

In the matter of the General Data Protection Regulation

DPC Case Reference: IN-19-1-1

In the matter of Twitter International Company

Decision of the Data Protection Commission made pursuant to

Section 111 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to Section 110 of the Data Protection Act 2018

DECISION

Decision-Maker for the Commission:

Helen Dixon
Commissioner for Data Protection

Dated the 9th day of December 2020



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

An Coimisiún um Chosaint Sonraí, 21 Cearnóg Mhic Liam, Baile Átha Cliath 2.

Data Protection Commission, 21 Fitzwilliam Square, Dublin 2.

www.cosantasonrai.ie | www.dataprotection.ie | eolas@cosantasonrai.ie | info@dataprotection.ie Tel: +353 (0)76 1104800

Table of Contents

1.	Introduction	4 - 6
	<i>Purpose of this document</i>	
	<i>Background in brief</i>	
2.	Legal Framework for the Inquiry	6 - 12
	<i>Outline of Inquiry process</i>	
	<i>TIC as controller</i>	
	<i>Competence of the Commission</i>	
	<i>Legal basis for Inquiry</i>	
	<i>Conduct of Inquiry</i>	
3.	Legal Framework for the Decision	12 - 15
	Decision-making process – materials considered	
	TIC's submissions in relation to the Preliminary Draft	
4.	The Facts as Established	15 - 21
5.	Issues for Determination	21
6.	Issue I – Article 33(1)	21 - 29
	<i>Requirements of Article 33(1)</i>	
	<i>Controller responsibility</i>	
	<i>Accountability</i>	
	<i>Controller obligations under the GDPR</i>	
7.	Issue I – TIC's Compliance with Article 33(1)	29 - 89
	<i>Analysis of facts relating to TIC's notification of the Breach</i>	
	<i>TIC's Submissions in relation to the Preliminary Draft</i>	
	<i>TIC's Submissions in respect of factual matters concerning its notification of the Breach to the Commission</i>	
	<i>TIC's Submissions in relation to the provisional finding that it did not comply with Article 33(1)</i>	
	<i>Finding – Article 33(1)</i>	
8.	Issue II – Article 33(5)	90 - 108
	<i>Requirements of Article 33(5)</i>	
	<i>TIC's submissions regarding the interpretation and application of Article 33(5)</i>	
	<i>Documentation requirements to enable verification of compliance with Article 33, in accordance with Article 33(5)</i>	
9.	Issue II – TIC's Documentation in relation to the Breach	109 - 113
	<i>Summary of documentation furnished by TIC</i>	

10.	Issue II – Analysis of Documentation furnished by TIC for the Purposes of Assessing Compliance with Article 33(5)	114 - 134
	<i>Analysis of the Incident Report for the purposes of assessing compliance with Article 33(5)</i>	
	<i>Analysis of the Jira Tickets</i>	
	<i>Analysis of the calendar invites and internal ‘Slack’ message</i>	
	<i>TIC’s offer to provide supplemental information by way of sworn affidavit</i>	
	<i>Finding – Article 33(5)</i>	
11.	Decision under Section 111(2) of the 2018 Act	135 - 138
12.	Corrective Powers – Article 58(2) GDPR	138 - 140
	<i>The Reprimand</i>	
13.	Administrative Fine – Article 58(2)(l)	141 - 144
	<i>TIC’s general submissions on the proposed imposition of an administrative fine</i>	
	<i>Binding decision of the EDPB</i>	
14.	Consideration of the Criteria in Article 83(2) in Deciding Whether to Impose an Administrative Fine	145 - 175
15.	Calculation of Administrative Fine	175 - 182
	<i>The relevant undertaking</i>	
	<i>Amount of the administrative fine</i>	
	<i>Annex I – Schedule of documentation considered by the decision maker for the purpose of preparation of the Decision</i>	184 - 188
	<i>Annex II – ‘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’ (‘the EDPB Decision’)</i>	

DECISION UNDER S.111 OF THE DATA PROTECTION ACT 2018 AND FOR THE PURPOSES OF ARTICLE 60 OF THE
GENERAL DATA PROTECTION REGULATION (EU) 2016/679 (GDPR)

TO: TWITTER INTERNATIONAL COMPANY, ONE CUMBERLAND PLACE, FENIAN STREET, DUBLIN 2,
IRELAND

1. INTRODUCTION

Purpose of this document

- 1.1 This is a decision ('the Decision') made by the Data Protection Commission ('the Commission') in accordance with Section 111 of the Data Protection Act 2018 ('the 2018 Act'), and the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council ('the GDPR') arising from an inquiry conducted of the Commission's own volition, pursuant to Section 110 of the 2018 Act ('the Inquiry'). For the avoidance of doubt, the within constitutes the notice in writing of the decision made under Section 111 of the 2018 Act that I am required to give to Twitter International Company, as the controller concerned, for the purpose of Section 116(1) of the 2018 Act.
- 1.2 The Inquiry, which commenced on 22 January 2019, examined whether Twitter International Company ('TIC') complied with its obligations under the GDPR in respect of its notification of a personal data breach to the Commission on 8 January 2019.
- 1.3 On 14 March 2020, a preliminary draft of this Decision ('the Preliminary Draft') was issued to TIC by the Commission. The Preliminary Draft set out my provisional findings, as the decision-maker in the Commission in this matter, in relation to (i) whether or not an infringement of the GDPR has occurred / is occurring; and (ii) the envisaged action to be taken by the Commission in respect of same.
- 1.4 The Preliminary Draft was provided to TIC for the purpose of allowing TIC to make any submissions in relation to my provisional findings. TIC furnished its submissions in respect of the Preliminary Draft on 27 April 2020. I carefully considered and took account of TIC's submissions for the purpose of preparing a draft of this Decision ('the Draft Decision'), which was submitted by the Commission, on 22 May 2020, to other concerned supervisory authorities (within the meaning of Article 4(22) of the GDPR) pursuant to Article 60.
- 1.5 Following this, and during the four-week timeframe provided for under Article 60(4), a number of concerned supervisory authorities raised objections in respect of aspects of the Draft Decision. In circumstances where the Commission was unable to follow the objections raised and / or was of the opinion that the objections were not relevant and reasoned, the Commission submitted the matter to the consistency mechanism referred to in Article 63, as is required by Article 60(4). Pursuant to that mechanism, the European Data Protection Board ('the EDPB') is required to adopt a binding

decision, in accordance with the dispute resolution process under Article 65, concerning all the matters which are the subject of any relevant and reasoned objections.

- 1.6 On 8 September 2020, the EDPB formally commenced the dispute resolution process under Article 65. The binding decision of the EDPB, Decision 1/2020, under Article 65(1)(a) ('the EDPB Decision') was adopted by the EDPB on 9 November 2020. The EDPB Decision was notified to the Commission on 17 November 2020. In accordance with Article 65(6), the Commission is required to adopt its final decision in this case on the basis of the EDPB Decision without undue delay and at the latest by one month after the EDPB has notified the EDPB Decision to the Commission.
- 1.7 The Commission hereby adopts this Decision, pursuant to Article 60(7) in conjunction with Article 65(6). In accordance with Article 65(5), the EDPB Decision (attached at Annex II) will be published on the website of the EDPB "without delay" after the Commission has notified this Decision to TIC in accordance with Article 60(7).

Background – in brief

- 1.8 The facts, as established during the course of the Inquiry, are as set out below in Section 4. At this point, it is useful to set out, in summary, the background facts that led to this Decision.
- 1.9 As set out above, this Decision considers whether TIC met its obligations under the GDPR in relation to a personal data breach which TIC notified to the Commission at 18:08 Greenwich Mean Time ('GMT') on 8 January 2019. Specifically, it examines the issue of a controller's compliance with the obligation to notify the relevant supervisory authority of a personal data breach in accordance with Article 33(1) GDPR, as well as a controller's obligation to document a personal data breach, as set out in Article 33(5) GDPR.
- 1.10 Twitter is a "microblogging" and social media platform that was launched in July 2006 and has 187 million daily users,¹ with a 6.48% share of the European social media market.² Users have the opportunity to document their thoughts in "tweets", which at the time of writing, are limited to 280 characters in the English language. Twitter was recently found to be the 45th most visited website in the world.³
- 1.11 The personal data breach that is the subject of this Decision ('the Breach') relates to a "bug"⁴ in Twitter's design. A user of Twitter can decide if their tweets will be "protected" or "unprotected".

¹https://s22.q4cdn.com/826641620/files/doc_financials/2020/q3/Q3-2020-Shareholder-Letter.pdf (Twitter Q3 2020 Letter to Shareholders, 29 October 2020, page 12)

² <https://gs.statcounter.com/social-media-stats/all/europe> (up to date as of 4 December 2020)

³ <https://www.alexa.com/topsites> (up to date as of 4 December 2020)

⁴ A bug is an unintentional feature embedded in the "code", i.e. the stream of computing language that constructs a piece of software, which results in a fault that the authors of the code did not anticipate, or that simply arose due to human error.

In the former case, only a specific set of persons (followers) can read the user's protected tweets. The bug that resulted in this data breach meant that, if a user operating an Android device changed the email address associated with that Twitter account, their tweets became unprotected and consequently were accessible to the wider public without the user's knowledge.

- 1.12 TIC informed the Commission 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. TIC confirmed that it dates the bug to 4 November 2014, but it also confirmed that they can only identify users affected from 5 September 2017. In this regard, it is possible that more users were impacted by the Breach.

2. LEGAL FRAMEWORK FOR THE INQUIRY

Outline of inquiry process

- 2.1 The legal basis of the Inquiry and an outline of the conduct of the Inquiry is set out below. Firstly, and by way of brief explanation, the Inquiry in this case was conducted by an appointed investigator in the Commission under Section 110 of the 2018 Act ('the Investigator').

The decision-making process for the Inquiry which applies to this case is provided for under Section 111 of the 2018 Act, and requires that the Commission must consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised. This function is performed by me in my role as the decision-maker in the Commission. In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Investigator as well as any other materials which have been furnished to me by TIC (to include the submissions made by TIC on the Preliminary Draft), and any other materials which I consider to be relevant, in the course of the decision-making process.

The table below sets out, in summary form, a chronology of the process of the Inquiry, leading up to the decision making stage, in this particular case.

22 January 2019	Commencement of Inquiry by Commission (by appointed Investigator)
25 January, 1 February, 8 February 2019	Written submissions received from TIC
28 May 2019	Draft Inquiry Report issued to TIC for submissions
17 June 2019	Submissions in relation to Draft Report received from TIC

16 July 2019	Request for clarification by Commission in respect of Submissions in relation to Draft Report
19 July 2019	Response / further submissions from TIC
18 October 2019	Final Inquiry Report, and associated materials, transmitted to decision-maker by Investigator
21 October 2019	Copy of Final Inquiry Report issued to TIC and commencement of decision-making stage
22 October 2019	Letter issued to TIC confirming commencement of decision-making stage. [The letter issued to TIC on this date but was erroneously dated 18 October 2019]
14 March 2020	Preliminary Draft issued to TIC for the purpose of allowing TIC to furnish its submissions on same.
27 April 2020	TIC Submissions in relation to Preliminary Draft furnished to Commission. Having carefully considered and taken account of TIC's submissions, the Draft Decision was prepared by Commission for issue to other concerned supervisory authorities in accordance with the process under Article 60, GDPR.

