weeks following the expiration of the extension by a simple majority of its members.

[1] OJ L 119, 4.5.2016, p. 1.
[2] References to "Member States" made throughout this decision should be understood as references to "EEA Member States". References to "EU" should be understood, where relevant, as references to "EEA".
[3] EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020.

1 SUMMARY OF THE DISPUTE

1. This document contains a binding decision adopted by the EDPB in accordance with Article 65(1)(a) GDPR. The decision concerns the dispute arisen following a draft decision (hereinafter "**Draft Decision**") issued by the Irish supervisory authority ("Data Protection Commission", hereinafter the "**IE SA**", also referred to in this context as the "**LSA**") and the subsequent objections expressed by a number of CSAs ("Österreichische Datenschutzbehörde", hereinafter the "**AT SA**"; "Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit"[4], hereinafter the "**DE SA**"; "Datatilsynet", hereinafter the "**DK SA**"; "Agencia Española de Protección de Datos", hereinafter the "**ES SA**"; "Commission Nationale de l'Informatique et des Libertés", hereinafter the "**FR SA**"; "Nemzeti Adatvédelmi és Információszabadság Hatóság", hereinafter the "**HU SA**"; "Garante per la protezione dei dati personali", hereinafter the "**IT SA**"; "Autoriteit Persoonsgegevens, hereinafter the "**NL SA**"). The draft decision at issue relates to an "own-volition inquiry" which was commenced by the IE SA following the **notification of a personal data breach** on 8 January 2019 (the "**Breach**") by Twitter International Company, a company established in Dublin, Ireland (hereinafter "**TIC**")[5].

2. The data breach arose from **a bug in Twitter's design**, due to which, if a user on an Android device changed the email address associated with their Twitter account, the protected tweets became unprotected and therefore accessible to a wider public (and not just the user's followers), without the user's knowledge[6]. The bug was discovered on 26 December 2018 by the external contractor managing the company's "bug bounty programme", which is a programme whereby anyone may submit a bug report[7].

3. During its investigation, Twitter discovered additional user actions that would also lead to the same unintentional result. The bug in the code was **traced back to a code change made on 4 November 2014**[8].

4. TIC informed the IE SA that, as far as they can identify, between 5 September 2017 and 11 January 2019, **88,726 EU and EEA users were affected** by this bug. Twitter has confirmed that it dates the bug to 4 November 2014, but it has also confirmed that it can only identify users affected from 5 September 2017 due to a retention policy applicable to the logs[9]. As a result, TIC acknowledged the possibility that more users were impacted by the breach[10].

5. The decision of the IE SA to commence the inquiry was taken in circumstances where TIC had, in its breach notification form, identified the **potential impact for affected individuals as being "significant"**[11].

[4] The objection by the Hamburg SA was submitted representing also "Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg", "Berliner Beauftragte für Datenschutz und Informationsfreiheit", "Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern", "Die Landesbeauftragte für den Datenschutz Niedersachsen". The objection has been also coordinated with other SAs in Germany.
[5] Draft Decision, paragraphs 1.1-1.2.
[6] Draft Decision, paragraph 1.9.
[7] Draft Decision, paragraphs 2.7 and 4.7.
[8] Draft Decision, paragraph 2.10.
[9] Draft Decision, paragraph 2.10.
[10] Draft Decision, paragraphs 1.10, 2.10, 14.2 and 14.3.
[11] Draft Decision, paragraph 2.8.

6. The IE SA stated in its Draft Decision that it was satisfied that the IE SA is the LSA, within the meaning of the GDPR, for TIC, as controller in respect of the cross-border processing of personal data carried out by TIC that was the subject of the breach[12].

7. The following table presents a summary timeline of the events part of the procedure leading to the submission of the matter to the consistency mechanism:

26.12.2018	Twitter, Inc., a company incorporated in the USA receives a **bug report** through their bug bounty programme. The report was sent by a third party contractor managing the bug bounty programme (Contractor 1) to the third party contractor engaged by Twitter, Inc. to search for and assess bugs (Contractor 2).
29.12.2018	Contractor 2 shares the result with Twitter, Inc. via a JIRA ticket.
02.01.2019	Twitter, Inc.'s Information Security Team reviews the JIRA ticket and decides it was not a security issue but that it might be a data protection issue.
02.01.2019	Twitter, Inc.'s Legal Team is notified.
03.01.2019	Twitter, Inc.'s Legal Team decides that the issue should be treated as an incident.
04.01.2019	Twitter, Inc. triggers the **incident response process**, but due to a mistake in applying the internal procedure, the Global DPO is not added as 'watcher' to the ticket. Therefore, they are not notified.
07.01.2019	The Global DPO is notified of the Data Breach during a meeting.
08.01.2019	TIC **notifies the Breach** to the IE SA using the IE SA's cross-border breach notification form.
22.01.2019	The scope and legal basis of the inquiry were set out in the notice of commencement of inquiry that was sent to TIC on 22 January 2019. The IE SA commences the inquiry and requests information from TIC.
28.05.2019 to 21.10.2019	Inquiry Report stage: • the IE SA prepares a **draft inquiry report** and issues it to TIC to allow TIC to make submissions in relation to the draft inquiry report; • TIC provides its submissions in relation to the draft inquiry report; • the IE SA requests clarifications in relation to the submissions made by TIC; • the IE SA issues its final inquiry report.
21.10.2019	The IE SA commences the decision-making stage.
11 and 28.11.2019	The IE SA corresponds with TIC and invites TIC to make further written submissions.
2.12.2019	TIC makes further submissions to the IE SA in response to the IE SA's correspondence of 11 and 28 November 2019.

[12] The IE SA has confirmed that its assessment in this regard was based both on its determination that (1) TIC, as the provider of the Twitter service in the EU/EEA, is the relevant controller and (2) that TIC's main establishment in the EU is located in Dublin, Ireland, where decisions on the purposes and means of processing of personal data of Twitter users in the EU/EEA are taken by TIC, in accordance with Article 4(16) GDPR. Draft Decision, paragraphs 2.2-2.3.

14.03.2020	The IE SA issues a **Preliminary Draft Decision** (hereinafter "**the Preliminary Draft Decision**") to TIC, concluding that TIC infringed Articles 33(1) and 33(5) GDPR; hence intends to issue a reprimand in accordance with Article 52(2) GDPR and an administrative fine in accordance with Article 58(2)(i) and Article 83(2) GDPR.
27.04.2020	TIC provides submissions on the Preliminary Draft Decision to the IE SA.
27.04.2020 - 22.05.2020	The IE SA takes account of TIC's submissions in relation to the Preliminary Draft Decision and prepares its draft decision for submission to the CSAs in accordance with Article 60 GDPR.
22.05.2020 - 20.06.2020	The IE SA shares its Draft Decision with the CSAs in accordance with Article 60(3) GDPR. Several CSAs (AT SA, DE SA (represented by the DE-Hamburg SA), DK SA, ES SA, FR SA, HU SA, IT SA and NL SA) raise **objections** in accordance with Article 60(4) GDPR.
15.07.2020	The IE SA issues a Composite Memorandum setting out its replies to such objections and shares it with the CSAs (hereinafter, "**Composite Memorandum**"). The IE SA requests the relevant CSAs to confirm whether, having considered the IE SA's position in relation to the objections as set out in the Composite Memorandum, the CSAs intend to maintain their objections.
27 and 28.07.2020	In light of the arguments put forward by the IE SA in the Composite Memorandum, the DK SA informs the IE SA that it does not maintain its objection, and the ES SA informs the IE SA that it withdraws its objection in part. The other CSAs (i.e., the AT, DE, ES, FR, HU, IT and NL SAs), confirm to the IE SA that they maintain their remaining objections.
19.08.2020	The IE SA refers the matter to the EDPB in accordance with Article 60(4) GDPR, thereby initiating the dispute resolution procedure under Article 65(1)(a).

8. The IE SA triggered the dispute resolution process on the IMI on 19 August 2020. Following the submission by the LSA of this matter to the EDPB in accordance with Article 60(4) GDPR, the EDPB Secretariat assessed the completeness of the file on behalf of the Chair in line with Article 11(2) of the EDPB Rules of Procedure. The EDPB Secretariat contacted the IE SA for the first time on 20 August 2020, asking for additional documents and information to be submitted in IMI and requesting the IE SA to confirm the completeness of the file. The IE SA provided the documents and information and confirmed the completeness of the file on 21 August 2020. A matter of particular importance that was scrutinized by the EDPB Secretariat was the right to be heard, as required by Article 41(2)(a) of the Charter of the Fundamental Rights. On 4 September 2020, the Secretariat contacted the IE SA with additional questions in order to confirm whether TIC has been given the opportunity to exercise its' right to be heard regarding all the documents that were submitted to the Board for making its decision. On 8 September 2020, the IE SA confirmed that it was the case and provided the documents to prove it[13].

9. On 8 September 2020, the decision on the completeness of the file was taken, and it was circulated by the EDPB Secretariat to all the members of the EDPB.

[13] Amongst the documents sent by IE SA, there were emails from the Global DPO acknowledging receipt of the relevant documents.

10. The Chair decided, in compliance with Article 65(3) GDPR in conjunction with Article 11(4) of the EDPB Rules of Procedure, to extend the default timeline for adoption of one month by a further month on account of the complexity of the subject-matter.

2 CONDITIONS FOR ADOPTING A BINDING DECISION

11. The general conditions for the adoption of a binding decision by the Board are set forth in Article 60(4) and Article 65(1)(a) GDPR[14].

2.1 Objection(s) expressed by CSA(s) in relation to a draft decision

12. The EDPB notes that CSAs raised objections to the Draft Decision via the information and communication system mentioned in Article 17 of the EDPB Rules of Procedure, namely the Internal Market Information System. The objections were raised pursuant to Article 60(4) GDPR.

13. More specifically, objections were raised by CSAs in relation to the following matters:

- the competence of the LSA;
- the qualification of the roles of TIC and Twitter, Inc., respectively;
- the infringements of the GDPR identified by the LSA;
- the existence of possible additional (or alternative) infringements of the GDPR;
- the lack of a reprimand;
- the calculation of the proposed fine.

14. Each of these objections was submitted within the deadline provided by Article 60(4) GDPR.

2.2 The LSA does not follow the relevant and reasoned objections to the draft decision or is of the opinion that the objections are not relevant or reasoned

15. On 15 July 2020, IE SA provided to the CSAs a detailed analysis of the objections raised by the CSAs in the Composite Memorandum, where it outlined whether it considered the objections to be "relevant and reasoned" in accordance with Article 4(24) GDPR, and whether it decided to follow any of the objections[15].

16. More specifically, the IE SA considered that only the objections raised by CSAs in relation to the calculation of the fine meet the threshold put forward by Article 4(24) GDPR in so far as they relate to the compliance with the GDPR of the envisaged action in relation to the controller or processor and also set out the risks posed as regards the fundamental rights and freedoms of data subjects[16]. However, the IE SA concluded that it would not follow the objections, for the reasons set out in the Composite Memorandum and below.

17. The IE SA considered that the other objections expressed by CSAs were not "relevant and reasoned" within the meaning of Article 4(24) GDPR.

[14] According to Article 65(1)(a) of the GDPR, the Board will issue a binding decision when a supervisory authority has raised a relevant and reasoned objection to a draft decision of the LSA or the LSA has rejected such an objection as being not relevant or reasoned.
[15] The purpose of the document, as stated by the IE SA, was to facilitate further cooperation with the CSAs in relation to the Draft Decision and to comply with the requirement in Article 60(1) GDPR that the LSA shall cooperate with the other CSAs in an endeavour to reach consensus.
[16] Composite Memorandum, paragraph 5.59.

2.3 Conclusion

18. The case at issue fulfils all the elements listed by Article 65(1)(a) GDPR, since several CSAs raised objections to a draft decision of the LSA within the deadline provided by Article 60(4) GDPR, and the LSA has not followed objections or rejected them as not relevant or reasoned.

19. The EDPB is therefore competent to adopt a binding decision, which shall concern all the matters which are the subject of the relevant and reasoned objection(s), in particular whether there is an infringement of the GDPR[17].

20. All results in this decision are without any prejudice to any assessment or binding decision made in other cases by the EDPB, including with the same parties, depending on further and/or new findings.

3 THE RIGHT TO GOOD ADMINISTRATION

21. The EDPB is subject to Article 41 of the EU Charter of fundamental rights, in particular Article 41 (right to good administration). This is also reflected in Article 11(1) EDPB Rules of Procedure[18].

22. The EDPB decision "*shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them*" (Article 65(2) GDPR). It is not aiming to address directly any third party. However, as a precautionary measure to address the possibility that TIC might be affected by the EDPB decision, the EDPB assessed if TIC was offered the opportunity to exercise its right to be heard in relation to the procedure led by the LSA and in particular if all the documents received in this procedure and used by the EDPB to take its decision have already been shared previously to TIC and if TIC has been heard on them.

23. Considering that TIC has been already heard by the IE SA on all the information received by the EDPB and used to take its decision[19] and the LSA has shared to the EDPB the written observations of TIC, in line with Article 11(2) EDPB Rules of Procedure[20], in relation to the issues raised in this specific Draft Decision, the EDPB is satisfied that the Article 41 of the EU Charter of fundamental rights has been respected.

4 ON THE QUALIFICATION OF CONTROLLER AND PROCESSOR AND THE COMPETENCE OF THE LSA

4.1 Analysis by the LSA in the Draft Decision

24. The Draft Decision states that *"[i]n commencing the Inquiry, the appointed investigator within the [IE SA] [...] was satisfied that TIC is the controller, within the meaning of Article 4(7) of the GDPR, in respect of the personal data that was the subject of the Breach*", and that *"[i]n this regard, TIC confirmed that*

[17] Article 65(1)(a) in fine GDPR. Some CSAs raised comments and not per se objections, which were, therefore, not taken into account by the EDPB.
[18] EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020.
[19] IE SA Preliminary Draft Decision (14 March 2020); IE SA Draft Decision (22 May 2020); Objections and comments raised by CSAs (18-20 June 2020); Composite Memorandum prepared by the IE SA (15 July 2020); and the remaining comments and objections from the CSAs (27-28 July 2020).
[20] EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020.

it was the controller" in the data breach notification form and in the correspondence with the IE SA[21]. The Draft Decision further states that "*TIC also confirmed that the Breach had arisen in the context of processing carried out on its behalf by Twitter Inc., its processor*"[22] and "*TIC is the data controller for the personal data which is the subject of the Inquiry. TIC has an agreement in place with Twitter Inc. (its processor) to provide data processing services*"[23].

25. Additionally, the Draft Decision specifies that the IE SA was further satisfied that it was competent to act as LSA in respect of cross-border processing carried out by TIC, in relation to the personal data that was the subject of the Breach[24].

26. In this regard, the Draft Decision further states that TIC confirmed to the IE SA in notifying the Breach that it was "*an Irish company*", and the "*provider of the Twitter services in Europe*", and that TIC's Privacy Policy (updated on Jan 2016) informed users of the Twitter service in the EU that they had the right to raise concerns either with their local supervisory authority or with TIC's LSA, the IE SA[25].

27. The IE SA further included in the Draft Decision an excerpt from TIC's Annual Report and Financial Statements relating to the Financial Year ended 31 December 2018 specifying that the "*ultimate controlling party and the largest group of undertakings for which group financial statements are drawn up, and of which the company is a member, is Twitter, Inc., a company incorporated in the United States of America and listed on the New York Stock Exchange*"[26].

28. The IE SA initially faced uncertainty arising from the use of the terms "we" and "our" in the data breach notification form to refer interchangeably to TIC and Twitter, Inc. The IE SA sought clarifications in this regard and TIC indicated that employees of TIC and Twitter, Inc. habitually use "we" and "our" loosely to refer to the group by its name. In addition, TIC indicated that whilst TIC is the controller and makes decisions with respect to the purposes and means of data processing, it does not operate alone: "*TIC, and its employees, are part of […] the Twitter Group [….]. All employees of the Twitter Group use the same computer systems, they adhere to the same general policies…and work together to ensure the global round-the-clock support required to keep the Twitter platform operational*"[27].

4.2 Summary of the objections raised by the CSAs

29. In its objection, the **ES SA** states that **the Draft Decision does not sufficiently justify the role of TIC as controller**. The ES SA stresses that an assessment on which entity really decides on the purposes and means should be carried out, alongside with a critical analysis of all the facts which took place. According to the ES SA, the elements underlying the Draft Decision seem to suggest a conclusion that is different from the one reached by the IE SA. In particular, the ES SA considers that the decisions on the essential purposes of the data processing are actually taken by Twitter, Inc. The ES SA supported its reasoning by listing some factors that, in its view, could suggest that TIC does not decide on the purposes and means. First, the ES SA recalled that TIC is a subsidiary of Twitter, Inc. and highlighted that it would therefore be hard to understand how TIC could "*issue orders*" to Twitter, Inc. relating to processing of personal data of EEA users. According to the ES SA, TIC was never in the position to independently choose Twitter, Inc. as its processor and would not be able to replace it. Additionally,

[21] Draft Decision, paragraph 2.2.
[22] Draft Decision, paragraph 4.2.
[23] Draft Decision, paragraph 4.6.
[24] Draft Decision, paragraph 2.3.
[25] Draft Decision, paragraph 2.3.
[26] Draft Decision, paragraph 2.4.
[27] Draft Decision, paragraph 4.5.

the ES SA argued that Twitter, Inc. does not seem to act as processor due to the "*absence of a direct channel*" between the two companies in the management of data breach cases other than the sending of an email with the Global DPO in copy. Thirdly, the ES SA stated that it was not clear how TIC could have independently adopted or influenced the decisions leading to the correction of the IT bug in the system managed and controlled by Twitter, Inc., and that it was rather Twitter, Inc. who undertook decisions relating to the solution of the Breach, whose effects were not limited only to European users.

30. The **NL SA** also raised an objection regarding the legal qualification of TIC and Twitter, Inc. as respectively controller and processor. Specifically, the objection relates to the way the IE SA has argued that TIC is the sole controller in this case and that Twitter, Inc. is a processor acting on their behalf. The NL SA considers that assessment of controllership is a fundamental aspect of this case and therefore any conclusion regarding the role of controller, processor or joint controllers should be supported by legal and factual evidence. In its objection, **the NL SA essentially submits that the Draft Decision does not contain enough evidence to legally and factually establish the roles of the entities concerned,** in particular to support the conclusion (i) that TIC is the (sole) controller and (ii) that Twitter, Inc. is merely a processor acting under instruction of TIC for the operation of the global Twitter service and/or the purposes that are relevant in this case. According to the NL SA, the LSA should verify **whether the legal statements of the organisation and/or their privacy policy corresponds with their actual activities.** The NL SA requested the IE SA to include more information on and/or a description of the factors that lead to the determination of roles in the Draft Decision document itself. The NL SA also mentions, as examples of factors to take into account: instructions from TIC to Twitter, Inc., or other objective evidence or practical clues from daily operations as well as examples from written records such as a data processing agreement.

31. In its objection, the **DE SA** argues that **the relationship between Twitter, Inc. and TIC is not a controller-processor relationship**, but rather a joint-controllers relationship. The objection in first instance relies on the fact that Twitter, Inc. and TIC do not operate separate data processing systems. According to the DE SA, the basic system operated by Twitter, Inc. is modified based on decisions made by TIC and that for EEA users, whereas the main processing system stays the same. The DE SA also highlighted that all the employees of the group use the same computer system and adhere to the same general policies.

32. Finally, the **FR SA** raised an objection regarding the competence of the IE SA, stating that it seemed that the IE SA came to the conclusion that the decision-making power on the purposes and means of the processing at stake was exercised by TIC. According to the FR SA, **the Draft Decision does not clearly indicate that other elements than the company TIC's statements were taken into account by the authority to consider that this company had a decision-making power on the processing**. The FR SA also specified that the Draft Decision does not clearly indicate if the competence of the authority is based either on the fact that the company TIC should be considered as the controller, or because TIC should be regarded as the main establishment as defined by Article 4(16) GDPR. The FR SA concluded that in its current state the Draft Decision does not prevent the risk of forum shopping, which the one-stop-shop mechanism is meant to avoid. The FR SA invited the IE SA to provide more elements allowing to prove that the company TIC has a decision-making power regarding the purposes and means of the processing for the social network Twitter.

4.3 Position of the LSA on the objections

33. In its Composite Memorandum, the IE SA considered that an objection based on the role or designation of the parties as controller and processor and/or on the competence of the IE SA "*neither disputes the finding of an infringement nor the envisaged action and, therefore, does not satisfy the definition at*

Article 4(24)" and that it "*does not fall within the meaning of the definition of 'relevant and reasoned' objection under Article 4(24)*"[28]. The IE SA nevertheless analysed such objections and, in doing so, set out the factors which it had considered in determining TIC's status as controller and as main establishment. In this regard, the IE SA outlined (by way of summary[29]) the facts and legal analysis leading to its conclusion in respect of TIC's status as controller, in essence:

- Twitter's previous confirmation in 2015 that it proposed to make TIC in Ireland the controller for personal data of Twitter users in the EU[30];
- TIC's confirmation that it was controller for the personal data affected by the Breach both in notifying the Breach to the IE SA and during the course of the inquiry;
- TIC's confirmation that a data processing agreement is in place between it and Twitter, Inc. as its processor, which includes the provisions required by Article 28 GDPR;
- the interactions between TIC and Twitter, Inc. following 7 January 2019, when TIC (through its DPO) was actually made aware of the Breach, demonstrating according to the IE SA that TIC exercised control and decision-making authority over Twitter, Inc. concerning the remediation activities and notification of the Breach and in relation to the underlying processing of personal data affected by the Breach; and
- the actions of Twitter, Inc. when it was notified of the incident by Contactor 2, which according to the IE SA also support the status of the relationship between the two entities as one in which TIC exercised authority and bore responsibilities as the controller.

34. The IE SA then set out, by way of summary[31], the facts and legal analysis leading to its conclusion that TIC is main established in Ireland, in essence (beyond the points above):

- TIC's designation and declaration of itself as main establishment;
- TIC's confirmation in its Privacy Policy of its status as the relevant controller for personal data of Twitter users in the EU;
- TIC's place of central administration is in Dublin, where it has approximately 170 employees;
- TIC's direct employment of a global DPO for the purposes of the GDPR, the reporting line for the Global DPO within TIC and the Global DPO's representation of TIC on a range of privacy and data processing related activities, including the ability to veto data processing;
- the historical and ongoing supervision of TIC by the IE SA, during which it has been apparent that TIC determines the purposes and means for which personal data are processed within the EU.

The IE SA reiterated that, notwithstanding its response to the substance of the objections raised on the matters of competence and/or the designation of the parties, it did not consider that the objections in relation to these issues satisfied the definition of being a "relevant and reasoned objection" under Article 4(24) GDPR. The IE SA stated that, in light of both its assessment that these matters did not

[28] Composite Memorandum, paragraph 5.39.
[29] Composite Memorandum, paragraph 5.35.
[30] In this regard, the Composite Memorandum explains that TIC informed the IE SA on 8 April 2015 that it proposed to make TIC in Ireland the controller for the personal data of its users outside of the USA and that TIC notified this fact to other EU supervisory authorities in May 2015 (paragraph 5.15).
[31] Composite Memorandum, paragraph 5.36.

satisfy the definition under Article 4(24) GDPR, and in light of its demonstration that it had adequately addressed the questions of main establishment, its competence, and the controller, processor designation in its Draft Decision, it did not intend to follow the objections on these matters[32].

4.4 Analysis of the EDPB

4.4.1 Assessment of whether the objections were relevant and reasoned

35. The EDPB will begin its analysis of the objections raised by assessing whether the aforementioned objections are to be considered as a "relevant and reasoned objection" within the meaning of Article 4(24) GDPR.

36. Article 4(24) of the GDPR defines "relevant and reasoned objection" as an "*objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union*"[33].

37. As clarified in the Guidelines on the concept of a relevant and reasoned objection, an objection needs to be both "relevant" and "reasoned". In order for the objection to be "relevant", there must be a direct connection between the objection and the draft decision and it needs to concern either whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR[34].

38. According to the same Guidelines, an objection is "reasoned" when it is coherent, clear, precise and detailed in providing clarifications and arguments as to why an amendment of the decision is proposed and how the change would lead to a different conclusion[35] and when it clearly demonstrates the significance of the risks posed by the draft decision for fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union. The CSA should thus "*show the implications the draft decision would have for the protected values*", by "*advancing sufficient arguments to show that such risks are substantial and plausible*"[36]. The evaluation of the risks posed to the rights and freedoms of data subjects[37] can rely, *inter alia*, on the appropriateness, necessity, and proportionality of the measures envisaged[38] and on the possible reduction of future infringements of the GDPR[39].

[32] Composite Memorandum, paragraph 5.40.
[33] GDPR, Article 4(24).
[34] See also the EDPB Guidelines 9/2020 on the concept of relevant and reasoned objection, version for public consultation (hereinafter, "**Guidelines on RRO**"), paragraph 12, currently subject to public consultation, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en. The Guidelines were adopted on 8 October 2020, after the commencement of the inquiry by the IE SA relating to this particular case.
[35] Guidelines on RRO, paragraph 17 and 20.
[36] Guidelines on RRO, paragraph 37.
[37] The "data subjects" whose rights and freedoms may be impacted may be both those whose personal data are being processed by the controller/processor and those whose personal data may be processed in the future. Guidelines on RRO, paragraph 43.
[38] Guidelines on RRO, paragraph 42.
[39] Guidelines on RRO, paragraph 43.

39. In terms of content, the objection can, as a first alternative, concern the existence of an infringement of the GDPR. In this case, it should explain why the CSA disagrees as to whether the activities carried out by the controller or processor led to the infringement of a given provision of the GDPR, and to which infringement(s) specifically[40]. This objection may also include a disagreement as to the conclusions to be drawn from the findings of the investigation (e.g. by stating that the findings amount to an infringement other than / in addition to those already analysed)[41] or could go as far as identifying gaps in the draft decision justifying the need for further investigation by the LSA[42]. However, this is less likely to happen when the obligation for the LSA to cooperate with the CSAs and exchange all relevant information has been duly complied with in the time preceding the issuance of the draft decision[43]. Alternatively, the content of the objection can refer to the compliance of the action in relation to the controller or processor (corrective measure or other) envisaged in the draft decision with the GDPR, by explaining why the action foreseen is not in line with the GDPR[44].

40. The EDPB considers it possible for an objection concerning the existence of an infringement of the GDPR to concern the absence or insufficiency of assessment or reasoning (with the consequence that the conclusion in the draft decision is not adequately supported by the assessment carried out and the evidence presented, as required in Article 58 GDPR), as long as the whole threshold set forth by Article 4(24) GDPR is met and provided there is a link between the allegedly insufficient analysis and whether there is an infringement of the GDPR or whether envisaged action complies with the GDPR[45].

41. The EDPB considers that an objection concerning the role, or designation, of the parties can fall within the meaning of the definition of 'relevant and reasoned' objection under Article 4(24) GDPR, as this can affect the determination as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation. However, the EDPB considers that an objection on the competence of the supervisory authority acting as LSA should not be raised through an objection pursuant to Article 60(4) GDPR and falls outside of the scope of Article 4(24) GDPR[46].

a) Assessment of the objection raised by the NL SA

42. The objection raised by the NL SA in first instance relates to an "*absence or insufficiency of assessment or reasoning*"[47] leading to the conclusions drawn by the IE SA as to the legal qualification of TIC and Twitter, Inc. As the NL SA points out, the assessment of controllership is indeed a fundamental aspect of the case. A different conclusion as to the legal qualification of TIC and Twitter, Inc. would affect the

[40] Guidelines on RRO, paragraph 25.
[41] Guidelines on RRO, paragraph 27.
[42] Guidelines on RRO, paragraph 28 (which also specifies that "In this regard, a distinction must be made between, on one hand, own-volition inquiries and, on the other hand, investigations triggered by complaints or by reports on potential infringements shared by concerned supervisory authorities").
[43] Guidelines on RRO, paragraph 27.
[44] Guidelines on RRO, paragraph 33. This means that the objection may, *inter alia*, challenge the elements relied upon to calculate the amount of the fine (Guidelines on RRO, paragraph 34).
[45] Guidelines on RRO, paragraph 29.
[46] The procedure pursuant to Article 65(1)(b) GDPR is applicable in this case and can be launched at any stage, Guidelines on RRO, paragraph 31.
[47] Guidelines on RRO, paragraph 29. A relevant and reasoned objection concerning whether there is an infringement of the GDPR can concern "*insufficient factual information or description of the case at stake", a "disagreement as to the conclusions to be drawn from the findings of the investigation*" (Guidelines on RRO, paragraph 27) or refer to an "*absence or insufficiency of assessment or reasoning (with the consequence that the conclusion in the draft decision is not adequately supported by the assessment carried out and the evidence presented, as required in Article 58 GDPR)*" (Guidelines on RRO, paragraph 29).

conclusions of the supervisory authority, both in relation to the determination of an infringement of Article 33 GDPR, as well as the decision on the corrective measures resulting from the investigation.

43. The EDPB recalls that each legally binding measure adopted by a supervisory authority must give the reasons for the measure[48]. The determination as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, hinges on the correct identification of the roles of parties who shall be the subject of the measure. Therefore, a draft decision must contain sufficient legal and factual elements to support the proposed decision[49]. As a result, the EDPB considers that the objection raised by the NL SA concerns both "whether there is an infringement of the GDPR" and "whether or not the envisaged action complies with the GDPR".

44. While the EDPB considers that the objection of the NL SA is therefore relevant and includes legal arguments supporting its position, it does not put forward arguments how such consequences would pose significant risks for the rights and freedoms of data subjects and/or the free flow of data[50]. The EDPB recalls that the obligation to clearly demonstrate the significance of the risk posed by the draft decision - established by the GDPR - lies with the CSA[51]. While the possibility for CSAs to provide such demonstration may also depend on the degree of detail of the draft decision itself and on the previous exchanges of information[52], such a circumstance, where applicable, cannot completely absolve the CSA from the obligation to clearly set out why it considers that the draft decision, if left unchanged, results in significant risks for the rights and freedoms of individuals.