TIC as controller

- 2.2 In commencing the Inquiry, the Investigator within the Commission 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. In this regard, TIC confirmed that it was the controller, both in its notification to the Commission on 8 January 2019 and in correspondence to the Commission during the course of the Inquiry.

Competence of the Commission

- 2.3 The Investigator was further satisfied, in commencing the Inquiry, that the Commission was competent to act as lead supervisory authority, within the meaning of Article 56(1) of the GDPR, in respect of cross-border processing carried out by TIC (within the meaning of Article 4(23)(b) GDPR)⁵, in relation to the personal data that was the subject of the Breach.

⁵ The Investigator initially understood, as reflected in the Notice of Commencement of Inquiry and in the Draft Report, that cross-border processing within the meaning of Article 4(23)(b) was applicable. However, as TIC's "main establishment" in the EU is located in Ireland, this was clarified in the Final Report, following on from submissions made by TIC, to reflect the fact that TIC was engaged in cross-border processing within the meaning of Article 4(23)(a).

The GDPR contains specific rules on the competence of supervisory authorities where processing of personal data is carried out on a cross-border basis. In this regard, Article 56 GDPR provides that the supervisory authority of the “main establishment” of a controller shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller in accordance with the procedure provided in Article 60 GDPR.⁶

The term “*main establishment*” is defined, in respect of a controller, by Article 4(16) GDPR as “...*the place of its central administration in the Union*” where “*decisions on the purposes and means of the processing of personal data are taken.*”⁷

Specifically, in this regard, TIC confirmed to the Commission, in notifying the Breach, that it was “*an Irish company, established in Dublin, Ireland...the provider of the Twitter services in Europe.*” Furthermore, the Investigator also noted that TIC, in its Privacy Policy, informed users of the Twitter service in the EU that they “*have the right to [raise a concern about TIC’s use of their information] with your local supervisory authority or Twitter International Company’s lead supervisory authority, the Irish Data Protection Commission.*” I am, therefore, satisfied that the Commission is the lead supervisory authority within the meaning of the GDPR, for TIC, as controller in respect of the cross-border processing carried out by TIC in relation to the personal data that was the subject of the Breach.

- 2.4 In terms of its corporate structure, TIC is an unlimited company and is incorporated in the Republic of Ireland (registered number 503351). As stated in its Annual Report and Financial Statements,

“the holding and controlling parties of the company are T.I. Group V LLC and T.I. Partnership III G.P. 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. (‘NYSE’).”⁸

Legal basis for Inquiry

- 2.5 As stated above, the Inquiry was commenced pursuant to Section 110 of the 2018 Act. By way of background in this regard, under Part 6 of the 2018 Act, the Commission has the power to commence an inquiry on several bases, including on foot of a complaint, or of its own volition.
- 2.6 Section 110(1) of the 2018 Act provides that the Commission may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, cause such inquiry as it thinks fit

⁶ GDPR, Article 56

⁷ GDPR, Article 4(16)(a)

⁸ Twitter International Company, Annual Report and Financial Statements, Financial Year Ended 31 December 2018. This was the position as at 22 May 2020, being the date on which the Draft Decision was issued. For the avoidance of doubt, this remains the position as set out in the Annual Report and Financial Statements, Financial Year Ended 31 December 2019, filed by TIC on 5 October 2020.

to be conducted, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR.

Section 110(2) of the 2018 Act provides that the Commission may, for the purposes of Section 110(1), where it considers it appropriate to do so, cause any of its powers under Chapter 4 of Part 6 of the 2018 Act (excluding Section 135 of the 2018 Act) to be exercised and / or cause an investigation under Chapter 5 of Part 6 of the 2018 Act to be carried out.

Conduct of Inquiry

- 2.7 As set out above, the Inquiry was commenced on 22 January 2019 for the purpose of examining and assessing the circumstances surrounding the notification by TIC to the Commission of the Breach. TIC's notification of the Breach was made by way of an e-mail to the Commission on 8 January 2019 at 18:08 (GMT), which attached a completed version of the Commission's Cross-Border Breach Notification Form ('the Breach Notification Form'). In that form, TIC outlined that

*"On 26 December 2018, we received a bug report through our bug bounty program 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."*⁹

The Breach Notification Form further outlined, in respect of the reasons for not notifying within the 72 hour period required by Article 33(1), that

*"The severity of the issue - and that it was reportable - was not appreciated until 3 January 2018 at which point Twitter's incident response process was put into action."*¹⁰

- 2.8 The Breach Notification Form identified the potential impacts for affected individuals, as assessed by TIC, as being "significant".¹¹
- 2.9 The Breach Notification Form also indicated that, in respect of the number of persons affected by the Breach and where they were located, that *"Our investigation is ongoing and we will supplement this response when available."*¹²

In the Breach Notification Form, TIC also stated, at section 7.1, in response to the question *"Have you informed affected individuals?"* that *"No – they will not be informed"*. The Commission (through its breach notification unit) subsequently wrote to TIC on 11 January 2019 in relation to the Breach

⁹ Breach Notification Form (8 January 2019), Section 2.8

¹⁰ Ibid, Section 3.2

¹¹ Ibid, Section 5.6

¹² Ibid, Section 5.3

noting certain categories of information that had not been provided to the Commission by TIC and requesting clarification on same. Subsequent to this, TIC submitted an updated Breach Notification Form to the Commission on 16 January 2019 (the 'Updated Breach Notification Form'), in which the same response was stated to Question 7.1 again. However, in response to Question 7.3 "*When do you intend to inform or update the affected individuals?*", TIC's reply was "*We will be providing user notice on 17 January 2019*".

- 2.10 As set out above, in addition to the Breach Notification Form received by the Commission on 8 January 2019, TIC sent a further, updated notification to the Commission on 16 January 2019. This Updated Breach Notification Form confirmed the number of affected EU and EEA users as being 88,726. It also confirmed that the bug which led to the Breach "*was introduced on 4 November 2014 and fully remediated by 14 January 2019*" and goes on to state, in that regard, that

*"The 88,726 people [identified in response to Section 5.4] reflects only the people we can identify from the period of 5 September 2017 to 11 January 2019. Due to retention limitations on available logs, we cannot identify all impacted persons, however, we believe that additional people were impacted during the period from 4 November 2014 and 14 January 2019 when the issue was fully remediated."*¹³

- 2.11 As 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, the Commission deemed it appropriate to commence an inquiry for the purpose of examining whether TIC had complied with its obligations under Article 33, GDPR, and more particularly, with its obligations under Article 33(1) and Article 33(5).
- 2.12 TIC was informed of the commencement of the Inquiry by way of a Notice of Commencement of Inquiry dated 22 January 2019 ('the Notice') from the Investigator. The Notice set out the scope and legal basis of the Inquiry. It also requested TIC to provide to the Commission all information in TIC's possession which, pursuant to Article 33(5), it had documented comprising the facts relating to the Breach, its effects and the remedial action taken. The Notice also requested TIC to provide the Commission with all relevant supporting documentary evidence.
- 2.13 TIC responded to the Notice by way of correspondence, with enclosed documentation, dated 25 January 2019 ('Submissions dated 25 January 2019').
- 2.14 Following this, and arising from the information and documentation provided by TIC in its Submissions dated 25 January 2019, two further requests for information and / or clarification were made by the Investigator to TIC, in correspondence dated 29 January 2019 and 6 February 2019, respectively. The purpose of these additional requests for information was to clarify certain facts relating to, *inter alia*:

¹³ Updated Breach Notification Form (16 January 2019), Section 5.7

- i. the timeline of the incident comprising the Breach; and
- ii. the timeline of the notification of the Breach to the Commission, including the question of when TIC (as controller) became aware of the Breach relative to when the notification was made.

TIC responded to the further requests for information and / or clarification by way of correspondence, and enclosed documentation, dated 1 February 2019 ('Submissions dated 1 February 2019') and further correspondence, with enclosed documentation, dated 8 February 2019 ('Submissions dated 8 February 2019').

- 2.15 Having received TIC's submissions, dated 25 January 2019, 1 February 2019 and 8 February 2019, the Investigator proceeded to prepare a draft inquiry report ('the Draft Report') wherein he set out his provisional views as to whether, in notifying the Breach to the Commission, TIC had complied with its obligations under Article 33(1) and Article 33(5), GDPR. The Draft Report was provided to TIC on 28 May 2019 and TIC was invited to make submissions in respect of same by 11 June 2019. On 30 May 2019, TIC sought an extension of time, until 17 June 2019, within which to make its submissions, and TIC's request in this regard was granted by the Commission.
- 2.16 TIC furnished its submissions in respect of the Draft Report to the Commission on 17 June 2019 ('Submissions in relation to the Draft Report'). Arising from TIC's Submissions in relation to the Draft Report, the Investigator considered it appropriate to refer a small number of additional queries to TIC in order to clarify issues relating to the matter of when TIC, as controller, had become aware of the Breach. These queries were forwarded to TIC on 16 July 2019, and TIC provided a response to same on 19 July 2019.
- 2.17 Having received TIC's response dated 16 July 2019, the Investigator prepared the final inquiry report ('the Final Report'). In doing so, the Investigator considered TIC's Submissions in relation to the Draft Report and took account of same, as is set out in the Final Report at Section D.3.5 and in Appendix 2 thereof.
- 2.18 During the course of the Inquiry, following the provision of the Draft Report to TIC for its submissions and in its correspondence enclosing its Submissions in relation to the Draft Report, TIC requested a meeting with the Commission. This was, as outlined by TIC, on the basis of TIC's view that certain factual 'nuances' or 'subtleties' were being lost in the written correspondence exchanged between TIC and the Commission.

In this regard, TIC stated, in its letter to the Investigator enclosing its Submissions in relation to the Draft Report, that it was requesting a meeting with the Investigatory team *"...to discuss some of the open concerns presented by the DPC's Draft Inquiry Report."*¹⁴ In circumstances where TIC was

¹⁴ Submissions in relation to the Draft Report, response dated 17 June 2019

afforded an opportunity to make submissions in respect of the contents of the Draft Report, prior to it being finalised and sent to me, and in circumstances where the Inquiry was ongoing, the Investigator did not consider that it was necessary or appropriate for such a meeting to take place. The Investigator communicated this to TIC by way of correspondence dated 21 June 2019.

2.19 The Final Report was provided to me on (Friday) 18 October 2019 and was sent to TIC on (Monday) 21 October 2019. The decision-making phase of this Inquiry, therefore, commenced on 21 October 2019. In terms of its contents, the Final Report sets out the factual background, and the scope and legal basis, for the Inquiry. It also provides an outline of the facts, as established during the course of the Inquiry, in respect of TIC's notification of the Breach to the Commission and TIC's documentation of the Breach, and having regard to the information and documentation provided by TIC to the Commission. The Final Report further sets out the Investigator's views as to whether, in respect of these matters, TIC complied with its obligations under Articles 33(1) and 33(5), GDPR.

- In this regard, in relation to Article 33(1), the Investigator's view was that, on the basis of the information and documentation provided by TIC, **it was not possible to ascertain whether TIC had complied with its obligations under Article 33(1)** to notify the Breach without undue delay or within 72 hours.
- In relation to Article 33(5), the Investigator's view was that, on the basis of the information and documentation supplied by TIC, **TIC had failed to comply with its obligation, under Article 33(5), to document the Breach** in such a manner as to enable the Commission to verify TIC's compliance with Article 33(1).