45. The EDPB finds that the objection raised by the NL SA does not clearly demonstrate the risks for the rights and freedoms of individuals as such. On this basis, the EDPB considers that the objection raised by the NL SA does not meet the requirements of Article 4(24) GDPR.

b) Assessment of the objection raised by the ES SA

46. The objection raised by the ES SA also challenges the sufficiency of the assessment or reasoning in relation to the conclusions drawn by the IE SA as to the legal qualification of TIC and Twitter, Inc. respectively. The objection also makes clear that the correct qualification of the TIC and Twitter, Inc. is key for determining their respective responsibilities, as well as for the competence of the IE SA. As a result, the EDPB also considers that the objection raised by the ES SA concerns both "whether there is an infringement of the GDPR" and "whether or not the envisaged action complies with the GDPR". The objection of the ES SA also sets out why it considers that a change to the Draft Decision is necessary and how the change would lead to a different conclusion.

47. While the EDPB considers that the objection of the ES SA is therefore relevant and includes legal arguments supporting its position, it does not clearly articulate why the decision, if left unchanged in this respect, would pose significant risks for the rights and freedoms of data subjects and, where applicable, the free flow of personal data. On this basis, the EDPB considers that the objection raised by the ES SA does not meet the requirements set out in Article 4(24) GDPR.

[48] Recital (129) GDPR.
[49] Such information is also necessary to ensure the effectiveness of the cooperation and consistency mechanism, so as to allow CSAs to make an informed decision on whether or not to agree or express a relevant and reasoned objection.
[50] Guidelines on RRO, paragraph 19.
[51] Guidelines on RRO, paragraph 36 and Article 4(24) GDPR.
[52] Guidelines on RRO, paragraph 36.

c) Assessment of the objection raised by the DE SA

48. While the objections expressed by the NL and ES SA primarily relate to an "absence of reasoning" justifying the conclusion that TIC acts as (sole) controller, the DE SA disagrees as to the conclusions to be drawn from the findings of the investigation[53]. In particular, the DE SA considers that the factual elements included in the file are sufficient to justify the conclusion that Twitter, Inc. does not qualify as a processor, but rather as a joint controller, together with TIC.

49. In its objection, the DE SA also sets out why the qualification of the parties is relevant to the determination of "whether there is in infringement". In particular, the DE SA argues that the legal assessment of the relationship between Twitter, Inc. and TIC affects the determination of the moment of becoming aware of the Breach. According to the DE SA, knowledge must be equally attributed to both (joint) controllers in light of Article 26(1) GDPR. Taking this into account, the DE SA argues that the relevant date when TIC as joint controller obtained knowledge (or rather should have obtained knowledge) needs to be reconsidered by the IE SA.

50. The EDPB considers that the objection raised by the DE SE clearly sets out why changing the Draft Decision is considered necessary and how the objection, if followed, would lead to a different conclusion. That being said, the EDPB does not find that the objection raised by the DE SA includes a clear statement regarding the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects in relation to the qualification of the parties as such. On this basis, the EDPB considers that the objection raised by the DE SA does not meet the requirements set out in Article 4(24) GDPR.

d) Assessment of the objection raised by the FR SA

51. The FR SA in essence also considers that the Draft Decision suffers from "an absence or insufficiency of assessment or reasoning", in that it does not clearly indicate that other elements than TIC's own statements were taken into account by the IE SA to consider that TIC exercised decision-making power over the processing. Similar to the NL SA and ES SA, the FR SA also stresses the importance that the decision of the LSA is sufficiently reasoned. Different from the NL SA and ES SA, however, the FR SA focuses in its objection primarily on the importance of including such reasoning in establishing the competence of an authority of the LSA, in particular with a view of preventing forum shopping.

52. The EDPB recalls that a disagreement on the competence of the supervisory authority acting as LSA to issue a decision in the specific case should not be raised through an objection pursuant to Article 60(4) GDPR and falls outside of the scope of Article 4(24) GDPR[54]. The EDPB considers that the objection raised by the FR SA does not advance sufficient arguments to clearly demonstrate the significance of the risk for the rights and freedoms of data subjects posed by the Draft Decision. As a result, the EDPB considers that the objection raised by the FR SA does not amount to a relevant and reasoned objection within the meaning of Article 4(24) GDPR.

4.4.2 Conclusion

53. The EDPB considers that the aforementioned objections satisfy several of the criteria of Article 4(24) GDPR. Differently to the conclusion made by the IE SA, the EDPB considers that each of those objections satisfied the condition of referring alternatively to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this

[53] Guidelines on RRO, paragraph 27.
[54] Guidelines on RRO, paragraph 31. The Guidelines go on to state that unlike the objection pursuant to Article 60(4) GDPR, the procedure pursuant to Article 65(1)(b) GDPR is applicable at any stage.

Regulation. In addition, the EDPB considers that an objection based on the role, or designation, of the parties can in principle fall within the meaning of the definition of 'relevant and reasoned' objection under Article 4(24) GDPR.

54. However, as stated above, the aforementioned objections do not meet the threshold of providing a clear demonstration as to the significance of the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union.

55. In addition, as regards the aforementioned objection raised by the FR SA, in addition to not advancing sufficient arguments to clearly demonstrate the significance of the risk for the rights and freedoms of data subjects posed by the Draft Decision, the objection concerns a disagreement on the competence of the supervisory authority acting as LSA. The EDPB recalls that such disagreement should not be raised through an objection pursuant to Article 60(4) GDPR and falls outside of the scope of Article 4(24) GDPR[55].

56. As a result, the EDPB considers that the aforementioned objections do not meet the requirements set out in Article 4(24) GDPR.

57. As a consequence, **the EDPB does not take any position on the merit of any substantial issues raised by these objections**. **The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs**.

5 ON THE INFRINGEMENTS OF THE GDPR FOUND BY THE LSA

5.1 On the findings of an infringement of Article 33(1) GDPR

5.1.1 Analysis by the LSA in the Draft Decision

58. The IE SA concluded that TIC did not meet its obligations as a controller under Article 33(1) GDPR, which "*cannot be viewed in isolation and must be understood within the context of the broader obligations on controllers under the GDPR, in particular, the obligation of accountability under Article 5(2), the relationship between controllers and processors (Article 28), and the obligation to implement appropriate (and effective) technical and organisational measures*"[56].

59. With regard to the moment at which the controller became aware of the Breach, the Draft Decision concluded that in case the Breach is suffered by the processor, the controller becomes aware when it is notified of the Breach by the processor[57], but the controller must ensure that it has sufficient measures in place to facilitate this awareness[58]. Because TIC as controller was responsible for

[55] Guidelines on RRO, paragraph 31.
[56] Draft Decision, paragraph 6.20. See also Draft Decision, paragraphs 6.5, 6.7, and 6.13. The Draft Decision (paragraph 7.129 (i)) also states that the "*requirement under Article 33(1) [...] is predicated upon the controller ensuring that it has internal systems and procedures (and where applicable, systems and procedures in place with any external parties including processors) that are configured, and followed, so as to facilitate prompt awareness, and timely notification, of breaches*".
[57] Draft Decision, paragraph 7.129 (iii).
[58] Draft Decision, paragraph 7.98.

overseeing the processing operations carried out by its processor Twitter, Inc.[59], the Draft Decision stated that where the processor does not follow the procedure or the procedure fails otherwise the controller cannot excuse its own delayed notification on the basis of the processor's fault[60], as the performance by a controller of its obligation to notify cannot be contingent upon the compliance by its processor with its obligations under Article 33(2) GDPR[61]. The IE SA found that in these circumstances the controller must be considered as having constructive awareness of the personal Breach through its processor[62], and that such an interpretation reflects the responsibility and accountability of the controller in the GDPR[63].

60. According to the Draft Decision, therefore, TIC became actually aware of the Breach on 7 January 2019[64] but should have been aware of the Breach at the latest by 3 January 2019, since on that date Twitter, Inc. as processor first assessed the incident as being a potential data breach and the Twitter, Inc. legal team instructed that the incident be opened[65]. The Draft Decision also stated that even in the particular circumstances of this situation (where earlier delays had also arisen[66], any arrangements in place with Twitter, Inc. should have enabled this[67]. Instead, due to the "ineffectiveness of the process" in the "particular circumstances" of the case at stake and/or "a failure by [the processor's] staff to follow its incident management process" there was a delay leading to the controller being notified only on 7 January 2019[68]. This led to the infringement of Article 33(1) GDPR even if less than 72 hours elapsed between the moment at which TIC became actually aware of the Breach (7 January 2019) and the notification (8 January 2019).

5.1.2 Summary of the objections raised by the CSAs

61. The **FR SA** raised an objection stating that the findings do not correspond to an infringement of Article 33(1) GDPR, but rather of Article 28 or Article 32 GDPR, which set out the obligations of the controller when it decides to have recourse to a processor. This argument relies on the fact that the finding of the infringement of Article 33(1) is mainly based on the failures in the application of the procedure

[59] Draft Decision, paragraph 7.129 (iv).
[60] Draft Decision, paragraph 7.129 (iv).
[61] Draft Decision, paragraph 7.129 (x).
[62] Draft Decision, paragraph 7.129 (v).
[63] Draft Decision, paragraph 7.98. According to the Draft Decision, an alternative interpretation leading to consider that a controller is only "aware" when informed by its processor, leaves a significant lacuna in the protection provided by the GDPR, as it could result in the controller avoiding responsibilities even in case of major delays if it showed it satisfied its obligations in choosing a processor and having proper systems in place, but such systems were disregarded by the processor (Draft Decision, paragraph 7.99). The IE SA further outlined in the Draft Decision that "the alternative application of Article 33(1), and that which was suggested by TIC, whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2), would undermine the effectiveness of the Article 33 obligations on a controller [and that] [s]uch an approach would be at odds with the overall purpose of the GDPR and the intention of the EU legislator".
[64] Draft Decision, paragraph 7.129 (vi).
[65] Draft Decision, paragraph 7.129 (vi).
[66] In identifying the 3 January 2019 as the date on which TIC ought to have been aware of the breach, the IE SA also took into account that an earlier delay had arisen during the period from when the incident was first notified by the External Contractor (Contractor 2) to Twitter, Inc. on 29 December 2018 to when Twitter, Inc. commenced its review of same, on 2 January 2019. TIC confirmed, during the course of the inquiry, that this was "*due to the winter holiday schedule*".
[67] Draft Decision, paragraph 7.129 (ix).
[68] Draft Decision, paragraph 7.129 (vi).

established between TIC and its processor in case of a data breach, whereas Article 33(1) GDPR refers only to the obligation of the controller to notify data breaches to the competent authority.

62. The objections of the **DE SA**, instead, focused on the reasoning leading to the conclusion that Article 33(1) GDPR was infringed, without challenging such conclusion per se, and referred more specifically to the determination of the *dies a quo* of the 72-hour deadline.

63. The DE SA argued in its objection that the issue of the allocation of roles affects the determination of the moment of awareness of the Breach, as the knowledge of a breach must be equally attributed to both joint controllers. According to the DE SA, this may lead to considering 26 December 2018 as the date when TIC as joint controller got knowledge/should have got knowledge of the Breach.

5.1.3 Position of the LSA on the objections

64. With regard to the objection raised by the FR SA, the IE SA considers that it requests consideration of alternative provisions of the GDPR and that the request by CSAs to consider alternate provisions of the GDPR, would essentially seek to re-scope the Inquiry conducted[69]: the IE SA concluded that such an objection does not fall within the definition of "relevant and reasoned objection" for the purposes of Article 4(24) GDPR[70]. The IE SA also stressed its view that an infringement of Article 33(1) GDPR has occurred and did not propose to consider infringements of any other provisions of the GDPR as an alternative to Article 33(1)[71], underlining that expanding the range of the infringements to other GDPR obligations at the request of CSAs would "*jeopardise the entirety of the Inquiry and Article 60 process by exposing it to the risk of claims of procedural unfairness*"[72]. The IE SA also pointed out that it is examining TIC's compliance with its broader obligations under the GDPR in the context of another ongoing inquiry[73].

65. Concerning the objection raised by the DE SA, with specific regard to the determination of the moment of awareness of the breach, the IE SA submitted that even if a relationship of joint controllership did exist (a view that, as outlined above in Section 4.3, the IE SA did not share) it would not necessarily mean that awareness of the Breach could be equally attributed to both joint controllers[74].

5.1.4 Analysis of the EDPB

5.1.4.1 Assessment of whether the objections were relevant and reasoned

66. As recalled above (see Section 4.4.1), it is necessary to assess whether the objections raised by the CSAs meet the threshold set by Article 4(24) GDPR.

67. Although the objection of the **FR SA** is relevant, since it outlines a disagreement on whether an particular infringement of the GDPR has taken place in the specific case, and it includes legal arguments supporting the objection, it fails to meet the Article 4(24) GDPR standard because it does not include justifications concerning the consequences of issuing a decision without the changes proposed in the objection, and how such consequences would pose significant risks to the rights and freedoms of data

[69] Composite Memorandum, paragraph 5.45.
[70] Composite Memorandum, paragraph 5.45.
[71] Composite Memorandum, paragraph 5.47.
[72] Composite Memorandum, paragraph 5.44(c).
[73] Composite Memorandum, paragraph 5.44(d).
[74] Composite Memorandum, paragraph 5.34 (also referring to the CJEU judgment in *Wirtschaftsakademie*, C-210/16, paragraph 43).

subjects[75]. Thus, the objection cannot be said to "clearly demonstrate" the significance of the risks posed by the issuance of the Draft Decision (if it were to be issued as final) since it does not provide sufficient arguments as to why such rights and freedoms of data subjects with specific regard to the finding of an infringement of Article 33(1) (instead of Article 32 / 28) GDPR are substantial and plausible[76]. Therefore, the EDPB concludes the objection of the **FR SA** is not relevant and reasoned due to the lack of a clear demonstration of the risks as specifically required by the Article 4(24) GDPR.

68. Additionally, with regard to the **DE SA**'s objection specifically in relation to the determination of the *dies a quo* for the infringement of Article 33(1) GDPR as depending on the qualification of the parties, the EDPB would like to recall the analysis performed above in Section 4.4 and finds that the objection does not show the implications the Draft Decision with its current content - specifically concerning the reasoning underlying the finding of a Breach of Article 33(1) GDPR - would have for the protected values[77] (rights and freedoms of data subjects or, where applicable, free flow of personal data).

5.1.4.2 Conclusion

69. The EDPB considers that the aforementioned objections satisfied the condition of referring alternatively as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, but they do not clearly demonstrate the significance of the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union.

70. Therefore, the FR and DE SA's objections do not to meet the requirements in Article 4(24) GDPR[78].

5.2 On the findings of an infringement of Article 33(5) GDPR

5.2.1 Analysis by the LSA in the Draft Decision

71. In the Draft Decision, the IE SA found that TIC did not comply with its obligations under Article 33(5) GDPR to document the Breach, since the documentation furnished by TIC in the course of the inquiry was not considered to contain sufficient information and was not considered to contain a record or document of, specifically, a "personal data breach", as they amounted to "documentation of a more generalised nature"[79].

72. On a different note, the IE SA acknowledged that TIC fully cooperated during the inquiry (although this was not considered as a mitigating factor)[80].

5.2.2 Summary of the objections raised by the CSAs

73. The EDPB takes the opportunity to highlight, for the sake of clarity, that none of the objections raised challenged the conclusion that TIC infringed Article 33(5) GDPR.

---

[75] Guidelines on RRO, paragraph 19.
[76] Guidelines on RRO, paragraph 37.
[77] Guidelines on RRO, paragraph 37.
[78] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[79] Draft Decision, paragraph 10.46.
[80] Draft Decision, paragraph 14.50.

74. However, the **IT SA** raised an objection arguing that the finding related to the violation of Article 33(5) GDPR does not appear consistent with the reasoning and elaborations put forward by the LSA as the inadequacy of the documentation that was produced during such an extensive investigation, as based upon multiple interactions between the LSA and the controller, allegedly points to the controller's poor cooperation with the DPA. According to the IT SA, the finding in the Draft Decision that TIC provided full cooperation during the investigative phase should be reviewed as such full cooperation can only be considered to exist if adequate, exhaustive documentation is made available by the controller in a straightforward manner.

5.2.3 Position of the LSA on the objections

75. The IE SA is of the opinion that the obligation under Article 33(5) GDPR applies independently of the obligation under Article 31 GDPR to co-operate with the supervisory authority and of how TIC behaved towards, and interacted with, the LSA at the time that the latter initiated its regulatory activities regarding TIC's Breach[81]. The IE SA argued the deficiencies on how TIC documented the Breach do not necessarily correlate with a lack of cooperation on TIC's part[82]. In addition, the IE SA highlighted that TIC cooperated with the IE SA during the inquiry by responding to all requests for information and by providing all the requested documents, without seeking to disrupt or obstruct the inquiry in any way[83]. In any case, the IE SA did not consider TIC's cooperation as a mitigating factor[84]. For the above-mentioned reasons, the IE SA considered that it was "questionable" as to whether the objection raised by the IT SA is reasoned and relevant, since while it relates to an infringement of the GDPR it does not demonstrate how the IE SA's position on TIC's degree of cooperation results in risks posed by the draft decision regarding fundamental rights and freedoms of data subjects[85]. The IE SA concluded it would not follow said objection[86].

5.2.4 Analysis of the EDPB

5.2.4.1 Assessment of whether the objections were relevant and reasoned

76. The IT SA in its objection does not dispute that an infringement of Article 33(5) GDPR has occurred. A relevant and reasoned objection may question the reasoning underlying the conclusions reached by the LSA in the draft decision only insofar as such reasoning has a link with such conclusions, the objection is adequately reasoned. In this case, the objection does not clearly argue how following it could entail a change in the Draft Decision. Additionally, the objection does not meet the criteria outlined in Article 4(24) GDPR because it fails to clearly demonstrate the significance of the risks posed by the Draft Decision as it does not show the implications the alleged mistake in the Draft Decision would have for the protected values.

5.2.4.2 Conclusion

77. As the IT SA's objection does not meet the requirements of the Article 4(24) GDPR, the Board does not take a position on the merit of the substantial issues raised by this objection. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make

[81] Composite Memorandum, paragraph 5.87.
[82] Composite Memorandum, paragraph 5.87.
[83] Composite Memorandum, paragraph 5.87.
[84] Composite Memorandum, paragraph 5.87.
[85] Composite Memorandum, paragraph 5.88.
[86] Composite Memorandum, paragraph 5.88.

in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

6 ON POTENTIAL FURTHER (OR ALTERNATIVE) INFRINGEMENTS OF THE GDPR IDENTIFIED BY THE CSAS

6.1 Analysis by the LSA in the Draft Decision

78. Based on the information provided by TIC when it notified the Breach to the IE SA, the IE SA noticed that it appeared from the breach notification form that a period of in excess of 72 hours had elapsed from when TIC (as controller) became aware of the Breach[87]. For this reason, the IE SA decided to commence, on its own volition, an inquiry to examine whether TIC had complied with its obligations under Article 33(1) and Article 33(5) GDPR[88].

79. In order to determine whether TIC complies with its obligations under Article 33(1) GDPR, the IE SA considered them in the context of a controller's broader obligations, including those of accountability (Article 5(2) GDPR), of engagement of a processor (Article 28 GDPR), and in respect of the security of processing of personal data (Article 32 GDPR)[89]. However, if the IE SA considered the factors and factual matters that led to TIC's delay in being made aware of the Breach by its processor and ultimately in notifying the Breach, the IE SA did not consider whether or not TIC complied with any or each of these obligations other than for the purpose of assessing TIC's compliance with its obligations under Article 33(1) and Article 33(5) GDPR[90].

6.2 Summary of the objections raised by the CSAs

80. The DE, FR, HU, and IT SAs raised objections that TIC infringed other provisions of the GDPR in addition to, or instead of, Article 33(1) and Article 33(5) GDPR.

6.2.1 Infringement of Article 5(1)(f) GDPR on the principle of integrity and confidentiality

81. The **DE SA** raised an objection stating that the "underlying bug" in TIC's application that resulted in the Breach notified to the IE SA should have been considered by the IE SA in its Draft Decision, so as to determine whether this bug actually constituted a significant violation of the confidentiality of personal data, ultimately infringing Article 5(1)(f) GDPR, in addition to Article 33(1) and Article 33(5) GDPR.

82. The **HU SA** raised an objection stating that given the "bug" in TIC's application over the years and its serious nature affecting data security, the IE SA should investigate whether TIC also infringed Article 5(1)(f) GDPR on the principle of integrity and confidentiality.

6.2.2 Infringement of Article 5(2) GDPR on the principle of accountability

83. The **IT SA** raised an objection stating that the infringement of Article 33(1) GDPR highlights a much more severe violation of the accountability principle (under Article 5(2) GDPR), since the lack of

[87] Draft Decision, paragraph 2.11.
[88] Draft Decision, paragraph 2.11.
[89] Draft Decision, paragraphs 6.13-6.20, 7.111-7.112, 7.122-7.124.
[90] Draft Decision, paragraphs 6.13, 7.111, 7.122-7.124.

corporate policies to handle security incidents or the failure to comply with them shows that the measures implemented by the controller are inadequate to ensure compliance and to document it. The IT SA argued that these procedural shortcomings are highlighted by the Draft Decision, but the Draft Decision fails to make this the subject of a specific analysis. As this may affect the handling of future data breaches, too, the findings on whether TIC complied with Article 5(2) GDPR should also be part of the IE SA's final decision according to the IT SA. The IT SA also considered that the infringement of Article 5(2) GDPR is confirmed by the controller's inability to state the exact number and nature of the personal data affected, or the total number of data subjects involved.

6.2.3 Infringement of Article 24 GDPR on the responsibility of the controller

84. The **DE SA** raised an objection stating that the Draft Decision is not clear on why the IE SA did not assess if the significant violation of the confidentiality of personal data caused by an "underlying bug" is due to an infringement of the requirements of Article 24 GDPR.

6.2.4 Infringement of Article 28 GDPR on the relationship with processors

85. The **FR SA** expressed an objection stating that TIC did not respect the obligation of the controller to verify the validity of the procedures set up by its processor. Therefore, the FR SA considers that there is no infringement of Article 33(1) GDPR, but of Article 28 GDPR instead (or Article 32 GDPR - see below Section 6.2.5). The FR SA argued that if TIC's processor is its parent company, "*it was all the more easy for TIC to verify the validity of the procedures set out by the parent company and to demand a correction if necessary*".

86. The **IT SA** expressed an objection stating that TIC's failure to involve the Global DPO in the Detection and Response Team of the processor (Twitter, Inc.), in spite of the fact that this practice was envisaged in TIC's internal policies, shows that the safeguards provided by the processor in terms of implementing the appropriate organisational measures under Article 28(1) GDPR are not extensive enough. In addition, the IT SA argued in its objections that the processor infringed its obligation to assist the controller, according to Article 28(3)(f) GDPR.

6.2.5 Infringement of Article 32 GDPR on the security of the processing

87. The **DE SA** raised objections stating that the IE SA should have examined if all appropriate technical and organisational measures (according to Article 32 GDPR) were complied with in this case, and whether infringements in this area should have been made the subject of these proceedings. The DE SA also argues that the Draft Decision is not clear on why the IE SA did not assess if the significant violation of the confidentiality of personal data caused by an "underlying bug" is due to an infringement of the requirements of Article 32 GDPR.

88. The **FR SA** expressed an objection concerning the legal characterisation of the facts carried out by the IE SA and stated that the TIC's failure to respect the obligation of the controller to verify the validity of the procedures set up by its processor corresponds to an infringement of Article 32 GDPR (or Article 28 GDPR - see above Section 6.2.4), rather than of Article 33(1) GDPR. The FR SA argued that if TIC's processor is its parent company, "*it was all the more easy for TIC to verify the validity of the procedures set out by its parent company and to demand a correction if necessary*".

89. The **HU SA** raised objections stating that given the "bug" in TIC's application over the years and its serious nature affecting data security, the IE SA should investigate whether TIC infringed also Article 32 GDPR on TIC's obligations of security of the processing.

6.2.6 *Infringement of Article 33(3) GDPR on the content of the notification of a personal data breach on security of processing*

90. The **DE SA** expressed objections stating that the IE SA's examination is lacking, with regard to the scope of the information to be provided in the case of a notification, which is stipulated as binding in Article 33(3) GDPR. Based on TIC's comments on the Breach they provided pursuant to Article 33(5) GDPR and on the description of the investigation of the facts of the case, TIC obviously did not fully comply with its documentation obligation when it first reported the Breach on 8 January 2019. The DE SA considered that there are therefore numerous indications that the result could also be an infringement of Article 33(3) GDPR.

6.2.7 *Infringement of Article 34 GDPR on the communication of a personal data breach to the data subject*

91. The **HU SA** raised objections stating that given the "bug" in TIC's application over the years and its serious nature affecting data security, the IE SA had to investigate whether TIC infringed also Article 34 GDPR on TIC's obligations of informing the data subjects about the Breach.

6.3 Position of the LSA on the objections

92. The LSA provided its response in respect of the objections concerning potential further (or alternative) infringements of the GDPR collectively in its Composite Memorandum shared with the CSAs. The LSA explained that it "*exercised its discretion [...] to confine the scope of the Inquiry to the consideration of two discrete issues, being whether TIC had complied with its obligations as a controller under Article 33(1) in respect of the notification of the Breach, and whether it had complied with its obligations under Article 33(5) to document the Breach*"[91]. The LSA relied on Section 110(1) of the Irish Data Protection Act 2018, which provides that the IE SA may "*cause such inquiry as it thinks fit to be conducted*"[92]. The purpose of the inquiry as described by the IE SA was thus "*solely to examine the circumstances surrounding TIC's apparent delayed notification of the Breach [...] and its documenting of the Breach*", an issue considered by the IE SA as "*of considerable importance given that, with close to 200,000 breaches notified in two years across the EU, there is a need for clarity on what is required under the breach notification and documentation requirements of the GDPR*"[93].

93. Within its Composite Memorandum[94], the IE SA maintains that objections raised in the context of Article 60(4) GDPR cannot have the effect of challenging the scope of an inquiry. In the case at hand, the LSA recalls that it informed TIC at the beginning of the inquiry that its purpose was to verify TIC's compliance with Article 33(1) and Article 33(5) GDPR in respect of its notification of a Breach to the LSA 8 January 2019. The whole inquiry process was therefore conducted within that scope, as well as the drafting of the Draft Decision, and TIC was afforded its right to be heard in that regard at each step of the procedure. Therefore, the LSA maintains that if it were to follow the CSAs' objections and include other infringements in its final decision "*on the basis of only the material contained in the Draft Decision*", this would result in jeopardising "*the entirety of the Inquiry and Article 60 process by exposing it to the risk of claims of procedural unfairness*"[95].

[91] Composite Memorandum, paragraph 1.7.
[92] Composite Memorandum, paragraph 1.5.
[93] Composite Memorandum, paragraph 1.9.
[94] Composite Memorandum, paragraph 5.44.
[95] Composite Memorandum, paragraph 5.44(c).

94. Furthermore, the LSA explains that it has another ongoing inquiry in relation to other data breaches notified to the LSA by TIC prior to the notification that concerns the case at hand. In that other inquiry, initiated before the one at hand, the LSA highlights that the scope of investigation concerns possible non-compliance with "*inter alia, Articles 5, 24, 25, 28, 29 and 32*" GDPR[96]. The LSA considers that this parallel inquiry is indeed assessing TIC's compliance with its broader obligations under GDPR to determine if compliance insufficiencies caused the data breaches. Consequently, the LSA is of the position that the CSAs will have the possibility to consider such possible infringements in the context of that other inquiry, as they will be consulted on its Draft Decision, in accordance with Article 60(4) GDPR[97].

95. TIC submitted that, since the Draft Decision states that "*a detailed examination of the technical and organisational measures is beyond the scope of the inquiry*"[98], it "*would not be reasonable or appropriate, and would offend well-established principles of natural justice, if the Decision were to make findings or impose sanctions on TIC in respect of obligations and principles which did not form part of the DPC's investigation, since TIC has not had an opportunity to address any concerns which the DPC or CSAs may have about TIC's processes in these areas*"[99].

6.4 Analysis of the EDPB

6.4.1 Assessment of whether the objections were relevant and reasoned

6.4.1.1 Infringement of Article 5(1)(f) GDPR on the principle of integrity and confidentiality

96. The EDPB notes that the **DE SA**'s objection on Article 5(1)(f) GDPR is referring to whether there is an infringement of the GDPR by expressing a disagreement as to the conclusions to be drawn from the findings of the investigation. The objection also put forward arguments to support the conclusion that compliance with Article 5(1)(f) GDPR should be assessed. The DE SA's objection clearly demonstrates the significance of the risks posed by the Draft Decision for the rights and freedoms of data subjects, in particular by highlighting that the facts amount to a "significant" and "substantial" breach of the confidentiality of personal data and that a large number of persons were concerned for a substantial period of time. Furthermore the DE SA also argued that there were indications to consider the existence "systemic error", which would have required a deeper scrutiny beyond the single specific bug involved.

97. The **HU SA**'s objection can also be considered as relevant as it concerns whether there is an infringement of the GDPR. Additionally it (only) briefly makes reference to factual arguments supporting the need to assess this additional provision (the duration of the bug and its serious nature affecting data security), but does not "clearly demonstrate" the significance of the risks posed by the Draft Decision for risks to the rights and freedoms of individuals as it does not put forward arguments

[96] Composite Memorandum, paragraph 1.10.
[97] Composite Memorandum, paragraph 5.44(d).
[98] Draft Decision, paragraph 7.19.
[99] "Representations in response to objections and comments from CSAs" submitted by TIC (14 August 2020), paragraph 4.1. The EDPB wishes to highlight that the objections raised by the CSAs were brought to TIC's attention by the IE SA, and TIC issued the aforementioned representations on the objections, which were taken into account by the IE SA prior to the initiation of the Article 65 procedure and are part of the file under consideration of the EDPB in the context of this procedure. See also footnote 19.

or justifications concerning the consequences of issuing a decision without the changes proposed in the objection[100].

98. As a consequence the EDPB considers the objection raised by the DE SA in relation to the potential additional infringement of Article 5(1)(f) GDPR to be relevant and reasoned for the purposes of Article 4(24) GDPR, but considers the HU SA's objection in relation to the same topic does not meet the requirements of Article 4(24)[101].