3. LEGAL FRAMEWORK FOR THE DECISION

3.1 As set out above, this Decision is made by the Commission, acting through me as the decision maker at the Commission, in accordance with Section 111 of the 2018 Act. Section 111 of the 2018 Act provides as follows:

- (1) *"Where an inquiry has been conducted of the Commission's own volition, the Commission, having considered the information obtained in the inquiry, shall –*
 - (a) *If satisfied that an infringement by the controller or processor to which the Inquiry relates has occurred or is occurring, make a decision to that effect, and*
 - (b) *If not so satisfied, make a decision to that effect.*
- (2) *Where the Commission makes a decision under subsection (1)(a), it shall, in addition, make a decision –*

- (a) *As to whether a corrective power should be exercised in respect of the controller or processor concerned, and*
- (b) *Where it decides to so exercise a corrective power, the corrective power that is to be exercised.*
- (3) *The Commission, where it makes a decision referred to in subsection (2)(b) shall exercise the corrective power concerned.”*

- 3.2 In accordance with Section 111, it is for me, as the sole member of the Commission, to consider the information obtained during the Inquiry; to decide whether an infringement is occurring or has occurred; and if so, to decide on the corrective powers, if any, to be exercised, as outlined in Section 111(2).

In so doing, I am required to carry out an independent assessment of all of the materials provided to me by the Investigator plus any further materials provided to me during the decision-making phase, to include any submissions from TIC.

- 3.3 Given that the Commission is the lead supervisory authority under Article 56(1) GDPR for the purposes of the data processing operations at issue, I was obliged under Article 60(3) GDPR to complete a draft decision to be provided to any supervisory authorities concerned, as defined in Article 4(22).
- 3.4 As set out above at paragraph 1, this document is the final Decision, as adopted by the Commission pursuant to Article 60(7) in conjunction with Article 65(6) GDPR.

Decision-making process – materials considered

- 3.5 As set out above, the Final Report was transmitted to me on (Friday) 18 October 2019, together with the Investigator’s file, containing copies of all correspondence exchanged between the Investigator and TIC; and copies of all submissions made by TIC, including the Submissions in relation to the Draft Report. (A full schedule of all documentation considered by me for the purpose of my preparation of this Decision is appended hereto). I commenced the decision-making phase of the Inquiry on (Monday) 21 October 2019 and issued a letter to TIC, on 22 October 2019, to confirm the commencement of the decision-making process. (As noted above, this letter was erroneously dated 18 October 2019, reflecting the date on which the Final Report and materials were transmitted to me).
- 3.6 Following the commencement of the decision-making process, TIC repeated its request, directly to me, for a meeting with the Commission (as outlined above at 2.18) on the basis of its view that the “*subtleties of what transpired...*” were lost in the written correspondence exchanged. I wrote to TIC (on 11 November 2019 and again on 28 November 2019) in relation to their request for a meeting.

In this regard, I outlined that my preference was for TIC to deal with any issues by way of written submissions to the Commission. This was, in particular, due to the fact that any matters relating to the fact-finding aspects of the Inquiry or relating to TIC's position on either legal or evidential matters considered in the Final Report which might be discussed during the course of a meeting would ultimately have to be committed to writing for the purpose of my preparation of a draft decision under Article 60 GDPR. On this basis, I invited TIC to make further written submissions to me on any issues in respect of which TIC believed that subtleties had been lost in correspondence or which it believed to comprise 'open concerns' (as had been raised by TIC in its letter dated 17 June 2019 enclosing its Submissions in relation to the Draft Report).

3.7 TIC furnished a response, dated 2 December 2019, wherein it set out further submissions in respect of three issues, relating to, respectively,

- the background to the breach notification made to the Commission on 8 January 2019 and the contents of same;
- the issue of when TIC became aware of the Breach, in relation to when it submitted the breach notification, and information / documentation provided by TIC to the Investigator in this regard; and
- the documentation of the Breach.

3.8 Having reviewed the submissions made by TIC on 2 December 2019 ('Submissions dated 2 December 2019'), it appeared to me that they comprised issues that had already been raised by TIC with the Commission, and which had been considered by the Investigator, during the course of the Inquiry. It further appeared to me that TIC's submissions on these issues had been taken into account by the Investigator. Notwithstanding this, I carefully considered TIC's further Submissions dated 2 December 2019 as part of my independent assessment of all materials. I corresponded with TIC to confirm this by letter dated 13 February 2019.

3.9 Having reviewed the Final Report, and the other materials provided to me by the Investigator (including the submissions made by TIC), I was satisfied that the Inquiry was correctly conducted and that fair procedures were followed throughout, including, but not limited to, notifications to the controller and opportunities for the controller to comment on the Draft Report before it was submitted to me as decision-maker.

3.10 Having considered the information obtained during the Inquiry, and as set out above at 3.5 – 3.9, I outlined my provisional findings in the Preliminary Draft, which was then furnished to TIC for the purpose of allowing TIC to make any submissions in respect of the provisional findings outlined therein.

TIC's submissions in relation to the Preliminary Draft

- 3.11 As outlined above, the Preliminary Draft was sent to TIC on 14 March 2020, and TIC was requested to furnish any submissions it wished to make to the Commission by 3 April 2020.
- 3.12 On 25 March 2020, TIC, through its legal advisors, sought an extension of time of six weeks (that is, up to 15 May 2020) in order to furnish its submissions. TIC's legal advisors confirmed that this was being sought in circumstances where staff in its office, and that of Twitter globally, were working from home (due to the COVID-19 pandemic) and also in circumstances where there had been a significant increase in usage of the Twitter service globally (also as a result of the COVID-19 pandemic) which had resulted in Twitter having to concentrate its resources on service delivery issues. Having considered TIC's request and the circumstances outlined therein, I considered it appropriate to grant an extension of the timeframe for receipt of submissions by a further three weeks, until 27 April 2020.
- 3.13 As already outlined, TIC furnished its submissions in respect of the Preliminary Draft by email dated 27 April 2020 ('Submissions in relation to the Preliminary Draft'). TIC made extensive submissions in respect of my provisional findings under both Article 33(1) and Article 33(5). It set out its objections to both the interpretation adopted in the Preliminary Draft in respect of those articles and to the provisional findings made in the Preliminary Draft that TIC had infringed both of those provisions. My full consideration and analysis of TIC's position on these matters contained in its submissions is outlined below. Specifically, section 7 below relates to my consideration and analysis of TIC's position in respect of my provisional finding under Article 33(1), and sections 8 and 10 below relate to my consideration and analysis of TIC's position in respect of my provisional finding under Article 33(5).

4. THE FACTS AS ESTABLISHED

- 4.1 During the course of the Inquiry, the Investigator, through requesting TIC's response to the Notice and to the queries raised in the letters dated 29 January 2019 and 6 February 2019, sought to establish the facts relating to TIC's notification of the Breach to the Commission, including the timing of same. The facts, as established during the course of the Inquiry, are set out below.
- 4.2 The starting point in terms of the facts relating to TIC's notification of the Breach is the information that was provided by TIC in the Breach Notification Form, which it sent to the Commission by e-mail on 8 January 2019 at 18:08 GMT. In that document, TIC outlined that

"On 26 December 2018, we received a bug report through our bug bounty program 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. This would render their previously protected Tweets (Tweets viewable by only approved followers of the account) public and

viewable to anyone...The bug in the code was traced back to a code change made on 4 November 2014.”¹⁵

Section 3 of the Breach Notification Form requires the party notifying to ‘Specify reasons for not informing DPC (the Commission) within 72 hours (if this is the case)’. In this section of the Breach Notification Form, TIC stated:

“The severity of the issue -- and that it was reportable -- was not appreciated until 3 January 2018 at which point Twitter’s incident response process was put into action.”¹⁶

TIC further confirmed in the Breach Notification Form that TIC was the controller in respect of the processing of personal data that was the subject of the Breach. TIC also confirmed that the Breach had arisen in the context of processing carried out on its behalf by Twitter Inc., its processor.

- 4.3 On the basis of the information, set out above, in the Breach Notification Form, the Investigator was of the initial understanding that TIC had become aware of the Breach either on 26 December 2018 or on 3 January 2019, which, in either case, meant that the notification to the Commission took place outside of the 72 hour timeframe allowed by Article 33(1), the breach notification having been made to the Commission on 8 January 2019.
- 4.4 As set out above, due to the nature of the Breach, including the number of EU/EEA users affected, and the apparent delay in notifying the Commission, the Inquiry was commenced to establish the facts.
- 4.5 It is important to note that an initial source of uncertainty, in respect of the facts surrounding the notification of the Breach to the Commission, was the language used in the Breach Notification Form, wherein the terms ‘we’ and ‘our’ were used to refer interchangeably to Twitter Inc. and TIC. During the correspondence exchanged during the course of the Inquiry, therefore, the Investigator sought and obtained clarification from TIC in relation to its language usage. TIC has itself acknowledged that the phrasing used in the Breach Notification Form (and Updated Breach Notification Form) gave rise to uncertainty and has made submissions to explain its use of language in the notification and the background to same. In this regard, in its Submissions in relation to the Draft Report, TIC outlined that:

“As is common with multinational corporate groups, employees of TIC and Twitter, Inc. habitually use “we” and “us” loosely or refer to the group by its name, for example, “Twitter”, when referring both to individual legal entities within the group of companies and/or the group of companies as a whole, without considering the implications of the distinction.

¹⁵ Breach Notification Form, Section 2.8

¹⁶ Breach Notification Form, Section 3.2

In addition, employees of TIC and Twitter, Inc. operate an internal target for submitting breach notifications to the DPC within 72 hours of someone at “Twitter” – whether that be Inc. or some other entity – becoming aware that there was a confirmed personal data breach. Depending on the sequence of events, this can be a tighter standard than that imposed by the GDPR.¹⁷

Similarly, in its Submissions dated 2 December 2019, TIC stated:

“Twitter International Company (“TIC”) is the Controller with respect to the Twitter services provided to people who reside in Europe. 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 a global group of companies (referred to herein as the “Twitter Group”). All employees of the Twitter Group use the same computer systems, they adhere to the same general policies (e.g., security, deletion, retention, human resources etc.) and work together to ensure the global round-the-clock support required to keep the Twitter platform operational. This is how we must function in order to efficiently and effectively meet our global customer’s needs.”¹⁸

- 4.6 In terms of the chronology of facts in relation to the timeline of the notification, this was set out by TIC in its various submissions to the Investigator. TIC also explained the relationship between it and the various other parties involved in the Breach.

At this point, it is useful to set out the various parties involved in the Breach, and their respective roles, as has been confirmed to the Commission by TIC:

- 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.
- The bug which led to the Breach in this case was reported to Twitter Inc. through its ‘bug bounty program,’ which is a program whereby anyone may submit a bug report. TIC has confirmed, in this regard, that the ‘bug bounty program’ *“provides a formal channel for independent security researchers to report certain kinds of security vulnerabilities, including flaws that may result in the leaking of personal data.”¹⁹*
- TIC has further confirmed that the ‘bug bounty program’ is operated on Twitter Inc.’s behalf by a third party contractor (‘Contractor 1’).
- Twitter Inc. employs an IT Security Company (‘Contractor 2’) to ‘triage’ or assess the bug reports submitted (through the ‘bug bounty program’) to Contractor 1. In this regard, TIC has explained that

¹⁷ Submissions in relation to the Draft Report, Executive Summary

¹⁸ Submissions dated 2 December 2019

¹⁹ Submissions in relation to the Preliminary Draft, para. 5.3

“Anyone may submit a report through the Twitter bug bounty program so receipt of a report does not necessarily mean that a bug exists or, if one does exist, that it is a significant one or one that may result in a personal data breach.

The role of [Contractor 2] is to establish whether a bug report is genuine and likely ‘real’, in the sense of not being a nuisance report or spam, and if that is the case, [Contractor 2] will then provide these reports to Twitter Inc.’s Information Security team for detailed investigation.”²⁰

4.7 In summary, the factual chronology in relation to the notification of the Breach, as has been confirmed by TIC in its submissions made to the Commission during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, is as follows:

- i. On **26 December 2018**, Contractor 2, the IT security company engaged by Twitter Inc. to search for and “triage” (or assess) bugs, received a bug report from Contractor 1 via the bug bounty program. The bug bounty report stated that if a Twitter user with the protected Tweets feature enabled was using Twitter for Android and changed their email address, the bug would result in the protected Tweets feature being disabled and making their previous Tweets publicly accessible on the service.
- ii. Contractor 2 assessed, or as TIC refers, “triaged”, the bug bounty report on **29 December 2018**. In its initial submissions to the Commission on 25 January 2019, TIC outlined that Contractor 2 *“did not begin their triage process until 29 December 2018”²¹* and also outlined that *“This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and [Contractor 2]. We are investigating the cause for this and it will be part of our post mortem process.”²²*

However, in its Submissions in relation to the Preliminary Draft, TIC outlined that the notification by Contractor 2 (via a JIRA ticket – see footnote 25) to Twitter Inc.’s Information Security team on 29 December *“...was in line with its contractual commitments so there was no delay in complying with the internal process requirement”* and that *“Given the nature of the majority of bug reports, this target is a reasonable and appropriate standard, and is in line with other bug bounty programs.”²³* TIC also confirmed that Contractor 2, in assessing the report, labelled the issue as being “low risk.”²⁴ (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below in section 7.)

²⁰ Submissions in relation to the Draft Report, paras 3.8, 3.9

²¹ Submissions dated 25 January 2019, Annex

²² Ibid, Annex, footnote 3

²³ Submissions in relation to the Preliminary Draft, paragraph 6.2

²⁴ In the Submissions in relation to the Preliminary Draft (para. 6.3), it is stated that *“The JIRA ticket classified the bug as low impact and low risk.”*

When Contractor 2 had completed its assessment of the report, they communicated the outcome of same to Twitter Inc. on 29 December 2018 in the form of a “JIRA²⁵ ticket”.

- iii. TIC outlined, in its submissions made during the course of the Inquiry including its Submissions in relation to the Draft Report and in its earlier Submissions²⁶ that *“as a result of the winter holiday schedule”²⁷*, Twitter Inc.’s Information Security team did not review the JIRA ticket until 2 January 2019.

In the Submissions in relation to the Preliminary Draft, TIC submitted that *“Given the initial risk classification of the Underlying Bug, this was a reasonable time period within which to review the report, taking into account that of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year’s Day)”²⁸*. At this point, Twitter Inc.’s Information Security team determined that, whilst the incident did not *“immediately trigger a security-related incident,”* it was identified as being *“a potential privacy-related concern.”²⁹* (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below at section 7.)

- iv. Following this, Twitter Inc.’s Information Security team requested its legal team to provide guidance on the privacy issue. In this regard, in its Submissions dated 1 February 2019, TIC set out a timeline of the incident, wherein it outlined as follows:

“2 January 2019 - Twitter Inc.’s Information Security Team reviewed the JIRA ticket and decided it was not a security issue but might be a privacy issue; 3 January 2019 - Twitter Inc.’s Information Security team asked Twitter Inc.’s legal team for guidance on the potential privacy issue;”

“3 January 2019 - Twitter Inc.’s legal team determined the issue may constitute a personal data breach and requested that the issue be treated as an incident and that Twitter Inc.’s Information Security incident response plan be invoked.”³⁰

The fact of Twitter Inc.’s legal team being consulted, and the question of when this took place, was also dealt with in TIC’s Submissions dated 1 February 2019, wherein it was confirmed that - *“As noted in our 25 January 2019 letter, a member of Twitter Inc.’s legal team who supports*

²⁵ JIRA is a “work management tool, from requirements and test case management to agile software development”. It facilitates the creation of tickets to manage incidents and cases in a workplace. <https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for>

²⁶ Submissions dated 25 January 2019

²⁷ Ibid, Annex

²⁸ Submissions in relation to the Preliminary Draft, paragraph 6.3

²⁹ Submissions dated 25 January 2019, Annex

³⁰ Submissions dated 1 February 2019

the Information Security team, was consulted on 3 January 2019 as part of his normal responsibilities.”³¹

In the Submissions in relation to the Preliminary Draft, however, it is stated that *“The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it).”³²* (I have considered TIC’s submissions on this issue, as set out in the Submissions in relation to the Preliminary Draft, below at section 7.)

- v. Thereafter, Twitter Inc.’s internal procedure for such incidents was commenced on **4 January 2019**. On TIC’s admission, however, the procedure was not followed correctly at that point, insofar as the Global Data Protection Officer (‘the DPO’) was not added to the incident “ticket”, which meant that TIC (as controller) was not made aware of the Breach at that time.³³ In its Submissions in relation to the Preliminary Draft, TIC again confirmed that this was the case, stating that

“The process required that the legal team and the DPO be immediately added as watchers to the ticket. This would have led to the DPO being automatically notified. This step was not followed.”

TIC also, in its Submissions in relation to the Preliminary Draft, outlined (by way of explanation as to how this deviation from the agreed process arose) that *“The Twitter Inc legal team were already involved in the incident as they had been consulted to determine whether an issue may exist and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied. As a result, the DPO was not added to the incident ticket or document and so was not automatically notified.”³⁴*

- vi. TIC has confirmed that on **7 January 2019** (at 10 am Pacific Standard Time (‘PST’)) (18:00 GMT), the DPO was notified (orally) of the Breach during a Twitter Group weekly team meeting attended by the TIC DPO³⁵. **TIC has confirmed, therefore, that this is when TIC (as controller) became aware of the Breach.**
- vii. Thereafter, TIC has confirmed that the DPO contacted (by way of an internal messaging system called, “Slack”³⁶) the Detection and Response Team (DART) leader and requested to be added

³¹ Ibid, Annex, point 2

³² Submissions in relation to the Preliminary Draft, para. 6.4

³³ Submissions dated 8 February 2019 and Submissions in relation to the Draft Report, para. 3.10

³⁴ Submissions in relation to the Preliminary Draft, para. 6.5

³⁵ Ibid, para. 7.1

³⁶ ‘Slack’ is an instant messaging / chatroom facility designed to replace email. It is described as *“a collaboration hub that can replace email to help you and your team work together seamlessly...so you can collaborate with people online as efficiently as you do face-to-face”* <https://slack.com/help/articles/115004071768-What-is-Slack->.

to the incident materials relating to the Breach. TIC has provided a copy of this message, which was sent on 7 January 2019 at 19:23 GMT. Following this, TIC has confirmed that the DPO was invited to a further meeting about the Breach at 15:30 PST (23:30 GMT) on the same date. TIC has also provided a copy of this meeting invitation.

- viii. As set out above, the Commission was notified of the Breach on the following day, just under 19 hours later, at 18:08 (GMT) on 8 January 2019.

5. ISSUES FOR DETERMINATION

Having reviewed the Report and the other materials provided to me, and having carefully considered and taken into account TIC's Submissions in relation to the Preliminary Draft, I consider that the following comprise the issues in respect of which I must make a decision:

- i. Whether TIC complied with its obligations, in accordance with Article 33(1) GDPR, to notify the Commission of the Breach without undue delay and, where feasible, not later than 72 hours after having become aware of it; and
- ii. Whether TIC complied with its obligation under Article 33(5) to document the Breach.

I have set out my findings, and my analysis in respect of same, in relation to each of the above issues below at section 7 (re. Article 33(1)) and section 10 (re. Article 33(5)). In doing so, in section 7, I have considered TIC's Submissions in relation to the Preliminary Draft, made in respect of my finding (which was set out on a provisional basis in the Preliminary Draft) in relation to Article 33(1). In sections 8 and 10, I have considered TIC's Submissions in relation to the Preliminary Draft in respect of my finding (which was set out on a provisional basis in the Preliminary Draft) in relation to Article 33(5).

Before addressing those matters, I have considered the requirements of Articles 33(1) and 33(5), at sections 6 and 8 below, respectively.

6. ISSUE I - ARTICLE 33(1)

Requirements of Article 33(1)

- 6.1 Article 33 sets out the requirements in respect of notification by a controller to the supervisory authority of a *personal data breach*.

Under Article 4(12), a personal data breach “means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”³⁷

- 6.2 At the outset of the Inquiry, the Investigator considered the information provided by TIC in the Breach Notification Form and determined, as a preliminary matter, that the incident notified comprised a personal data breach within the meaning of Article 4(12). In this regard, the Investigator considered that the incident, whereby an individual’s “Tweets” become unprotected, and consequently accessible to the wider public, without the user’s knowledge constitutes the unauthorised disclosure of, and access to, personal data.³⁸ I do not consider it necessary to consider any further the application of Section 4(12) in circumstances where it is not in dispute by TIC or by the Commission that the incident in question comprised a personal data breach.
- 6.3 Article 33(1) obliges a controller to notify a personal data breach to the competent supervisory authority unless the personal data breach is “unlikely to result in a risk to the rights and freedoms of natural persons.”³⁹

In terms of the timescale for notification of a personal data breach by a controller, Article 33(1) requires that this should take place ‘without undue delay⁴⁰ and, where feasible, not later than 72 hours after having become aware of it.’

The importance of being able to identify a breach, assess the risk to individuals and notify it promptly is emphasized in Recital 85, which provides that

*“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons...”*⁴¹

³⁷ Article 4(12), GDPR

³⁸ Personal data are defined in Article 4(1) GDPR as data “relating to an identifiable or identified natural person”. This definition has been elaborated upon by the Court of Justice of the European Union (CJEU) in *Nowak v Data Protection Commissioner* (C-434/16 ECLI:EU:C:2017:994) to clarify that any data that “by reason of its content, purpose or effect, is linked to [a particular person]” are personal data. Tweets associated with a personal account are linked by purpose (to broadcast thoughts), effect (making one’s thoughts known), and in many cases by content (i.e. personal information), to the data subject associated with that personal account. As such, the Breach meets the definition set down in Article 4(12) GDPR and elaborated on in the jurisprudence of the CJEU.

³⁹ Article 33(1), GDPR

⁴⁰ The Article 29 Working Party (now the EDPB) addressed the meaning of the term ‘undue delay’ in the context of the requirement to communicate a breach to affected individuals in its ‘Guidelines on Personal Data Breach Notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)’. In this regard, the Guidelines outline on page 20 that “The GDPR states that communication of a breach to individuals should be made “without undue delay,” which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves.”

⁴¹ Recital 85, GDPR

- 6.4 The obligation to notify, and the timing of this, is connected with when the controller becomes ‘aware’ of a personal data breach.