99. The EDPB will assess the merits of the substantial issues raised by the DE SA objection in relation to the potential additional infringement of Article 5(1)(f) GDPR (see section 6.4.2 below).

6.4.1.2 Infringement of Article 5(2) GDPR on the principle of accountability

100. The objection raised by the **IT SA** is to be considered "relevant" since if followed, it would lead to a different conclusion as to whether there is an infringement of the GDPR[102]. More specifically, it includes a "disagreement as to the conclusions to be drawn from the findings of the investigation", since it states that the "*findings amount to the infringement of a provision of the GDPR [...] in addition to [...] those already analysed by the draft decision*"[103].

101. Additionally, the objection is "reasoned" as it includes clarifications as to why the amendment of the decision is proposed[104]: the proposed change relies on the "*lack of formalised corporate policies to handle security incidents [...] or the failure to comply with said policies*", on the fact that such "*procedural shortcomings are highlighted by the [IE SA] repeatedly*" in the Draft Decision, and on the controller's inability to state the exact number and nature of the personal data / data subjects affected.

102. The **IT SA** clearly demonstrated the significance of the risks posed by the Draft Decision for fundamental rights and freedoms of data subjects, by showing the "implications the draft decision would have for the protected values"[105] and more specifically the "impact on the rights and freedoms of data subjects whose personal data might be processed in the future"[106]: the objection did so by arguing that the aspects mentioned are "*structural in nature as regards the controller's organization" and "bound to produce effects not simply on the case at issue, but also on the handling of any personal data breach that may occur in the future*".

103. As a consequence, the IT SA's objection on Article 5(2) GDPR meets the requirements set out in Article 4(24) GDPR. The EDPB will therefore analyse the merits of the substantial issues raised by this objection[107].

[100] Guidelines on RRO, paragraph 19.
[101] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by the HU SA's objection. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[102] Guidelines on RRO, paragraph 13.
[103] Guidelines on RRO, paragraph 27.
[104] Guidelines on RRO, paragraph 17.
[105] Guidelines on RRO, paragraph 37.
[106] Guidelines on RRO, paragraph 43.
[107] See section 6.4.2 below.

6.4.1.3 Infringement of Article 24 GDPR on the responsibility of the controller

104. The **DE SA**'s objection specifically refers to Chapter 5 "Issues for determination" of the Draft Decision[108], and objects to the Draft Decision as to whether Article 24 GDPR was also infringed by TIC[109]. It relies on the facts[110] set out in the Draft Decision that "*if a Twitter user with a protected account, using Twitter for Android, changed their email address the bug would result in their account being unprotected*"[111]. and their protected tweets were made publicly available via the service. More precisely, the DE SA is questioning why the IE SA did not examine, in the Draft Decision, the causes of the Breach, in particular in light of Article 24 GDPR, and why the IE SA did not explain in the Draft Decision why it did not perform such examination.

105. The DE SA argues that given that the Breach notification revealed "*deficiencies in compliance with the GDPR, ... [a] company that is not capable by own means and resources, by inspections of internal or external security teams to find a bug of that prominence and scope should be subject to a deeper scrutiny regarding its security and data processing setup, beyond the single specific bug involved*".

106. According to the DE SA, a higher scrutiny into TIC's data processing setup "*could result, as the case may be, in an order to the controller to bring processing operations into compliance with the provisions of the GDPR. The case at hand fails to reflect this task. This makes it all the more urgent to examine the corrective powers under Article 58(2) GDPR in this context*".

107. Therefore, the DE SA pointed out what it considered as an absence of assessment, with the consequences that the conclusions drawn from the findings of the investigation by the LSA could be different[112].

108. The DE SA's objection that "*According to Art. 83 (1) GDPR, fines must be "effective, proportionate and dissuasive in each individual case. A sanction is effective and dissuasive if, on the one hand, it is suitable as a general preventive measure to deter the general public from committing infringements and to affirm the general public's confidence in the validity of Union law, but, on the other hand, it is also suitable as a preventive measure to deter the offender from committing further infringements*". Consequently, the DE SA demonstrates how not changing the Draft Decision to include an assessment of compliance with Article 24 GDPR would pose significant risks for the fundamental rights and freedoms of data subjects[113].

109. In its Guidelines on RRO, the EDPB accepts that an objection may challenge the conclusion of the LSA, by considering that the LSA's findings actually lead to the conclusion that another provision of the GDPR has been infringed in addition to or instead of the provision identified by the LSA[114]. The EDPB considers that this is precisely the essence of the DE SA's objection, hence not preventing it from being relevant and reasoned.

110. Additionally, the DE SA's objection clearly demonstrates the significance of the risks posed by the Draft Decision for the rights and freedoms of data subjects, including by highlighting that a large number of persons were concerned for an equally substantial period of time, reflecting a systemic error that calls

[108] Guidelines on RRO, paragraph 20.
[109] Guidelines on RRO, paragraph 12.
[110] Guidelines on RRO, paragraph 14.
[111] Draft Decision, paragraph 2.7.
[112] Guidelines on RRO, paragraph 29.
[113] Guidelines on RRO, paragraph 19.
[114] Guidelines on RRO, paragraph 27.

for deeper scrutiny, looking beyond the single specific bug involved. As a consequence, the DE SA's objection on Article 24 GDPR meets the threshold set out in Article 4(24) GDPR.

111. In light of the assessment above, the EDPB considers that the DE SA's objection relating to a possible infringement of Article 24 GDPR is relevant and reasoned in accordance with Article 4(24) GDPR. As a consequence, the EDPB is assessing the merit of the substantial issues raised by this objection (see section 6.4.2 below).

6.4.1.4 Infringement of Article 28 GDPR on the relationship with processors

112. The **FR SA**'s objection specifically refers to paragraphs 7.129 iii), iv) and v) of the Draft Decision[115], and objects to the Draft Decision as to whether Article 28 GDPR was infringed by TIC instead of Article 33(1) GDPR[116]. It relies on the facts[117] set out in the Draft Decision and on the findings by the LSA that "TIC did not respect the obligation of the controller to verify the validity of the procedures set up by its processor".

113. According to the FR SA, since Article 28(3)(h) GDPR sets forth the controller's duties when it uses a processor, the findings should have led the LSA to the conclusion that Article 28(3)(h) GDPR was infringed, instead of Article 33(1) GDPR. Ultimately, it means, for the FR SA, that the sanction issued in fine should address different infringements.

114. In its Guidelines on RRO, the EDPB accepts that an objection may challenge the conclusion of the LSA, by considering that the LSA's findings actually lead to the conclusion that another provision of the GDPR has been infringed in addition to or instead of the provision identified by the LSA[118]. The EDPB considers that this is precisely the essence of the FR SA's objection, hence not preventing it from being relevant. The objection also adequately puts forward arguments supporting the conclusion proposed. At the same time, the EDPB notes that the FR SA's objection does not clearly demonstrate the significant risks posed by the Draft Decision for the fundamental rights and freedoms of data subjects with specific regard to the failure to conclude on the infringement of this specific provision[119]. In light of this assessment, the EDPB considers that the FR SA's objection relating to a possible infringement of Article 28 GDPR instead of Article 33(1) GDPR is not relevant and reasoned in accordance with Article 4(24) GDPR[120].

115. The IT SA's objects to the Draft Decision as to whether Article 28 GDPR, *inter alia*, was infringed by TIC in addition to Article 33(1) GDPR[121].

116. The IT SA relies on the facts set out in the Draft Decision and on the findings by the LSA that whilst the involvement of the Global DPO in the Detection and Response Team of its processor, Twitter, Inc., is envisaged in TIC's internal policies, in practice, the Global DPO was not involved. The IT SA also notes that Twitter, Inc., as the processor, failed to assist TIC.

---

[115] Guidelines on RRO, paragraph 20.
[116] Guidelines on RRO, paragraph 12.
[117] Guidelines on RRO, paragraph 14.
[118] Objection Guidelines on RRO, paragraph 27.
[119] Guidelines on RRO, paragraph 29.
[120] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[121] Guidelines on RRO, paragraph 12.

117. According to the IT SA, with Article 28(1) GDPR requiring controllers to only use processors providing sufficient guarantees to implement appropriate technical and organisational measures, and Article 28(3)(f) GDPR requiring the contract between the controller and the processor to stipulate that the processor assist "the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of the processing and the information available to the processor"; the findings should have led the LSA to the conclusion that Article 28(1) and Article 28(3)(f) GDPR were also infringed.

118. The EDPB considers that the IT objection in relation to Article 28(1) and Article 28(3)(f) GDPR it is to be considered "relevant" since if followed, it would lead to a different conclusion as to whether there is an infringement of the GDPR[122]. More specifically, it includes a "disagreement as to the conclusions to be drawn from the findings of the investigation", since it states that the "findings amount to the infringement of a provision of the GDPR [...] in addition to [...] those already analysed by the draft decision"[123].

119. Additionally, according to the EDPB, the objection is "reasoned" as it includes clarifications as to why the amendment of the decision is proposed[124]: the proposed change relies on the fact that the controller did not comply with its internal policies according to which TIC's DPO should be involved. Besides, the objection raises the point that the processor failed to comply with its contractual obligation to assist the controller, in accordance with Article 28(3)(f) GDPR.

120. However, the EDPB notes that the IT SA's objection relating to Article 28(1) and Article 28(3)(f) GDPR does not clearly demonstrate significant risks posed by the Draft Decision for the fundamental rights and freedoms of data subjects[125]. As a consequence this objection raised by the IT SA does not meet the requirements set out in Article 4(24) GDPR[126].

6.4.1.5 Infringement of Article 32 GDPR on the security of the processing

121. The **DE SA**'s objection, if followed, would entail a change leading to a different conclusion as to whether there is an infringement of the GDPR, since it identified a "*disagreement as to the conclusions to be drawn from the findings of the investigation*"[127] by pointing out that the findings may indicate an infringement also of Article 32 GDPR. Thus, the EDPB therefore considers that there is a link between the content of the objection and the potential different conclusion[128]. In addition, this objection is related to specific legal and factual content of the Draft Decision[129].

122. Additionally, the DE SA's objection clearly demonstrates the significance of the risks posed by the Draft Decision for the rights and freedoms of data subjects, in particular by highlighting that the facts amount to a "significant" and "substantial" breach of the confidentiality of personal data and that a large number of persons were concerned for a substantial period of time. Furthermore the DE SA also argued

[122] Guidelines on RRO, paragraph 13.
[123] Guidelines on RRO, paragraph 27.
[124] Guidelines on RRO, paragraph 17.
[125] Guidelines on RRO, paragraph 29.
[126] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[127] Guidelines on RRO, paragraph 28.
[128] Guidelines on RRO, paragraph 13.
[129] Guidelines on RRO, paragraph 14.

that there were indications to consider the existence of a "systemic error", which would have required a deeper scrutiny beyond the single specific bug involved.

123. In light of the assessment above, the EDPB considers that the DE SA's objection relating to a possible infringement of Article 32 GDPR is relevant and reasoned in accordance with Article 4(24) GDPR. As a consequence, the EDPB is assessing the merit of the substantial issues raised by this objection (see point 6.4.2 below).

124. As regards the **FR SA**'s objection, the EDPB considers it as meeting the criterion of "relevant" because if the LSA would have followed it, there would be a different conclusion as to whether there is an infringement of the GDPR[130]. The FR SA's objection is based on the reasoning provided by the IE SA in its Draft Decision and this reasoning is linked with conclusion as to whether an infringement of the GDPR has been correctly identified[131]. The EDPB recalls that the CSA has to present the facts allegedly leading to a different conclusion[132] and notes that in the case at stake the objection analyses the facts that would lead to the violation of Article 32(1)(d) GDPR, instead of violation of Article 33(1) GDPR, and does so in a coherent, clear and precise way, by clearly indicating which parts of the decision of the IE SA it disagrees with. The FR SA's objection is clearly relevant by outlining a disagreement on whether an infringement of the GDPR has taken place. However, the FR SA's objection only succinctly explains the reasons for its proposed change and does not clearly demonstrate the significance of the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects in relation to the failure to find an infringement of Article 32 GDPR. As a consequence this objection raised by the FR SA does not meet the requirements set out in Article 4(24) GDPR[133].

125. The **HU SA**'s objection also referred to whether there is an infringement of the GDPR, arguing that the possible infringement of the principle of integrity and confidentiality should also be investigated. The HU SA's objection is clearly relevant by outlining that an additional provision of the GDPR (i.e. Article 32 GDPR) should have been investigated. However, the HU SA does not explain how the Draft Decision would pose such risks, nor does it fully explain why specific aspects of the decision are deficient in its point of view[134]. The HU SA's objection fails to meet the criterion of providing sound reasoning for its objection, by referring to legal or factual arguments. On the contrary, it just recommends that the IE SA would also need to investigate the controller's compliance with Article 32 GDPR. As a consequence this objection raised by the HU SA does not meet the requirements set by Article 4(24) GDPR[135].

6.4.1.6 Infringement of Article 33(3) GDPR on the content of the notification of a personal data breach on security of processing

126. The **DE SA** considers that the Draft Decision indicates that Article 33(3) GDPR could be infringed in addition to other provisions of GDPR. In that sense, it is about "whether there is an infringement" of

[130] Guidelines on RRO, paragraph 13.
[131] Guidelines on RRO, paragraph 16.
[132] Guidelines on RRO, paragraph 18.
[133] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.
[134] Guidelines on RRO, paragraph 18.
[135] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

the GDPR, and that it has not been examined and addressed by the Draft Decision. Hence, the DE SA considers that, if changed, the Draft Decision would lead to the conclusion of additional infringements of GDPR.

127. However, the DE SA does not clearly demonstrate the significant risks posed by the Draft Decision to the fundamental rights and freedoms of data subjects. As a consequence, the DE SA's objection on Article 33(3) GDPR fails to meet the requirements set out in Article 4(24) GDPR[136].

6.4.1.7 Infringement of Article 34 GDPR on the communication of a personal data breach to the data subject

128. The **HU SA** considers that the Draft Decision indicates that Article 34 GDPR could be infringed in addition to other provisions of GDPR, especially in light of the fact that the bug lasted over the years, and given the serious nature affecting the controller's security. In that sense, it is about "whether there is an infringement" of the GDPR, and that it has not been examined and addressed by the Draft Decision. Hence, the HU SA considers that, if changed, the Draft Decision would lead to the conclusion of additional infringements of GDPR.

129. However, the HU SA does not clearly demonstrate the significant risks posed by the Draft Decision to the fundamental rights and freedoms of data subjects. As a consequence, the HU SA's objection on Article 34 GDPR do not meet the requirements set out in Article 4(24) GDPR[137].

6.4.2 Assessment of the merits of the substantial issue(s) raised by the relevant and reasoned objections and conclusion

130. The Board now analyses the objections found being relevant and reasoned - in particular the DE SA's objections on Article 5(1)(f), Article 24 and 32 GDPR, as well the IT SA's objection on Article 5(2) GDPR - as well as the LSA's response to those objections and the TIC submissions.