The Article 29 Working Party, in its *Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)* (as adopted by the EDPB) (‘the Breach Notification Guidelines’), addresses the issue of controller ‘awareness’ and, in this regard, states as follows:

“...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. However...the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. This 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.”⁴² (Emphasis added)

- 6.5 In this respect, the issue of controller ‘awareness’, and its role in terms of defining the timeframe within which notification is required to take place, must be understood in the context of the broader obligation on a controller to ensure that it has appropriate measures in place to facilitate such ‘awareness’. This requirement is reflected in Recital 87, which provides that

“It should be ascertained whether all appropriate technical and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject...”⁴³

- 6.6 Similarly, the Breach Notification Guidelines state that

“...the GDPR requires both controllers and processors to have in place appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Also the GDPR requires all appropriate technological protection and organizational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged.

⁴² Breach Notification Guidelines, page 11

⁴³ Recital 87, GDPR

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.”⁴⁴

- 6.7 Having regard to the above, therefore, it is clear that the obligations on a controller, in terms of notifying a personal data breach, must be understood within the context of the broader obligations on controllers under the GDPR, and specifically, the overarching responsibility on controllers to ensure that there is compliance with the principles of data protection, as encompassed in the accountability obligation under Article 5(2) GDPR.

In considering whether TIC, as a controller, complied with its obligation to notify a personal data breach under Article 33(1), therefore, I have firstly considered (below) the objectives underlying this obligation and the broader context in which this obligation arises. At this point, it is appropriate to note that, in its Submissions in relation to the Preliminary Draft, TIC raised objections to the interpretative approach which was outlined in the Preliminary Draft with regard to the meaning and effect of Article 33(1). I consider TIC’s position on this issue [in the course of the analysis that follows] in section 7 below.

Controller responsibility

- 6.8 The role and concept of a ‘controller’ was addressed by the Article 29 Working Party in its 2010 *Opinion on the concepts of “controller” and “processor”*⁴⁵. (Although this Opinion relates to Directive 95/46, the concepts of controller and processor have not changed under the GDPR).⁴⁶

Discussing the concept of ‘controller’, the Opinion refers to the numerous responsibilities and obligations of the controller under Directive 95/46 and states that

“...the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words, to allocate responsibility. This goes to the heart of the Directive, its first objective being “to protect individuals with regard to the processing of personal data”. That objective can only be realized and made effective in practice, if those who are responsible for data processing can be sufficiently stimulated by legal and other means to take all measures that are necessary to ensure that this protection is delivered in practice...”⁴⁷ (Emphasis added)

The Guidelines go on to state that

⁴⁴ Breach Notification Guidelines, page 6

⁴⁵ Article 29 Data Protection Working Party ‘Opinion 1/2010 on the concepts of “controller” and “processor”’

⁴⁶ The EDPB published new guidelines on the concept of controllership on 7 September 2020 – *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. These guidelines were not in existence at the time of the Preliminary Draft or Draft Decision and, therefore, the analysis which follows (on which TIC was given the opportunity to make submissions) does not refer to these new guidelines.

⁴⁷ Article 29 Data Protection Working Party ‘Opinion 1/2010 on the concepts of “controller” and “processor”’, page 4

“In terms of the objectives of the Directive, it is most important to ensure that the responsibility for data processing is clearly defined and can be applied effectively.”⁴⁸

- 6.9 The CJEU has also associated the definition, or concept, of controllership with the presence of overall responsibility. In this regard, the CJEU has held that once controllership as a matter of fact has been established for a particular processing operation, equivalent responsibility must follow.⁴⁹

CJEU jurisprudence dealing with the issue of controllership also demonstrates how the CJEU has applied a broad interpretation of the concept of controllership in order to ensure the highest level of protection of data subject rights.⁵⁰

Accountability

- 6.10 In order to ensure that controller responsibility for the processing of personal data is applied more effectively, the principle of *accountability* was specifically incorporated, as a central principle, into the GDPR. While the principle of accountability was expressly enunciated in the text of the GDPR, the principle was already established in EU data protection law prior to the application of the GDPR.

In this regard, the Article 29 Working Party in its *Opinion on the principle of accountability*⁵¹ outlined that the purpose of including an accountability principle, within a legislative framework, would be to “...reaffirm and strengthen the responsibility of controllers towards the processing of personal data...” and further stated that such a provision would focus on two elements, being “the need for a controller to take appropriate and effective measures to implement data protection principles” and the need to demonstrate upon request that appropriate and effective measures have been taken...”⁵²

In terms of what is meant by the principle of ‘accountability’, the Article 29 Working Party also stated that “In general terms...its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance.”⁵³ In a similar vein, the European Data Protection Supervisor (EDPS), in its guidelines on accountability, states that “[a]ccountability means that the controller is in charge of ensuring compliance and being able to demonstrate compliance.”⁵⁴

- 6.11 In the GDPR, the issue of controller accountability is specifically addressed in Article 5(2) and Recital 74. Recital 74, in this regard, provides that

⁴⁸ Ibid, page 7

⁴⁹ Case 25/2017 *Tietosuojavaltuutettu Other party: Jehovan todistajat — uskonnollinen yhdyskunta*, paras 63-69.

⁵⁰ Case 210/2016 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, paras 26-44

⁵¹ Article 29 Data Protection Working Party ‘Opinion 3/2010 on the principle of accountability’, Page 8

⁵² Ibid, pages 8 and 9

⁵³ Ibid, page 7

⁵⁴ EDPS, ‘Accountability on the Ground: Guidance on Documenting Processing Operations for EU Institutions, Bodies and Agencies (v 1.3 July 2019) Section 3

“The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures.”⁵⁵

Article 5(2) then places overall responsibility for compliance with the accountability principle on the controller, stating, in this regard, that the controller *shall be responsible* for compliance with the data protection principles set out in Article 5(1), and in addition, that the controller *shall be able to demonstrate* such compliance.

Controller obligations under the GDPR

- 6.12 Controller responsibility for the processing of personal data is more specifically articulated in a number of other provisions of the GDPR. Whilst this Inquiry has not considered the question of compliance with those provisions and, therefore, makes no findings in respect of these provisions in the context of the present circumstances under examination, I have referred to them simply for the purposes of considering how the GDPR addresses the issue of controller responsibility.
- 6.13 At this juncture, it is of note that, in TIC’s Submissions in relation to the Preliminary Draft, it does not agree with the Commission’s consideration of other provisions of the GDPR (namely Articles 5(2), 24, 25 and 32) in the context of its examination of the meaning and effect of the controller obligation under Article 33(1). In this regard, TIC asserts (in its submissions) that the Commission, in its Preliminary Draft, de facto extended the scope of the Inquiry to consider compliance with these provisions and that it relies on inferences to the effect that TIC has not complied with these provisions⁵⁶. I deal with TIC’s submissions on these points below in section 7 in detail. However, for the present purposes, I emphasise, in the strongest possible terms, that this Inquiry and this Decision is solely concerned with the question of compliance with Articles 33(1) and 33(5) by TIC. No findings are made in respect of any other provisions of the GDPR and, contrary to TIC’s assertion, neither are there any inferences to the effect of findings in respect of compliance with any other provisions.

However, as detailed below at section 7, having considered the submissions of, and CJEU case law referred to by, TIC, I consider that it is appropriate to have regard to the overall context of the controller responsibilities contained in the GDPR when interpreting the meaning and effect of Article 33(1) in a real life scenario. I do not accept, however, that such an analysis amounts to a direct or de facto examination of TIC’s compliance with any other obligations. Rather, its purpose is simply to assist in understanding Article 33(1) within the context of the broader obligations on controllers under the GDPR.

⁵⁵ Recital 74 GDPR

⁵⁶ Submissions in relation to the Preliminary Draft, para. 9.3

6.14 The overall responsibility of the controller for the processing of personal data is established in Article 24 of the GDPR (*‘Responsibility of the Controller’*), which provides that a controller ...*“shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation...”*⁵⁷

6.15 Article 25 (*‘Data Protection by Design and by Default’*) then imposes an obligation on a controller to ensure that it has *appropriate* technical and organizational measures in place that are designed to implement the data protection principles in Article 5.

The EDPB has considered the meaning of the term *‘appropriate’* in the context of Article 25 of the GDPR in its *Guidelines on Article 25 Data Protection by Design and by Default*. In this regard, the EDPB has stated that, in order to be *‘appropriate’*, the technical and organizational measures applied by a controller must be

*“...suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness.”*⁵⁸

6.16 Of more specific relevance in the context of the requirements under Article 33(1), is the obligation on controllers, under Article 5(1)(f) and Article 32, to have appropriate technical and organizational measures in place to ensure the security of personal data. This includes the requirement (in Article 32(2)) that a controller shall, in assessing the appropriate level of security, take account

*“in particular of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”*⁵⁹

Similarly, Recital 83 provides that the impact of a potential personal data breach to data subjects should comprise a major aspect of the risk assessment exercise:

*“In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.”*⁶⁰

6.17 It is of note that both Article 25 and Article 32, in obliging controllers to implement appropriate technical and organizational measures, require controllers to do so, *“taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well*

⁵⁷ Article 24, GDPR

⁵⁸ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 Nov 2019), page 6

⁵⁹ Article 32(2), GDPR

⁶⁰ Recital 83 GDPR

as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing...⁶¹ (Emphasis added)

In this regard, in implementing the measures in question, controllers are obliged to take into account the inherent characteristics of the processing; the size and range of the processing; the context of the processing, which may influence the expectations of the data subject; and the aims of the processing.⁶² In addition, controllers are obliged to adopt a risk based approach in determining the appropriate technical and organizational measures to be applied.

- 6.18 In circumstances where a controller engages a processor, the overarching accountability obligation of the controller to ensure compliance with the data protection principles will, necessarily, require the controller to ensure that any contract, or arrangement, which it has with a processor is effective in enabling the controller to comply with *its* obligations. Article 28, in this regard, imposes a positive obligation on controllers to

*“...only use processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”*⁶³

It further provides (at Article 28(3)(f)) that any such contract should stipulate, *inter alia*, that the processor “*assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36...*”

- 6.19 This requirement of assistance by a processor, referred to in Article 28(3)(f), in the context of the notification of personal data breaches, is reflected in Article 33(2), which provides that

*“The processor shall notify the controller without undue delay after becoming aware of a personal data breach.”*⁶⁴

Whilst the processor is required to ‘assist’ the controller in meeting the obligation to notify, however, this requirement of assistance does not amount to a shift in responsibility. The responsibility to notify in compliance with Article 33(1), and to ensure that it has sufficient measures in place to facilitate such compliance, remains that of the controller. In this regard, the Breach Notification Guidelines provide that

⁶¹ Article 25, GDPR; Article 32, GDPR

⁶² EDPB Guidelines 4/2019, page 9

⁶³ Article 28, GDPR

⁶⁴ Article 33(2), GDPR

“The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification.”⁶⁵

- 6.20 In summary, therefore, and having regard to the above, the obligations on a controller in terms of notifying a personal data breach under Article 33(1), 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 governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.

The Breach Notification Guidelines⁶⁶ refer, in this regard, to breach notification as *“a tool enhancing compliance in relation to the protection of personal data”⁶⁷* and further state that

“controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority...Notification to the Supervisory Authority should form a part of that incident response plan.”⁶⁸

I have already noted above that TIC, in its Submissions in relation to the Preliminary Draft, objected (on a number of grounds) to the interpretation of Article 33(1) in the context of the broader obligations on controllers under the GDPR. I have addressed TIC’s submissions on this issue below at section 7 herein.