131. In accordance with Article 65(1)(a) GDPR, in the context of a dispute resolution procedure the EDPB shall take a binding decision concerning all the matters which are the subject of the relevant and reasoned objections, in particular whether there is an infringement of the GDPR. The EDPB can (and must) make a binding decision which shall whenever possible, taking into account the elements of the file and the respondent's right to be heard, provide a final conclusion on the application of the GDPR in relation to the case at hand. The LSA will then be obliged to implement the changes in its final decision.

132. The Board considers that the available factual elements included in the Draft Decision and in the objections are not sufficient to allow the EDPB to establish the existence of further (or alternative) infringements of Article 5(1)(f), 5(2), 24 and 32 GDPR.

133. The Board considers that, as a general matter, the limited scope of the inquiry by the IE SA - focused since the outset only on whether there were infringements by TIC of Article 33(1) and 33(5) GDPR -

[136] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

[137] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

directly affects the remit of the investigation and further fact finding, as well as the ability for CSAs to put forward sufficient elements for the EDPB to sustain the objections.

134. The EDPB recalls the duty for the LSA to "endeavour to reach consensus" with the CSAs (Article 60(1) GDPR) and to provide, without delay, the CSAs with "the relevant information" on the matter (Article 60(3) GDPR). Even in case of an own-volition inquiry, the Guidelines on reasoned and relevant objections state that LSA "should seek consensus regarding the scope of the procedure (i.e. the aspects of data processing under scrutiny) prior to initiating the procedure formally"[138], including in the context of a possible new proceeding.

135. Whilst the EDPB considers that SAs enjoy certain degree of discretion to decide how to frame the scope of their inquiries, the EDPB recalls that one of the main objectives of the GDPR is to ensure consistency throughout the European Union, and the cooperation between the LSA and CSAs is one of the means to achieve this. The EDPB also recalls the existence of a full range of the cooperation tools provided for by the GDPR (including Articles 61 and 62 GDPR), bearing in mind the goal of reaching consensus within the cooperation mechanism and the need to exchange all relevant information, with a view to ensuring protection of the fundamental rights and freedoms of data subjects.

136. The EDPB considers that in determining the scope of the inquiry, whilst it can be limited, a LSA should frame it in such a way that it permits the CSAs to effectively fulfil their role, alongside the LSA, when determining whether there has been an infringement of the GDPR.

7 ON THE CORRECTIVE MEASURES DECIDED BY THE LSA - IN PARTICULAR, THE IMPOSITION OF A REPRIMAND

7.1 Analysis by the LSA in the Draft Decision

137. The Draft Decision explains that, while in the Preliminary Draft Decision the proposed corrective powers to be imposed were both a reprimand, pursuant to Article 58(2)(b) GDPR, and an administrative fine, pursuant to Article 58(2)(i) GDPR, the final Draft Decision consists of the imposition only of an administrative fine on TIC as the controller[139].

138. In its submissions in relation to the Preliminary Draft Decision, TIC objected to the decision to issue a reprimand, contending that the infringements of Article 33(1) and Article 33(5) GDPR do not comprise "processing operations", while Article 58(2)(b) GDPR provides supervisory authorities with the power to issue reprimands where processing operations have infringed provisions of the GDPR[140]. TIC's argument mainly relied on the fact that neither the delay in notifying the SA nor the failure to keep appropriate records amounts to a processing operation in itself[141].

139. In its Draft Decision, the IE SA explained its decision not to issue a reprimand by recalling the argument put forward by TIC in its submissions in relation to the Preliminary Draft Decision, contending that the infringements of Article 33(1) and Article 33(5) GDPR do not comprise "processing operations", while Article 58(2)(b) GDPR provides supervisory authorities with the power to issue reprimands where processing operations have infringed provisions of the GDPR[142]. The IE SA considered that the term

[138] Guidelines on RRO, paragraph 28.
[139] Draft Decision, paragraph 12.1.
[140] TIC's submissions in relation to the Preliminary Draft Decision, paragraph 11.1.
[141] Draft Decision, paragraph 12.4.
[142] TIC's submissions in relation to the Preliminary Draft Decision, paragraph 11.1.

'processing operation(s)' appears 50 times in the GDPR and seems to be used to denote the treatment or use of, in other words things that are done to, personal data controlled by a controller, but that at the same time the definition of "processing" provided by the GDPR is very broad, which makes it arguable that given that a breach is something affecting or done to, personal data, it follows that the notification obligation (insofar as it inherently must entail an examination of what has happened to personal data or how it has been affected) is intrinsically connected to one or more processing operations[143]. The IE SA did not consider it necessary to definitely conclude on the meaning and effect of the term "processing operations" in the Draft Decision, but "on balance" considered that TIC's legal argument was "a stateable one", deciding not to proceed with the issuing of a reprimand to TIC[144].

7.2 Summary of the objections raised by the CSAs

140. The **DE SA** raised an objection concerning the fact that while in the Preliminary Draft Decision both a reprimand and a fine were envisaged, only a fine was included in the Draft Decision. The DE SA disagreed with the reasoning put forward by the IE SA concerning the decision to not impose a reprimand. According to the DE SA, the legal reasoning accepted by the LSA as "stateable" is not convincing as the legal interpretation requires not only an examination of the wording of the provision, but also of its meaning and purpose, the history of its development and its systematic integration into the entire regulatory complex.

7.3 Position of the LSA on the objections

141. In its Composite Memorandum, the IE SA considered that whereas the DE SA's objection does relate to "whether envisaged action in relation to a controller or processor complies with [the GDPR]", it does not demonstrate how not issuing a reprimand to TIC could lead to significant risks for data subjects[145] on the decision to not issue a reprimand was not relevant and reasoned in accordance with Article 4(24) GDPR.

142. Nonetheless addressing the merits of the substantial issue(s) raised by the objections, the LSA explained that it considered the term "processing operations" in accordance with its meaning and application throughout the whole GDPR, noticing that this term is only used for SAs' powers under Article 58 GDPR. Following TIC's submissions in its response to the CSAs' objections on that point, the LSA decided, having regard to the scope of the inquiry that focussed on the controller's obligations in relation to the Breach notification, that its inquiry "*did not involve a finding that the underlying 'processing operations' relating to the Breach infringed [...] the GDPR*"[146]. Therefore, the LSA considered that there was no reason to review its decision to not issue a reprimand in light of the DE SA's objection.

143. The LSA noted that its position in the Draft Decision to not issue a reprimand is only applicable to the specific circumstances of this case; hence is without any prejudice for future decisions on reprimands that could be made by the LSA or any other CSA[147].

[143] Draft Decision, paragraph 12.5.
[144] Draft Decision, paragraph 12.5. The other separate arguments made by TIC concerning reasons why the imposition of a reprimand was not considered appropriate (TIC's submissions in relation to the Preliminary Draft Decision, paragraphs 11.2-11.4) were not considered separately, in light of the aforementioned decision (Draft Decision, paragraph 12.6).
[145] Composite Memorandum, paragraph 5.79.
[146] Composite Memorandum, paragraph 5.78.
[147] Composite Memorandum, paragraph 5.78.

7.4 Analysis of the EDPB

7.4.1 Assessment of whether the objections were relevant and reasoned

144. The **DE SA** objection refers to the compliance of the envisaged action with the GDPR, as it indicates what corrective action would, in its view, be appropriate for the LSA to include in the final decision: it is therefore a relevant objection, which adequately shows the different conclusion proposed. Furthermore, it includes legal reasoning supporting its view and proposes an alternative legal interpretation. Nevertheless, the objection does not clearly demonstrate the significance of the risk posed by the Draft Decision for rights and freedoms of data subjects and/or the free flow of personal data. In particular, it does not provide motivation on how the failure to impose a reprimand in this specific case - where a fine is also imposed - may trigger risks for data subjects' fundamental rights and freedoms.

7.4.2 Conclusion

145. The EDPB considers that this objection does not meet the requirements of Article 4(24) GDPR.

146. The EDPB notes the LSA position that its position to not issue a reprimand is only applicable to the specific circumstances of this case; hence is without any prejudice for future decisions on reprimands that could be made by the LSA or any other CSA[148].

147. As previously indicated, the decision of the EDPB not to assess the merits of the substance of the objection raised is without prejudice to future EDPB decisions on the same or on similar issues.

8 ON THE CORRECTIVE MEASURES - IN PARTICULAR, THE CALCULATION OF THE ADMINISTRATIVE FINE

8.1 Analysis by the LSA in the Draft Decision

148. The Draft Decision explains how the IE SA considered the criteria in Article 83(2) GDPR in deciding whether to impose an administrative fine and how to determine its amount[149].

149. As regards the calculation of the fine, the Draft Decision analysed, first, **the nature, gravity and duration of the infringement**, as per Article 83(2)(a) GDPR[150]. The Draft Decision took into account the "*nature, scope or purpose of the processing*" by referring to the nature of the processing operations carried on by Twitter (a "microblogging" and social media platform on which users have the opportunity to document their thoughts in "tweets"), to the nature of the processing that gave rise to the Breach (arising from a bug leading to previously 'protected' tweets becoming 'unprotected' and publicly accessible - in cases where Android users changed the email address), and to the scope of the processing (the bug affected at least 88,726 EU/EEA users, as additional people were affected between

[148] Composite Memorandum, paragraph 5.78.
[149] Draft Decision, paragraphs 14.1-14.62.
[150] Article 83(2)(a) GDPR refers to "*the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them*".

the date of the bug on 4 November 2014 and its full remediation on 14 January 2019 but it was not possible for them to be all identified)[151].

150. The Draft Decision also took into account **the number of data subjects affected and the level of damage suffered by them**[152] by concluding that the number of data subjects who could have been potentially affected by the delayed notification and the potential for damage to data subjects arising from the consequent delayed assessment by the SA were relevant factors to take into consideration[153]. It was recalled that the impact on individual users and the possibility of damage arising therefrom will impact on the level and nature of the personal data made public and that there was at least a potential for damage to data subjects linked to the delaying of remedial actions[154]. The position of the IE SA in the Preliminary Draft was that *"whilst TIC had not confirmed the precise nature of the data made public in the Breach, it was reasonable to deduce that, given the scale of the affected users and the nature of the service offered by TIC, some of the personal data released in relation to, at least, some of the users will have included sensitive categories of data and other particularly private material*"[155]. This position was further nuanced in the Draft Decision in light of TIC's submissions, as the IE SA decided that "*less weight should be attributed to this factor*", on the basis of the fact that "*while it cannot be definitively said that no users affected by the Breach were affected by the delayed notification, there was no direct evidence of damage to them arising from the delayed notification*"[156].

151. With respect to the **nature of the infringement**, the Draft Decision highlighted that the infringements of Articles 33(1) and 33(5) GDPR do not relate to the substantive matter of the Breach[157]. The IE SA also considered that the nature of the obligations under Articles 33(1) and 33(5) GDPR are such that compliance is central to the overall functioning of the supervision and enforcement regime performed by supervisory authorities in relation to both the specific issue of personal data breaches but also the identification and assessment of wider issues of non-compliance by controllers and that non-compliance with such obligations has serious consequences in that it risks undermining the effective exercise by SAs of their functions under the GDPR[158].

152. With regard to the **gravity of the infringement** of Article 33(1) GDPR, the Draft Decision took account of how it interfered with the overall purpose of notifying a personal data breach to the supervisory authority, of the fact that no material damage to data subjects was shown, of the fact that the remedial measures by TIC were limited to forward looking action to close down the bug (and did not amount to a backward looking analysis to identify the risks to data subjects arising from the Breach) and TIC's apparent failure to carry out any formal risk assessment[159]. The Draft Decision did not consider TIC's contention that the Breach was due to an isolated failure (which led to the delay in notifying the DPO) to be of sufficient weight as to lessen the gravity of the infringement (but did take into account of such isolated nature of the incident, departing from the provisional view in the Preliminary Draft that the

[151] Draft Decision, paragraph 14.2.
[152] Draft Decision, paragraphs 14.3-14.5.
[153] Draft Decision, paragraph 14.5.
[154] Draft Decision, paragraph 14.5 (the Draft Decision notes that "Clearly, the impact on individual users, and the possibility of damage arising therefrom, will depend on the level of personal data made public and, also, the nature of that personal data").
[155] Draft Decision, paragraph 14.5.
[156] Draft Decision, paragraph 14.5.
[157] Draft Decision, paragraph 14.6.
[158] Draft Decision, paragraph 14.11.
[159] Draft Decision, paragraphs 14.16-14.18.

Breach was indicative of a broader, more systemic issue)[160]. Concerning the gravity of the infringement of Article 33(5) GDPR, the Draft Decision highlighted that proper documentation of breaches is required in order to enable a supervisory authority to verify the controller's compliance with Article 33 GDPR[161] and that the IE SA was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach[162], but acknowledged that the deficiencies in the documentation arose from a good faith misunderstanding of the requirements (which are, however, clear from the wording of the provision)[163]. The Draft Decision concluded that each infringement was at the "*low to moderate end of the scale of gravity*"[164].

153. With regard to the **duration of the infringement** of Article 33(1) GDPR, the Draft Decision considered that it was a period of two days and evaluated it in light of the overall timeframe generally permitted for breach notifications (72 hours), noting that it was not a trivial or inconsequential one[165]. Concerning the duration of the infringement of Article 33(5) GDPR, the Draft Decision concluded that it was ongoing[166].

154. In relation to **Article 83(2)(b) GDPR** (the intentional or negligent character of the infringement), the IE SA concluded in its Draft Decision that there was a **negligent character** to TIC's infringement of Article 33(1) GDPR[167], outlining that the delay in the notification of the Global DPO occurred because part of the internal protocol of the Twitter Group was not completed as prescribed and the protocol was not as clear as it could have been[168]. This led to the conclusion that the delay arose as a result of a negligence on the part of the controller, but TIC's submission that the delayed notification was not indicative of a broader systemic issue and amounted to an isolated occurrence was accepted[169]. The IE SA did not identify any evidence of intentional conduct with regard to the infringement of Article 33(1) GDPR[170]. The Draft Decision also identified that there was a negligent character to TIC's infringement of Article 33(5) GDPR[171], since there was no knowledge and wilfulness to cause the infringement (which would have amounted to intent) but the documentation was not sufficient to enable compliance with Article 33 to be verified[172].

155. As regards **Article 83(2)(c) GDPR**, i.e. action taken by the controller to **mitigate the damage suffered by data subjects**, the Draft Decision considered that remedial measures were taken to avoid repetition of the issue and to rectify the bug, which were considered as the sole mitigating factor in assessing the amount of the fine to be imposed[173].

156. The Draft Decision considered **Article 83(2)(d) GDPR**, i.e. the **degree of responsibility** for the controller or processor, by noting the existing and subsequently enhanced technical and organisational measures

[160] Draft Decision, paragraph 14.19.
[161] Draft Decision, paragraph 14.20.
[162] Draft Decision, paragraph 14.21.
[163] Draft Decision, paragraph 14.24.
[164] Draft Decision, paragraph 14.24.
[165] Draft Decision, paragraph 14.26 (it commenced on the expiration of the 72 hours from 3 January 2019 (i.e. on 6 January 2019) and ended at the time of TIC's notification of the Breach on 8 January 2019).
[166] Draft Decision, paragraph 14.29.
[167] Draft Decision, paragraph 14.34.
[168] Draft Decision, paragraphs 14.33-14.34.
[169] Draft Decision, paragraph 14.34.
[170] Draft Decision, paragraph 14.35.
[171] Draft Decision, paragraph 14.38.
[172] Draft Decision, paragraphs 14.36, 14.38.
[173] Draft Decision, paragraphs 14.39-14.42.

implemented by TIC as controller, including the amendment of the internal protocol of the Twitter Group (which the IE SA found was not as clear as it could have been) and the staff training measures taken afterwards by Twitter, Inc.(additional training was provided internally highlighting the importance of mentioning the DPO team - and therefore TIC as controller - in the internal ticket system), as well as the existence of internal structures and safeguards concerning responsibility for information security issues and the existence of a recurring external third party expert audit of Twitter, Inc.'s Information Security Programme[174]. Although the issues that arose were not found to be indicative of a broader systemic issue[175] and TIC demonstrated a generally responsible and accountable approach towards data security[176], it was considered that there was a moderate to high level of responsibility demonstrated by the controller as a lack of clarity in the protocol was shown also by its subsequent amendment[177].

157. The **degree of cooperation** with the supervisory authority was evaluated, in line with **Article 83(2)(f) GDPR**, and was found to not amount to a mitigating factor[178]. The IE SA acknowledged that TIC cooperated fully but noted that this was a statutory obligation and TIC did not go beyond such duty[179].

158. In relation to **Article 83(2)(g) GDPR** concerning the **categories of personal data affected**, the Draft Decision concluded that any category of personal data could have been affected by the delayed notification and that it cannot be definitively said that there was no damage to data subjects or no affected categories of personal data[180].

159. The **manner in which infringement became known** to the IE SA was considered to be a relevant factor in the determination of the amount of the fine (in line with Article 83(2)(h) GDPR), since while TIC was forthcoming in furnishing all available documentation the records did not allow the IE SA to verify compliance with Article 33 GDPR and the information originally provided in the notification made to the IE SA was of an imprecise nature[181].

160. The criteria in **Article 83(2)(e), (i) and (j) GDPR** were found to be not applicable, and no further elements were identified in relation to **Article 83(2)(k) GDPR**[182].

161. The IE SA underlined in its Draft Decision that in the absence of specific EU-level guidelines on the calculation of fines, it was not bound to apply any particular methodology or use a fixed financial starting point[183] and that the expression "due regard" provides SAs with a broad discretion as to how to weigh the factors in Article 83(2) GDPR[184].

162. As regards the identification of the relevant undertaking to calculate the fining cap established by **Article 83(4) GDPR**, the IE SA underlined that the fact that TIC enjoys autonomy in its control over data processing does not mean that it ceases to be part of a **single economic entity** with its parent company

[174] Draft Decision, paragraphs 14.43-14.47.
[175] Draft Decision, paragraphs 14.45.
[176] Draft Decision, paragraph 14.47.
[177] Draft Decision, paragraph 14.47.
[178] Draft Decision, paragraph 14.50.
[179] Draft Decision, paragraph 14.49.
[180] Draft Decision, paragraph 14.54.
[181] Draft Decision, paragraph 14.58.
[182] Draft Decision, paragraphs 14.48, 14.59, 14.60, 14.61.
[183] Draft Decision, paragraph 15.2.
[184] Draft Decision, paragraph 15.1.

and noted that, in addition to the ownership of TIC by Twitter, Inc., the General Counsel of Twitter, Inc. appears to be one of the three directors of TIC[185].

163. For this reasons, the cap for the value of any fine imposed was calculated by the LSA with reference to Twitter, Inc.'s turnover[186]. As the annual turnover of Twitter, Inc., in 2018, amounted to 3 billion USD, the cap was considered to be 60 million USD (2% of 3 billion USD)[187].

164. In applying the principles of **effectiveness, proportionality and dissuasiveness** (**Article 83(1) GDPR**), the Draft Decision considered that a fine cannot be effective if it does not have significance relative to the revenue of the controller, that the infringement needs to not be considered in the abstract, regardless of the impact on the controller, and that future infringements need to be deterred[188].

165. The IE SA proposed to impose an administrative fine within the range of 150,000-300,000 USD, i.e. between 0.005% and 0.01% of the undertaking's annual turnover or between 0.25% and 0.5% of the maximum amount of the fine which may be applied in respect of these infringements. This equates to a fine in Euro of between 135,000 and 275,000[189].

8.2 Summary of the objections raised by the CSAs

166. The **AT SA** raised an objection concerning the amount of the proposed fine and the fact that the LSA proposed a range of amounts instead of a fixed sum. With regard to Article 83(2)(a) GDPR, the AT SA highlighted that at least 88,726 people (but probably more) were affected by the Breach and "*it is very likely that sensitive data were disclosed to the broader public*".

167. The objection raised by the AT SA expressed a disagreement as to how the *time at which the controller should be deemed to be aware of a data breach* was analysed in the Draft Decision. More specifically, the AT SA argued in its objection that TIC should have made a data breach notification within 72 hours after the processor received the bug report and thus became aware of the Breach. The AT SA highlighted that TIC is responsible for overseeing the processing operations carried out by its processor, and that a controller should not seek to hide the failure of its processor with whom it has a contractual relationship and which was selected by the controller itself. This contributes to the assessment of the infringement of Article 33(1) GDPR by the AT SA as "grave".

168. With regard to the "*intentional or negligent character of the infringement*" (Article 83(2)(b) GDPR), the AT SA argued that the behaviour of TIC should be labelled as "intentional", on the basis of the criteria of knowledge and wilfulness established in the Guidelines on the application and setting of administrative fines ("WP253") of the Article 29 Working Party, endorsed by the EDPB[190]. As to the criterion referring to *actions taken to mitigate the damage* suffered by data subjects (Article 83(2)(c) GDPR), the AT SA highlighted that "*initially it was not TIC's intention to notify users who were affected by the breach*" and "*the steps taken by Twitter Inc. to rectify the bug are the sole mitigating factor*".

[185] Draft Decision, paragraph 15.13.
[186] Draft Decision, paragraph 15.14.
[187] Draft Decision, paragraph 15.19.
[188] Draft Decision, paragraph 15.18.
[189] Draft Decision, paragraph 15.20 (The higher end of the range proposed in the Draft Decision is lower than in the Preliminary Draft Decision, in order to reflect changes in the views in relation to gravity, the degree of responsibility of the controller and whether the infringements were systemic). In paragraph 15.21, the Draft Decision underlined that in order to protect TIC's procedural rights a range of a fine was proposed as opposed to a fixed figure, and acknowledged the possibility that CSAs would comment on where in that range the penalty should lie.
[190] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

Finally, AT SA considers the range of fine proposed by the IE SA neither effective, nor proportionate, nor dissuasive having regard to the criteria listed in Article 83(2)(a) – (k) GDPR. As a conclusion, the AT SA proposed the imposition of a higher administrative fine, which could meet the requirement of effectiveness, proportionality and dissuasiveness (namely "*a minimum amount of 1 % of the undertaking's annual turnover*").

169. The **DE SA** raised an objection arguing that the fine proposed by the LSA is "too low" and "does not comply with the provisions of Article 83(1) GDPR". More specifically, the DE SA argued that the fine is not dissuasive. The objection recalled that a sanction can be deemed effective and dissuasive if it is suitable both as a general preventive measure - to deter the general public from committing infringements and to affirm the general public's confidence in the validity of Union law - and as a special preventive measure - to deter the offender from committing further infringements. The DE SA goes on to argue that the financial capacity of an undertaking (in terms of turnover) can provide an important indication of the amounts required to achieve dissuasiveness: this may entail taking into account the part of the turnover generated by the products in respect of which the infringement has been committed, which may provide an indication of the scale of the infringements. The DE SA also argues that the dissuasive effect of high fines can only be achieved if the amounts imposed cannot be easily paid because of large assets or high income, highlighting that the fine must have a dissuasive effect, particularly in relation to specific data processing. As a consequence, the threatened fine must be high enough to make data processing uneconomic and objectively inefficient. As Twitter's business model is based on processing data, and as Twitter generates turnover mainly through data processing, the DE SA considers that a dissuasive fine in this specific case would therefore have to be so high that it would render the illegal data processing unprofitable. On the basis of the fine concept applicable to the DE SAs, the fine for the infringement described in the Draft Decision would range from approximately EUR 7,348,035.00 to EUR 22,044,105.00.

170. The **HU SA** argued that, although "*fines are justified for the committed infringements*", "*the fine set out in the draft is unreasonably low, disproportionate and thus not dissuasive in view of the gravity of the committed infringement and the Controller's worldwide market power*".

171. The **IT SA** asked the LSA to "*review the draft decision as also related to quantification of the administrative fine, taking also account of specific aggravating elements of the case with regard to the nature of the data controller and the severity and duration of the data breach*".

8.3 Position of the LSA on the objections

172. The IE SA assessed that the objections raised by the AT SA, DE SA and HU SA in relation to the administrative fine to be 'relevant and reasoned' within the meaning of Article 4(24) GDPR. At the same time, the IE SA did not follow these objections for the reasons set out in the Composite Memorandum[191].

173. In particular, as regards to the AT and DE SA's objections, the IE SA considers that its assessment and application of the factors at Articles 83(2)(a) and (b) GDPR, as elaborated in its Draft Decision, is appropriate. Regarding the AT SA's objection, the IE SA argues that TIC's infringement of Article 33(1) and Article 33(5) GDPR was the result of TIC's negligence rather than an intentional omission[192]. Therefore, the IE SA believes that the fine as proposed by the AT SA is not proportionate[193]. In addition,

[191] Composite Memorandum, paragraphs 5.60-5.72.
[192] Composite Memorandum, paragraph 5.62.
[193] Composite Memorandum, paragraph 5.63.

the IE SA argues that the concern of the AT SA regarding the fining range proposed in the Draft Decision, as opposed to a fixed sum, was not well elaborated and clarified by this CSA[194]. With regard to the DE SA's objection, the IE SA took note of the objection of the DE SA regarding the need for the fine to meet the requirement of dissuasiveness, but is of the opinion that the level of the fine proposed by the DE SA is not proportionate in this case[195]. For the above-mentioned reasons, the IE SA considers these objections are reasoned and relevant, but proposes not to follow them[196].

174. The IE SA has taken due account of the AT SA's view in relation to the timing of TIC's awareness and notification of the Breach but concluded that notwithstanding TIC's actual 'awareness' of the Breach on 7 January 2019, TIC ought to have been aware of the Breach at the latest by 3 January 2019[197]. In identifying 3 January 2019 as the date on which TIC ought to have been aware of the breach, the IE SA took into account that an earlier delay had arisen during the period from when the incident was first notified by a contractor to Twitter, Inc. to when Twitter, Inc. commenced its review[198]. Further, the IE SA clarifies that it is not suggesting that, "*as a matter of generality, data controllers ought to automatically be considered to have awareness of data breaches at the same time at which their processor becomes aware of the breach*"[199]. Also, the IE SA states that "*it will usually be the case that a processor which experiences a breach will be aware of the incident at an earlier point in time than its controller, and that, provided the process agreed between the controller and the processor is effective and / or is followed, the controller will be made 'aware' of the breach [...] in a manner that enables it to comply with its obligation to notify same*"[200].

8.4 Analysis of the EDPB

8.4.1 Assessment of whether the objections were relevant and reasoned

175. Concerning the possibility for relevant and reasoned objections on whether envisaged action in relation to the controller or processor complies with the GDPR[201] to challenge the amount of proposed fines, the EDPB recently clarified that "*it is possible that the objection challenges the elements relied upon to calculate the amount of the fine*"[202]. This can amount to an example of objection concerning whether the envisaged action in relation to the controller or processor complies with the GDPR.

176. In the case at stake, the **AT SA**'s objection challenges the elements relied upon by the IE SA in calculating the amount of the fine and thus concerns the compliance of the proposed action vis-a-vis the controller with the GDPR. The AT SA clarified the connection between its objection and the Draft Decision and demonstrated how the proposed changes would lead to a different conclusion. Additionally, it provided arguments on why the amendment of the decision is proposed, by providing an alternative interpretation of three of the criteria listed by Article 83 GDPR and by making reference to factual and legal arguments. The AT SA clearly demonstrates the significance of the risks posed by the Draft Decision, first of all, by arguing that the proposed fine is not adequately effective and dissuasive and by recalling that to this end it needs to be likely to deter the general public from committing a similar infringement and confirm the public's confidence in the application of Union law,

[194] Composite Memorandum, paragraph 5.64.
[195] Composite Memorandum, paragraph 5.68.
[196] Composite Memorandum, paragraphs 5.65, 5.68.
[197] Composite Memorandum, paragraph 5.48.
[198] Composite Memorandum, paragraph 5.50.
[199] Composite Memorandum, paragraph 5.50.
[200] Composite Memorandum, paragraph 5.50.
[201] GDPR, Article 4(24).
[202] Guidelines on RRO, paragraph 34.

as well as to deter the controller from committing further infringements. Additionally, in the assessment of the gravity of the infringement the objection also refers to the extent to which data subjects (in a number likely to be higher than the one identified) were affected by the Breach (e.g. by having their previously protected tweets, likely to include sensitive data, exposed to the wider public). The alleged intentionality of the infringement, according to the AT SA, implies a far greater impact on the ability to know right from wrong than a negligent infringement. In light of the assessment above, the EDPB considers that the AT SA's objection is relevant and reasoned in accordance with Article 4(24) GDPR. As a consequence, the EDPB will assess the merit of the substantial issues raised by this objection (see section 8.4.2 below).

177. The **DE SA**'s objection is also to be considered relevant as it concerns the compliance of the envisaged action with the GDPR, by challenging the elements relied upon to calculate the amount of the fine. More specifically, it argues that the fine imposed by the IE SA is not dissuasive and thus the calculation performed does not comply with Article 83(1) GDPR. The DE SA clarified that a sanction is to be considered effective and dissuasive, when it serves as a general preventive measure to deter general public from committing infringements as well as to affirm its trust to the validity of the Union law, but also when it deters the offender from committing additional infringements. In addition, the DE SA clearly demonstrates the significance of the risks that the Draft Decision poses to the rights and freedoms of the data subjects as the failure to impose a dissuasive and effective sanction may not be able to deter the controller from committing further infringements.

178. Another argument provided by the DE SA to demonstrate the significance of the risks is that the failure to appropriately handle the Breach suggests a "*systemic error*", which would have required submitting the controller to a deeper scrutiny, beyond the single specific incident. The DE SA also recalled that a large number of persons was concerned and the period of time was equally substantial and concluded that the corrective powers imposed on the basis of Article 58(2) GDPR need to be examined in light of these elements. To conclude, the EDPB considers that the DE SA's objection is reasoned and relevant within the definition of Article 4(24) GDPR. As a consequence, the EDPB will assess the merit of the substantial issues raised by this objection (see section 8.4.2 below).

179. The **HU SA**'s objection is relevant as it also concerns the compliance of the envisaged action with the GDPR, by stating that the proposed fine is "*unreasonably low, disproportionate and thus not dissuasive*". However, while the objection refers to "*the "bug" in the controller's application over the years" and to "its serious nature affecting data security*", as well as to the "*gravity of the committed infringement*" and to the "*controller's worldwide market power*", it does not clearly demonstrate the significance of the risks for rights and freedoms of data subjects posed by the amount of the fine as proposed by the IE SA. As a consequence, the EDPB considers this objection does not meet the requirements of Article 4(24) GDPR[203].