7. ISSUE 1 – TIC’S COMPLIANCE WITH ARTICLE 33(1)

Analysis of facts relating to TIC’s notification of the Breach

- 7.1 Having regard to the above, in the context of the facts giving rise to this Inquiry, I now turn to consider whether TIC complied with its obligation to notify the Commission in accordance with Article 33(1). In so doing, I firstly consider the issue of TIC’s ‘awareness’ of the Breach. This is necessary in circumstances where the obligation to notify, under Article 33(1), is addressed to the controller and where the required timeframe for notification is stated to be *“without undue delay and, where feasible, not later than 72 hours after having become aware of it.”*

⁶⁵ Breach Notification Guidelines, page 13

⁶⁶ *Guidelines on Personal data breach notification under Regulation 2016/679 (Adopted on 3 October 2017; As last Revised and Adopted on 6 February 2018)* (as adopted by the EDPB)

⁶⁷ Ibid, page 5

⁶⁸ Ibid, page 6

- 7.2 The question of when TIC (as controller), as distinct from Twitter (as processor) became aware of the personal data breach was examined by the Investigator during the course of the Inquiry. This issue also informed the Investigator's finding in respect of Article 33(1), which is a matter that I address below.

Before setting out my findings, therefore, it is useful to consider how the issue of when TIC became 'aware' of the Breach, and, more importantly, the facts as to how this took place, evolved during the course of the Inquiry.

- 7.3 As set out above, at paragraphs 4.2 to 4.5, the Commission's understanding of when TIC was 'aware' of the Breach was initially informed by the contents of the Breach Notification Form. This referred to 'Twitter' generically - i.e. without specifying which 'Twitter' entity was at issue - as having received the bug report on **26 December 2018**, and further explained that the reason for the delayed notification to the Commission was that *'Twitter' had not appreciated the severity of the issue, and that it was reportable, until the 3 January 2019 "at which point Twitter's incident response plan was put into action."*⁶⁹

Arising from the Breach Notification Form, it initially appeared to be the case that TIC was aware of the Breach on 26 December 2018 or on 3 January 2019. In either case, this meant that the notification to the Commission had taken place outside of the 72 hour timeframe allowed by Article 33(1) as it had been made on 8 January 2019.

- 7.4 As also set out above, TIC made submissions, both in relation to the Draft Report and by way of letter dated 2 December 2019, wherein it explained the background to the format of its notification to the Commission and, in particular, the language used in the Breach Notification Form. It also set out an explanation in relation to the timing of the notification of the Breach, stating in this regard that

*"Since 25 May 2018, when an employee of the Twitter Group **confirms** a breach (i.e. actual confirmation of a breach as opposed to a report of a potential breach that requires investigation) to exist, the policy was to begin the running of the 72 hour reporting timeframe from that point."*⁷⁰

As noted previously above, TIC also submitted (in its Submissions in relation to the Draft Report) that:

*"...employees of TIC and Twitter Inc. operate an internal target for submitting breach notifications to the DPC within 72 hours of someone at "Twitter" – whether that be Inc. or some other entity – becoming aware that there was a confirmed personal data breach. Depending on the sequence of events, this can be a tighter standard than that imposed by the GDPR..."*⁷¹

⁶⁹ Breach Notification Form, Section 3.2

⁷⁰ Submissions dated 2 December 2019

⁷¹ Submissions in relation to the Draft Report, Executive Summary

“Since more than 72 hours had elapsed since the personal data breach was known by a Twitter Group employee, TIC believed that it had failed to meet its internal standard and so TIC filled out the “reasons for delay” to explain why this was the case, without considering when TIC itself became aware of the Breach for the purposes of Article 33(1).”⁷²

TIC further outlined that:

“It is with this background that on 8 January 2019 TIC submitted the Breach Report that would result in In-19-1-1 (the “Breach Report”) to the DPC and why the Breach Report (a) stated that it was being made outside the 72 hour reporting window, and (b) used terminology including “Twitter” and “we”. Indeed, when TIC began submitting breach notifications following 25 May 2018, TIC did so according to (a) a 72 hour clock that began to run when an employee of the Twitter Group confirmed a breach, and (b) using terminology including “Twitter” and “we”.

When the Investigator questioned when TIC – as a distinct legal entity – became aware of the breach, an examination of the timelines of the incident at issue in IN-19-1-1 was conducted. The earliest date at which TIC became aware of the breach was when TIC’s Data Protection Officer was made aware of the issue on 7 January 2019, the day before the Breach Report was submitted...”⁷³

- 7.5 In its first submission to the Investigator, dated 25 January 2019, by way of response to the Notice of Commencement of the Inquiry (the ‘Notice’), TIC provided an overview of the Breach and, in particular, of the timeline in terms of the involvement of various parties within Twitter Inc. and TIC.

In this regard, TIC outlined that the bug report was received by Contractor 2 on 26 December 2018 and was assessed, or “triaged”, by it on 29 December 2018, following which a notification was created, via a JIRA ticket, to Twitter Inc.’s Information Security team. TIC also outlined, in that regard, that *“This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and Contractor 2. We are investigating the cause for this and it will be part of our post mortem process.”⁷⁴*

However, in its Submissions in relation to the Preliminary Draft, TIC stated that the timeframe in relation to Contractor 2’s review of the bug report actually did not represent a delay or deviation from the agreed process between Twitter Inc. and Contractor 2. In this regard, TIC stated that Contractor 2 was subject to a service level at the time of the Breach, and it confirmed that, in notifying Twitter Inc.’s Information Security team on 29 December 2019, Contractor 2 acted in line with its contractual commitments *“so there was no delay in complying with the internal process*

⁷² Submissions in relation to the Draft Report, para 2.4

⁷³ Submissions dated 2 December 2019

⁷⁴ Submissions dated 25 January 2019, Annex, footnote 3

*requirement.*⁷⁵ (TIC did not specify what that service level required in terms of the timeframe for Contractor 2 completing assessments of such bug reports).

TIC further outlined, in its Submissions in relation to the Preliminary Draft, that the service level to which Contractor 2 was subject had since been revised and that “[Contractor 2] is now required to action all submissions within 24 business hours, unless it is granted an SLA extension for a particular report. It may only apply for an SLA extension where a report requires more than three hours for technical triage.”⁷⁶

- 7.6 TIC also outlined, in its Submissions dated 25 January 2019 that “as a result of the winter holiday schedule the internal Twitter security team did not review the 29 December ticket ...until 2 January 2019.”⁷⁷

In its Submissions in relation to the Preliminary Draft, TIC submitted that the time period between the submission of the JIRA ticket by Contractor 2 to Twitter Inc. on 29 December 2019 and its review by Twitter Inc.’s Information Security team was reasonable, given the initial classification by Contractor 2 of the incident as ‘low risk’ and also “...taking into account that of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year’s Day).”⁷⁸ (I have considered further TIC’s submissions on this issue below).

- 7.7 This was followed with assessment of the issue by Twitter Inc.’s legal team, which assessed the issue “as needing to be treated as an incident”.⁷⁹ As set out above at paragraph 4.7(iv), TIC stated in its submissions made during the Inquiry (including its Submissions in relation to the Draft Report) that this step took place on 3 January 2019, stating in this regard that

*“3 Jan 2019 – Twitter Inc’s Information Security team asked Twitter Inc.’s legal team for guidance on the potential privacy issue. On the same day Twitter Inc.’s legal team determined the issue may constitute a personal data breach and requested that the issue be treated as an incident and that Twitter, Inc’s Information Security Incident response plan be invoked.”*⁸⁰

In the Submissions in relation to the Preliminary Draft, TIC, however, outlined that “The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it).”⁸¹ (Emphasis added). (Whilst I am noting this as it represents a change in the facts as previously outlined by TIC, I do not consider that it impacts upon my findings).

⁷⁵ Submissions in relation to the Preliminary Draft, para 6.2

⁷⁶ Ibid, para 5.6

⁷⁷ Submissions dated 25 January 2019, annex

⁷⁸ Submissions in relation to the Preliminary Draft, para 6.3

⁷⁹ Submissions dated 25 January 2019, annex

⁸⁰ Submissions in relation to the Draft Report, para 2.6

⁸¹ Submissions in relation to the Preliminary Draft, para. 6.4

- 7.8 The above was followed, on 4 January 2019, by the opening (by Twitter Inc.'s Security Team) of the Incident Management Ticket ('the IM Ticket'), initiating the incident response plan.

It should be noted that, during the course of the Inquiry, TIC referred to the assessment by Twitter Inc.'s legal team of the incident on 3 January 2019 as comprising an assessment that the incident 'may' or 'might' constitute a personal data breach. Having considered this, 3 January 2019 appeared to be the date when Twitter Inc. had established, with a 'reasonable degree of certainty'⁸² that the incident comprised a breach of personal data. While it was asserted by TIC (in its Submissions in relation to the Preliminary Draft) that the Twitter legal team became involved on 2 January 2019, I note that it is still TIC's position that the legal team's identification that the matter potentially constituted a GDPR issue occurred on 3 January 2019⁸³. In this regard, I have also taken into account TIC's submission, in its Submissions in relation to the Preliminary Draft, that in its consideration of the matter, "[the] Twitter legal team did not itself consider whether the vulnerability constituted a notifiable personal data breach under GDPR as that was not its role. This is consistent with the Breach Notification Guidelines which state that "the process (sic) does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller."⁸⁴

- 7.9 TIC also outlined, in its submissions dated 25 January 2019, that

*"On 7 January 2019, during an incident response meeting including TIC's Data Protection Officer, and Twitter Inc's Information and Security and legal teams, the potential impact of the issue led to the determination that the incident should be treated as a Severity 1 incident...Pursuant to the incident response plan for a Severity 1 incident, members of TIC's and Twitter's executive teams were made aware of the incident on 7 January 2019."*⁸⁵

- 7.10 Following this, further queries were raised by the Investigator (in correspondence dated 29 January 2019) with a view to clarifying certain matters, relating to, *inter alia*, the timeline of the notification and when and how TIC had become aware of the Breach. In this regard, the Investigator queried whether TIC, or the DPO, had been informed of the incident on 3 January 2019, following the assessment of same by Twitter Inc.'s legal team as being a potential personal data breach.

In its response, dated 1 February 2019, TIC confirmed that

⁸² The Breach Notification Guidelines outline, at page 10, 11, that a controller will be deemed to be 'aware' of a breach when it has a 'reasonable degree of certainty' that a security incident has occurred that has led to personal data being compromised.

⁸³ Submissions in relation to the Preliminary Draft, para. 6.4

⁸⁴ Ibid, para. 6.4

⁸⁵ Submissions dated 25 January 2019, Annex

“TIC was not made aware of the issue on 3 January 2019. TIC became aware of this incident on 7 January 2019.”⁸⁶

TIC also outlined, in its response of that date, that:

“While TIC reported this incident to the DPC less than 72 hours after becoming aware of it, delays appear to have occurred in the triage of the [bug bounty] report, execution of the Twitter, Inc. Incident Response plan by Twitter Inc., and notification to TIC. TIC believes this was an isolated breakdown of the Twitter Inc. incident response process, and the Global DPO would typically be involved at the earliest stages of the Twitter Inc. incident response process as past practice has demonstrated.”⁸⁷

(As outlined above, in its Submissions in relation to the Preliminary Draft, TIC changed its position that delays appeared to have occurred and submitted that Contractor 2’s triage of the bug bounty report took place in accordance with its contractual requirements).