180. Last, the relevance of the objection raised by the **IT SA** is also shown by its reference to whether the proposed action complies with the GDPR, as it argues that the IE SA should review the Draft Decision in relation to the quantification of the administrative fine. By referring to the "*foregoing objections*" and thus to the fact that the aspects mentioned are "*structural in nature as regards the controller's organisation*" and "*bound to produce effects not simply on the case at issue, but also on any data*

[203] As a consequence, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

breach that may occur in the future", the IT SA's objection clearly demonstrates the significance of the risks for the rights and freedoms of data subjects with respect to the quantification of the fine.

181. Therefore, EDPB considers that the IT SA's objection is reasoned and relevant meeting the requirements of Article 4(24) GDPR. As a consequence, the EDPB will assess the merit of the substantial issues raised by this objection.

8.4.2 Assessment of the merits of the substantial issue(s) raised by the relevant and reasoned objections

182. The EDPB considers that the objections found to be relevant and reasoned in this subsection[204] require the assessment of whether the Draft Decision proposes a fine in line with the criteria established by Article 83 GDPR and the Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 ("WP253") (endorsed by the EDPB)[205].

183. Indeed, the consistency mechanism may also be used to promote a consistent application of administrative fines[206]: where a relevant and reasoned objection challenges the elements relied upon by the LSA to calculate the amount of the fine, the EDPB can instruct the LSA to engage in a new calculation of the proposed fine by eliminating the shortcomings in the establishment of causal links between the facts at issue and the way the proposed fine was calculated on the basis of the criteria in Article 83 GDPR and of the common standards established by the EDPB[207]. A fine should be effective, proportionate or dissuasive, as required by Article 83(1) GDPR, taking account of the facts of the case[208]. In addition, when deciding on the amount of the fine the LSA shall take into consideration the criteria listed in Article 83(2) GDPR.

184. As regards the nature, gravity and duration of the infringement found in Articles 33(1) and 33(5) GDPR, **Article 83(2)(a) GDPR** requires to take into consideration *inter alia* the **nature, scope and purpose of the processing concerned** as well as the **number of data subjects affected** and the **level of damage** suffered by them.

185. The EDPB agrees with the IE SA that the infringement to consider is not the Breach as such but the compliance with Articles 33(1) and 33(5) GDPR to notify that breach to the competent SA and to document that breach.

186. The EDPB notes that the IE SA takes into account the nature of the processing as well as the number of data subjects affected. As regards the **nature of the processing**, the IE SA describes as a "microblogging" and social media platform on which users have the opportunity to document their thoughts in "tweets". The EDPB considers that when assessing the nature of the processing, one must also take into consideration the fact the "processing concerned" involved communications by data subjects who deliberately chose to restrict the audience of those communications. The EDPB takes note that the IE SA Draft Decision considered that: "*the impact on individual users, and the possibility of damage arising therefrom, will depend on the level of personal data made public and, also, the nature of that personal data. In this regard, I indicated in the Preliminary Draft that whilst TIC had not*

[204] These objections are those of the AT SA, DE SA, and IT SA.
[205] Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253 adopted on 3 October 2017 (endorsed by the EDPB on 25 May 2020).
[206] GDPR, Recital 150.
[207] Guidelines on RRO, paragraph 34.
[208] EDPB Guidelines on administrative fines, p. 7.

confirmed the precise nature of the data made public in the Breach, it was reasonable to deduce that, given the scale of the affected users and the nature of the service offered by TIC, some of the personal data released in relation to, at least, some of the users will have included sensitive categories of data and other particularly private material"[209]. However, the IE SA, based on TIC submissions, gave less weight to this factor than it did in the Preliminary Draft, as there was no direct evidence of damage[210]. The EDPB considers, however, that the IE SA should still have given significant weight to the fact that the "processing concerned" involves communications by data subjects who deliberately chose to restrict the audience of those communications, when evaluating the nature of the processing concerned. In particular, the IE SA should have given significant weight to this fact given that it was recalled by the IE SA in the Draft Decision, where the IE SA considered that "t*he large scale of the affected user segment gives rise to the possibility of a much broader spectrum of damage arising from the Breach, particularly given the nature of the service being offered by TIC*" and "*the likelihood that many users will have relied on the function of keeping "tweets" private to share information or views (in the comfort of what they believe to be a private and controlled environment) that they would not ordinarily release into the public domain*"[211].

187. Moreover, when it comes to the scope of the processing concerned as such, the IE SA appears to substitute the scope of the processing with the number of the data subjects affected. The EDPB considers that the **nature and the scope of the "processing**" to take into consideration in the determination of the fine is not the processing operation consisting in the (accidental) disclosure (personal data breach), or the cause thereof, but rather the scope of the underlying processing carried out by TIC, as described in the previous paragraph.

188. According to the AT SA, **the timing when the controller became aware of the breach impacts on the gravity of the infringement** of Article 33(1) GDPR. The objection raised by the AT SA expressed a disagreement as to how the time at which the controller should be deemed to be aware of a data breach should be determined or assessed. More specifically, the AT SA argued in its objection that TIC should have made a data breach notification within 72 hours after the processor became aware of the bug. This contributes to the assessment of the infringement of Article 33(1) GDPR by the AT SA as "grave".

189. In this respect, the EDPB recalls that the Guidelines on personal data breach notification under Regulation 2016/679 ("WP250")[212], which were endorsed by the EDPB, state that the "*focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data*"[213].

190. According to the Guidelines on personal data breach notification, a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised[214]. Since the controller uses the processor to achieve its purposes, in principle, the controller should be considered as "aware" once

[209] Draft Decision, paragraph 14.51.
[210] See paragraph 150 above.
[211] Draft Decision, paragraph 14.51.
[212] Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, WP250 rev.01, endorsed by the EDPB (hereinafter, "Guidelines on personal data breach notification").
[213]Guidelines on personal data breach notification, p. 5.
[214] Guidelines on personal data breach notification, p.10-11.

the processor has informed it of the breach[215]. However, the GDPR puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action"[216] and explain that "*the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware"*"[217]. However, the Guidelines clarify that this initial investigation should begin as soon as possible and that a more detailed investigation can then follow[218].

191. The Guidelines thus make it clear that the controller, and by extension, the processor, are to act swiftly. "In most cases these preliminary actions should be completed soon after the initial alert (i.e. *when the controller or processor suspects there has been a security incident which may involve personal data*) – it should take longer than this only in exceptional cases"[219].

192. Having regard to the above, the EDPB agrees with the position of the IE SA's assessment according to which the controller cannot be expected to have become aware at the moment its processor has realised that a security incident has occurred. As provided in the WP29 Guidelines on data breach notifications, which were endorsed by the EDPB, there needs to be a degree of certainty that a personal data breach has occurred before awareness can be stipulated. It is not clear from the facts at issue as reflected in the Draft Decision that this was the case before the 3 January 2019. In this case, AT SA did not prove that TIC reached the necessary degree of certainty as to the fact that a data breach had occurred earlier than when the IE SA found TIC to be "aware" of the breach. As a consequence, the EDPB considers that the assessment of the gravity of the infringement does not need to be adjusted in light of a different determination of when the controller became aware of the data breach.

193. Moreover, as regards **the gravity of the infringement**, the EDPB agrees with IE SA that the compliance with Articles 33(1) and 33(5) GDPR are central to the overall functioning of the supervision and enforcement regime.

194. As regards the objection raised by the AT SA regarding the **intentional nature of the infringement**, the EDPB considers that the objection did not sufficiently demonstrate that from the moment the controller gained knowledge it intentionally disregarded its duty of care.

195. However, as regards the negligent nature of the infringement, the EDPB considers that a company for whom the processing of personal data is at the core of its business activities should have in place sufficient procedures for the documentation of personal data breaches, including remedial actions, which will enable it to also comply with the duty of notification under Article 33(1) GDPR. This element implies an additional element to take into consideration in the analysis of the gravity of the infringement.

196. The EDPB recalls that the CJEU has consistently held that a dissuasive penalty is one that has a **genuine deterrent effect**[220]. In that respect, a distinction can be made between general deterrence (discouraging others from committing the same infringement in the future) and specific deterrence

[215] Guidelines on personal data breach notification, p. 13.
[216] Guidelines on personal data breach notification, p.11.
[217] Guidelines on personal data breach notification, p.11 (emphasis added).
[218] Guidelines on personal data breach notification, p.11.
[219] Guidelines on personal data breach notification, p.12 (emphasis added).
[220] See Opinion of Advocate General Geelhoed of 29 April 2004 in Judgment of 12 July 2005, Commission / France, C-304/02, EU:C:2005:444, par. 39.

(discouraging the addressee of the fine from committing the same infringement again)[221]. Moreover, the severity of penalties must be commensurate with the seriousness of the infringements for which they are imposed[222]. It follows that fines must not be disproportionate to the aims pursued, that is to say, to compliance with the data protection rules and that the amount of the fine imposed on an undertaking must be proportionate to the infringement viewed as a whole, account being taken in particular of the gravity of the infringement[223].

197. While the LSA in its Draft Decision made reference to the requirement that the file must be **dissuasive and proportionate**, the EDPB considers that the LSA did not sufficiently substantiate how the fine proposed addresses these requirements. In particular, the EDPB notes that the LSA moves from calculating the maximum amount of the fine (set at $60 million) to stating the proposed fining range (set between $150.000,- and $300.000,-), without further explanation as to which particular elements led the LSA to identify this specific range[224]. Beyond the general reference to the relevant factors of Article 83 (2) GDPR, there is not a clear motivation for the choice of the proposed percentage (between 0.25% and 0.5%) of the maximum applicable fine under Article 83(4) GDPR.

198. In this regards, the EDPB has elaborated above the reasons to why the LSA in its Draft Decision should have given greater weight to the element relating to the nature, scope and negligent character of the infringement and therefore consider that the proposed fine range should be adjusted accordingly.

8.4.3 Conclusion

199. Following this, the EDPB considers that the fine proposed in the Draft Decision is too low and therefore does not fulfil its purpose as a corrective measure, in particular it does not meet the requirements of Article 83(1) GDPR of being effective, dissuasive and proportionate.

200. Thus, the EDPB requests the IE SA to re-assess the elements it relies upon to calculate the amount of the fixed fine[225] to be imposed on TIC so as to ensure it is appropriate to the facts of the case.

201. The EDPB notes that the analysis of the objections is limited to the substance of the objections to be considered as relevant and reasoned. The scope of the EDPB's analysis concerning the calculation of the fine is therefore limited to an analysis of the method of the calculation of the fines as such. It does not constitute an implicit or explicit validation by the EDPB, of the analysis carried out by the LSA regarding the infringement of Article 33(1) or Article 33(5) GDPR or the legal qualification of the Twitter Inc. and TIC respectively. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

9 BINDING DECISION

202. In light of the above and in accordance with the task of the EDPB under Article 70(1)(t) GDPR to issue binding decisions pursuant to Article 65 GDPR, the Board issues the following binding decision in accordance with Article 65(1)(a) GDPR:

[221] See *inter alia* Judgment of 13 June 2013, Versalis Spa / Commission, C-511/11, ECLI:EU:C:2013:386, para. 94.
[222] CJEU Judgment of 25 April 2013, Asociaţia Accept, C-81/12.
[223] Marine - Harvest EU General Court T-704/14, 26 October 2017.
[224] Draft Decision 15.19 and 15.20.
[225] This should preferably already be provided in the Art 60 GDPR draft decision.

203. On the objections concerning the qualification of controller and processor and the competence of the LSA:

- The EDPB decides that the IE SA is not required to amend its Draft Decision on the basis of the objections raised, as they do not meet the requirements of Article 4(24) GDPR.

204. On the objections concerning the infringements of Article 33(1) and 33(5) GDPR found by the LSA:

- In relation to the objection of the FR SA on the absence of an infringement of Article 33(1) GDPR, the objection of the DE SA on the determination of the *dies a quo* for the infringement of Article 33(1) GDPR, and the objection of the IT SA relating to the infringement of Article 33(5) GDPR, the EDPB decides that the IE SA is not required to amend its Draft Decision on the basis of the objections raised as they do not meet the requirements of Article 4(24) GDPR.

205. On the objections relating to the possible further (or alternative) infringements of the GDPR identified by the CSAs:

- In relation to the objection of the DE SA on the possible infringements of Article 5(1)(f), Article 24, and Article 32 GDPR, and to the objection of the IT SA on the possible infringement of Article 5(2) GDPR, the EDPB decides that, while they meet the requirements of Article 4(24) GDPR, the IE SA is not required to amend its Draft Decision because the available factual elements included in the Draft Decision and in the objections are not sufficient to allow the EDPB to establish the existence of infringements of Articles 5(1)(f), Article 5(2), Article 24, and Article 32 GDPR.

- In relation to the objection of the DE SA relating to the possible infringement of Article 33(3) GDPR, the objection of the FR SA relating to the possible infringement of Article 28 and Article 32 GDPR, the objection of the HU SA relating to the possible infringement of Article 5(1)(f), Article 32, and Article 34 GDPR, and the objection of the IT SA relating to the possible infringement of Article 28 GDPR, the EDPB decides that the IE SA is not required to amend its Draft Decision on the basis of the objections raised as they do not meet the requirements of Article 4(24) GDPR.

206. On the objection concerning the decision of the LSA to not issue a reprimand:

- In relation to the objection of the DE SA concerning the decision of the IE SA not to issue a reprimand, the EDPB decides that the IE SA is not required to amend its Draft Decision on the basis of the objection raised as it does not meet the requirements of Article 4(24) GDPR.

207. On the objection concerning the calculation of the fine suggested by the LSA:

- In relation to the objection of the HU on the insufficiently dissuasive nature of the fine, the EDPB decides that the IE SA is not required to amend its Draft Decision on the basis of the objection raised as it does not meet the requirements of Article 4(24) GDPR.

- In relation to the objection of the AT SA, the objection of the DE SA, and the objection of the IT SA on the insufficiently dissuasive nature of the fine, the EDPB decides that they meet the requirements of Article 4(24) GDPR and that the IE SA is required to re-assess **the elements it relies upon to calculate the amount of the fixed fine** to be imposed on TIC, and to amend its Draft Decision by increasing the level of the fine in order to ensure it fulfils its purpose as a corrective measure and meets the requirements of effectiveness, dissuasiveness and proportionality established by Article 83(1) GDPR and taking into account the criteria of Article 83(2) GDPR.

10 FINAL REMARKS

208. This binding decision is addressed to the IE SA and the CSAs. The IE SA shall adopt its final decision on the basis of this binding decision pursuant to Article 65(6) GDPR.

209. Regarding the objections deemed not to meet the requirements stipulated by Art 4(24) GDPR, the EDPB does not take any position on the merit of any substantial issues raised by these objections. The EDPB reiterates that its current decision is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

210. According to Article 65(6) GDPR, the IE SA shall communicate its final decision to the Chair within one month after receiving the binding decision.

211. Once such communication is done by the IE SA, the binding decision will be made public pursuant to Article 65(5) GDPR.

212. Pursuant to Article 70(1)(y) GDPR, the IE SA's final decision communicated to the EDPB will be included in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)