- 7.11 The Investigator also, in the correspondence to TIC dated 29 January 2019, raised queries as to whether the process, as outlined in the incident management procedure document furnished by TIC with its response dated 25 January 2019 (the Data Breach Investigation through Vulnerability Disclosure (DART) Runbook), had been followed. In this regard, the Investigator referred to the DART Runbook, which included, at Step 5 “*Escalation to Legal*” a direction to

“1. Add @[Name], @[Name] and @[Name] (DPO) as watchers to both the Investigation Ticket and the IM Ticket; 2.@mention both [Name] and [Name] (DPO) in the Investigation Ticket, making them aware of a possible GDPR in-scope Data Breach”⁸⁸ (Emphasis added)

The Investigator sought confirmation as to when this step had been completed.

- 7.12 In its response (dated 1 February 2019), TIC did not address, specifically, the issue of the addition of the DPO to the Investigation and IM Tickets, but outlined that

*“...a member of Twitter Inc.’s legal team **who supports the Information Security team was consulted on 3 January 2019 as part of his normal responsibilities.** During this consultation, the Twitter Inc. attorney informed the teams that the issue should be treated as an incident, which in turn prompted Twitter Inc.’s Detection and Response Team’s (DART) involvement and the initiation of the incident response plan. In turn, the Investigation Ticket and IM Ticket were created on 4 January 2019 and Twitter, Inc.’s legal team was also added at this time.”⁸⁹ (Emphasis added)*

⁸⁶ Submissions dated 1 February 2019, Annex, point 2

⁸⁷ Submissions dated 1 February 2019

⁸⁸ DART Runbook provided with TIC Submissions dated 25 January 2019

⁸⁹ Submissions dated 1 February 2019, Annex, point 2

- 7.13 In correspondence dated 6 February 2019, the Investigator directed TIC’s specific attention to the direction (referred to above) in the DART Runbook (that the DPO be added to the Investigation and Incident Management tickets) and sought clarification as to when this step had been completed.

In its response, dated 8 February 2019, TIC confirmed as follows:

“As noted in our 25 January letter, a member of the Twitter Inc. legal team – who would have been added pursuant to “5/Escalation to Legal” – was consulted by the Information Security team on 3 January 2018 (sic) after they had determined that the issue was not a security risk but may have been a potential privacy risk. As a result, this member of Twitter Inc’s legal team who would have been added pursuant to step “5/Escalation to Legal” was already involved in the incident. Thus, “5/Escalation to Legal” was not followed as prescribed in the runbook, and resulted in a delay in notifying the Global DPO.”⁹⁰ (Emphasis added)

TIC further clarified, in its Submissions in relation to the Draft Report, that the delay in notifying the DPO arose from a failure, by Twitter Inc. staff, to follow the process as outlined in the DART Runbook, stating in this regard as follows:

“Twitter Inc.’s legal team determined the issue might constitute a personal data breach on 3 January at which point a formal breach had been identified. An IM ticket was opened on 4 January and the TIC DPO was notified on 7 January. The engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant that TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.”⁹¹

In its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of the contents of the DART Runbook, and in respect of the failure by the Twitter Inc. employee to follow the prescribed process in relation to notifying the TIC DPO. TIC’s submissions in this regard are considered below.

- 7.14 In respect of how the DPO was made aware of the incident on 7 January 2019, TIC confirmed as follows:

“On 7 January during a weekly meeting between members of the Twitter Inc. legal team and the Global Data Protection Officer, a member of the Twitter Inc legal team raised the topic of an ongoing incident. Upon hearing this, the Global DPO immediately reached out to the Detection and Response Team (“DART”) leader and requested to be added to the incident materials. Thereafter, the Global DPO attended the next incident response meeting on 7 January 2019...”⁹²

⁹⁰ Submissions dated 8 February 2019, Annex, point 2

⁹¹ Submissions in relation to the Draft Report, para 3.10

⁹² Submissions dated 8 February 2019

TIC further confirmed that, as the DPO was informed *verbally* of the Breach at the weekly meeting, no contemporaneous record exists of this. However, it provided a number of records, comprising calendar appointments and an internal message, in support of the sequence of events in terms of when TIC was first informed of the Breach.

- 7.15 TIC has maintained the position, as set out in its Submissions in relation to the Draft Report, its Submissions dated 2 December 2019 and its Submissions in relation to the Preliminary Draft that, as Twitter Inc. (as processor) informed TIC of the Breach on 7 January 2019, it was at that point that TIC became “aware” of the Breach, and that

“As TIC submitted the Notification on 8 January 2019, its notification to the DPC was within the required time period”⁹³...

TIC also submitted that the documentation furnished by it in respect of the notification of the Breach to the DPO comprises sufficient evidence of its compliance with Article 33(1). (This matter is addressed by me below, in respect of the issue of TIC’s compliance with Article 33(5)).

- 7.16 Having regard to the above, therefore, the facts (in summary), as confirmed by TIC, in relation to the timeline of the notification to the Commission, and in particular, the issue of when TIC (as controller) became ‘aware’ of the Breach are as follows:

- Contractor 2 received the bug bounty report on **26 December 2018**, regarding the bug, and commenced its assessment of the report on **29 December 2018**. Contractor 2 then issued, on **29 December 2018**, a notification, in the form of a JIRA ticket, to Twitter Inc.
- Twitter Inc.’s Information Security team commenced its review of the JIRA ticket on **2 January 2019** and determined that the issue was a potential privacy-related concern.

Twitter Inc.’s Legal Team was then consulted about the issue on 2 January 2019 by the engineer reviewing the JIRA ticket⁹⁴ and it determined (on 3 January 2019) that the issue may potentially constitute a “GDPR issue”⁹⁵ and that Twitter’s Incident Response plan should be triggered

- Twitter Inc.’s Information Security team initiated the incident response plan on **4 January 2019** and on that date opened an IM Ticket – however, due to a failure (by Twitter Inc. staff) to follow the internal incident management process, the DPO was not added to the IM Ticket, resulting in a delay in the DPO being notified of the Breach. TIC acknowledged, in its

⁹³ Submissions in relation to the Draft Report, para 3.5

⁹⁴ This is based on the account at para 6.4 of the Submissions in relation to the Preliminary Draft

⁹⁵ Ibid

submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that, at this point, “a divergence from the prescribed process occurred”⁹⁶.

- The DPO (and, therefore TIC) was not notified of the Breach until **7 January 2019** during the course of a meeting between the Twitter, Inc. legal team and the DPO on that date when it was raised during discussions.

7.17 As set out above, the Investigator’s view, as set out at Section E.1 of the Final Report, is that it was not possible to establish whether TIC had complied with its obligation under Article 33(1). This was on the basis that TIC’s documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became ‘aware’ of the Breach, did not verify such compliance.

As decision maker, I am not bound by the conclusions of the Investigator and I am, as set out above, required to carry out an independent assessment of all materials that have been provided to me by the Investigator and further received by me during the course of the decision-making phase of the Inquiry. In this regard, having reviewed the materials, including all submissions, with regard to the obligations on a controller under Article 33(1), I concluded, as set out in my provisional finding in the Preliminary Draft, that TIC did not meet its obligations as a controller under that provision.

Paragraphs 7.18 to 7.26 below set out a summary of my provisional finding under Article 33(1), and my reasons for same, as it was outlined in the Preliminary Draft.

At paragraphs 7.27 to 7.128 below then, I have considered and analysed TIC’s Submissions in relation to the Preliminary Draft.

7.18 As outlined in the Preliminary Draft , my provisional view was that TIC had not complied with Article 33(1) in circumstances where, as a matter of law, the issue of TIC’s awareness of the Breach under Article 33(1) must be understood within the context of the broader obligations on controllers under the GDPR, including, as set out above at section 6, the obligation of accountability under Article 5(2); the relationship between controllers and processors governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.

I outlined my view that, had sufficient measures been in place and / or had they been followed, TIC would have been aware of the Breach at an earlier point in time (as it ought to have been) and, specifically, by 3 January 2019, that appearing to be the date on which the incident was assessed by Twitter Inc.’s legal team as being likely to comprise a reportable personal data breach.

In coming to this conclusion, I explained that I had had particular regard to the fact that the obligation on a controller, under Article 33(1), to notify a personal data breach (and the prescribed timeframe

⁹⁶ Submissions in relation to the Preliminary Draft, para 6.5

for same), must, as detailed above, in order to be effective, be understood within the context of the broader obligations on controllers under the GDPR.

In particular, and as has been set out above, both the Recitals to the GDPR and the Breach Notification Guidelines, provide that a controller is required to ensure that it has appropriate measures in place to ensure that it can effect compliance with Article 33(1).

- 7.19 I further outlined that, having reviewed the materials provided to me in the context of this Inquiry, I was not satisfied that this was the case in these circumstances. In this regard, I noted that TIC had confirmed in its submissions to this office that several delays had occurred during the timeline of the incident. I noted that these delays, which in turn led to the delayed notification of the Breach to the Commission, included an initial delay (between 26 December 2018 and 29 December 2018) in Contractor 2 commencing its “triage” process, which TIC had at that time described as appearing “*to have been a deviation from the agreed upon process between Twitter and [Contractor 2].*”⁹⁷ (TIC’s submissions in the Submissions in relation to the Preliminary Draft in respect of this matter have already been noted above and are further addressed by me below).
- 7.20 In addition, I noted that TIC had confirmed that a further delay then occurred “*as a result of the winter holiday schedule*”⁹⁸ in terms of the review of the JIRA ticket by Twitter Inc.’s security team.

I further noted that there was then a further, third delay occurring from 3 January 2019, when Twitter Inc.’s legal team assessed the incident as being a potential personal data breach, to the notification of same to the Global DPO on 7 January 2019. I noted that TIC confirmed, by way of explanation for this particular delay, that

“...the engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.”

- 7.21 I outlined that a detailed examination of the technical and organizational measures, or processes, and the operation of same by Twitter Inc., which gave rise to the delays set out above, was beyond the scope of this Inquiry. However, I explained that I had considered TIC’s submissions in relation to these issues, and as summarised above, for the purpose of determining whether TIC had met its obligations under Article 33(1).
- 7.22 In this regard, I noted that TIC had asserted that, whilst it reported the Breach to the Commission less than 72 hours after becoming aware of it, delays had occurred in the timeline up to that point. As set out above, I noted that TIC had confirmed that these delays arose as a result of a deviation from, or failure to follow, agreed processes on the part of its processor, Twitter Inc. (and by a third

⁹⁷ Submissions dated 25 January 2019, Annex footnote 3

⁹⁸ Ibid, Annex

party (Contractor 2) engaged by Twitter Inc.) and TIC had, in respect of one delay, confirmed that this arose as a result of *“the winter holiday schedule”*. (TIC’s submissions (in the Submissions in relation to the Preliminary Draft) in respect of these matters have already been noted above and are further addressed by me below.)

- 7.23 Further, in the Preliminary Draft, I noted, having regard to the foregoing, and to the analysis set out above at section 6, that TIC’s obligations under Article 33(1) could not be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

I explained that position was supported by both the Recitals to the GDPR and the views of the EDPB, as set out in the Breach Notification Guidelines. I also noted briefly that this approach accorded with the established principle of interpretation of EU law, applied by the CJEU in numerous decisions, whereby a provision of law is interpreted by reference not only to its wording but also to its purpose and the overall context in which it occurs.

- 7.24 In my analysis in this regard in the Preliminary Draft, I referred to TIC’s assertions that it was in compliance with Article 33(1) because it had notified the Breach to the Commission within 72 hours of TIC becoming aware of it. However, I set out my legal reasons for disagreeing with TIC’s interpretation of the Article 33(1) obligation in this regard as follows:

(1) This interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor Twitter Inc. and for ensuring that its own processor made it aware of any data breach in a manner that would allow TIC to comply with the 72 hour notification requirement in Article 33(1).

(2) A controller has the freedom to appoint whichever processor it wishes to appoint, but under the GDPR (e.g. Article 28(1)) it remains the responsibility of the controller to ensure that the processor it appoints provides sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing carried out by that processor complies with the GDPR and protects the rights of data subjects.

(3) A controller cannot avoid its responsibility under Article 33(1) by seeking to hide behind the failure of a processor, which it has appointed, to notify it of a personal data breach in relation to the personal data for which the controller is responsible, particularly where there are agreed protocols in place between the controller and its own processor for these purposes which have not been followed.

(4) The consequence of such an interpretation contended for by TIC - whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with the processor’s own freestanding obligations under Article 33(2) (for which the processor may separately face enforcement action by a supervisory authority in the event of non-compliance) –

would operate to render the obligation in Article 33 on a controller ineffective. Such an approach would effectively mean that the time for notification of a personal data breach to a supervisory authority would only start to run at the point when the processor finally informed the controller of the breach (if at all).

(5) Furthermore, the interpretation contended for by TIC would be entirely at odds with the overall purpose of the GDPR and the intention of the legislator, which is clearly to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded (to the extent possible by mitigating the risks to them arising from a data breach), by action on the part of the supervisory authority e.g. by requiring the controller to notify data subjects about the breach under Article 34(4).

(6) I also noted that, as signalled in Recital 85 of the GDPR, one of the primary purposes of notifying a personal data breach to a supervisory authority is clearly to enable the risk, presented by the breach, to affected individuals to be assessed by the supervisory authority and to determine whether additional action needs to be taken to protect such individuals. This will include consideration by the supervisory authority as to whether affected individuals should be notified, and a supervisory authority may, where appropriate, order a controller to communicate a personal data breach to affected data subjects (under Article 58(2)(e)). (There is also a power under Section 109(5)(d) of the 2018 Act whereby the Commission, in a complaint handling scenario, may issue an enforcement notice to a controller requiring it to communicate a personal data breach to the data subject). The ability of a supervisory authority to take such a step, and the provisions in respect of requiring the communication of a personal data breach to data subjects as set out in Article 34, would potentially be rendered ineffective, (or certainly much less effective with regard to the overarching objective of safeguarding the interests of data subjects in the case of a data breach), were it the case that a controller's obligation to notify a breach, in accordance with the timeframe in Article 33(1), was contingent in the first place upon the compliance by its processor with its own specific obligations, whether under Article 33(2) or under any protocols/arrangements agreed between the controller and the processor.

- 7.25 Having regard to the above, therefore, my provisional view in the Preliminary Draft was that Twitter Inc.'s failure to notify TIC (through the Global DPO), in line with what were, in effect, the agreed protocols between Twitter Inc. and TIC, about the Breach until 4 days after Twitter Inc. formed the view that it was a notifiable personal data breach did not obviate TIC's legal obligation to notify in accordance with the timeframe under Article 33(1). My provisional conclusion was that this obligation under Article 33(1) remains extant, vis-à-vis the controller, notwithstanding any failures of protocol or procedure on the processor side.
- 7.26 On the basis of the above, my provisional finding was that TIC did not comply with its obligations under Article 33(1). The below sets out the summary of the factual and legal reasons for my provisional finding as it was set out in the Preliminary Draft:

- *“Compliance with Article 33(1) requires that a controller must notify a personal data breach within a prescribed timeframe. This, in turn, means that a controller must have appropriate measures in place to ensure that it can effect such notification, as discussed above at paragraphs 6.5 – 6.19. The obligation on a controller to notify under Article 33(1), therefore, must be understood in the context of the broader obligations on a controller under the GDPR.*
- *In this particular case, TIC has confirmed that Twitter Inc., its processor, assessed the issue as being a potential personal data breach on 3 January 2019 but a failure by Twitter Inc. staff to follow its incident management process led to a delay in TIC (as controller) being notified of the Breach, which did not occur until 7 January 2019.*
- *TIC has also confirmed that other delays arose from the time at which the incident was first identified on 26 December 2018 to when it was assessed by Twitter Inc., on 3 January 2019, as being a potential personal data breach. In particular, TIC has confirmed that a 4-day delay occurred, from the incident first being reported to Contractor 2 (an IT Security company engaged by Twitter Inc.) on 26 December 2018 to Contractor 2’s “triage” of the incident on 29 December 2018. In addition, TIC has confirmed that a further delay ensued “due to the winter holiday schedule” between the notification of the issue by Contractor 2 to Twitter Inc. on 29 December 2018 and the commencement of the review of the issue by Twitter Inc.’s security team on 2 January 2019.*
- *TIC has asserted that “Twitter Inc. informed TIC of the Breach on 7 January 2019 so it was at this point that TIC became “aware” of the breach for the purposes of Article 33(1). As TIC submitted the notification on 8 January 2019, its notification to the DPC was within the required time period...”⁹⁹*
- *However, notwithstanding TIC’s actual ‘awareness’ of the breach on 7 January 2019, I am of the view that, having regard to the issues set out above, TIC did not comply with its obligations as a controller to notify the Breach within the prescribed timeframe. This arises in circumstances where, as discussed above at 6.5 – 6.19, a controller must have appropriate measures in place to ensure that it can effect such notification.*
- *The alternative application of Article 33(1), and that being 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 operate to render the obligations in Article 33 on a controller ineffective. Such an approach would be entirely at odds with the overall purpose of the GDPR and the intention of the legislator.”*

⁹⁹ Submissions in relation to the Draft Report, para. 3.5

TIC's Submissions in relation to the Preliminary Draft

7.27 As noted above, TIC's Submissions in relation to the Preliminary Draft were provided to the Commission on 27 April 2020. TIC's submissions in relation to my provisional finding in respect of Article 33(1) were set out, **in summary form**, at paragraph 2 of the Submissions in relation to the Preliminary Draft, as follows.

- a. *A controller should be considered as "aware" for the purposes of Article 33(1) of the GDPR only once its processor has informed it of the breach; the controller is not to be imputed (sic) with the awareness of its processor.*
- b. *The DPC's interpretation of Article 33(1) does not accord with the established principles of interpretation of EU law, and it is not open to the DPC to apply a unique, national interpretation to the meaning of "after having become aware of it" in Article 33(1).*
- c. *The obligations on the controller to have processes in place to ensure personal data breaches are identified and responded to in accordance with Article 33 of the GDPR arise under Articles 24 and 32 of the GDPR, rather than being implied into Article 33 of the GDPR.*
- d. *TIC had extensive and robust processes in compliance with Articles 24 and 32 at the time of the Underlying Bug and continues to have such processes as part of the Twitter Security Program, which it keeps under regular review.*
- e. *The effectiveness of TIC's processes in relation to notifying personal data breaches is evidenced by its strong track record to date. Between May 2018 and June 2019, it notified 8 personal data breaches to the DPC, each within seventy-two hours (with the exception of the Underlying Bug).*
- f. *The Twitter Security Program, including those aspects that address breach notification, has been the subject of four independent assessments against relevant ISO standards by [a third party] and found to be 'operating with sufficient effectiveness'.*
- g. *The DPC is wrong to state that there were multiple delays in the early part of the process; there were not. This issue arose as a result of an isolated failure by a Twitter, Inc. employee (TIC's processor) to follow an established process that would have resulted in TIC being made aware of the Underlying Bug.*
- h. *TIC became aware of the personal data breach on 7th January 2019 and notified the DPC on 8 January, well within the seventy-two hour period required by Article 33(1). The seventy-two hour period does not commence, as the DPC suggests, at the point at which the controller ought to have been aware.*

- i. *The DPC has not investigated, nor enquired of Twitter or TIC, whether TIC did in fact have appropriate processes in place. Indeed, the DPC's Draft Decision expressly states in Paragraph 7.19 that a "detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic)".*
- j. *The terms of reference of the DPC's inquiry were limited to Article 33(1) and Article 33(5) of the GDPR; as stated above, the Draft Decision expressly states that "a detailed examination of the technical and organizational measures is beyond the scope of the enquiry." The DPC, however, has de facto extended the scope of the inquiry by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice."*

7.28 I have addressed TIC's submissions, in respect of the above matters, under the following headings:

- **TIC's submissions in relation to factual matters concerning its notification of the Breach to the Commission.** Under this heading, I have taken account of TIC's submissions as summarized at paragraph 2 of its Submissions in relation to the Preliminary Draft (and as set out above) at (d), (e), (f) and (g) thereof. These matters comprise, in summary, TIC's submissions on factual matters relating to the notification of the Breach to the Commission and in respect of the relevant protocol(s) which it had in place and had agreed with Twitter Inc. for this purpose.
- **TIC's submissions in relation to the provisional finding that it did not comply with Article 33(1).** Under this heading, I have taken account of TIC's submissions as summarized at paragraph 2 of its Submissions in relation to the Preliminary Draft (and as set out above) at (a), (b), (c), (h), (i) and (j) thereof. In summary, TIC made submissions that, in making a provisional finding to the effect that it had not complied with Article 33(1), the Commission had
 - (i) Incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1);
 - (ii) Implied obligations arising under other Articles of the GDPR, in particular, Articles 24 and 32, into Article 33(1); and
 - (iii) Failed to adhere to fair procedures.

TIC's submissions in respect of factual matters concerning its notification of the Breach to the Commission

- 7.29 As set out above, in its Submissions in relation to the Preliminary Draft, TIC made submissions in relation to certain factual matters relating to the notification of the Breach to the Commission and, in particular, the events that occurred in the time period leading up to the notification.
- 7.30 Paragraphs 7.19-7.20 above outline that, based on the information furnished by TIC during the course of the Inquiry, my provisional finding noted that multiple delays had arisen during the early part of the timeline, leading up to the point, on 3 January 2019, at which Twitter Inc. assessed the incident as being likely to be a notifiable personal data breach.

In this regard, I noted in the Preliminary Draft that TIC had outlined (in its Submissions dated 25 January 2019) that a 4-day delay had occurred from the bug first being reported to Contractor 2 (an IT Security company engaged by Twitter Inc.) on 26 December 2018 to Contractor 2's "triage" of the issue on 29 December 2018.

In addition, the Preliminary Draft referred to TIC having stated that a further delay had ensued "*due to the winter holiday schedule*" between the notification of the issue by Contractor 2 to Twitter Inc. on 29 December 2018 and the commencement of the review of the issue by Twitter Inc.'s security team on 2 January 2019.

TIC submissions in relation to events during timeline of Notification

Paragraphs 7.31 – 7.39 below outline, in summary form, the issues which TIC raised in its Submissions in relation to the Preliminary Draft and which pertain to the events that arose during the timeline leading up to the Notification to the Commission on 8 January 2019.

Paragraphs 7.40 – 7.49 below then set out my consideration of those issues raised by TIC.

TIC submitted that "*There were not multiple delays*" in the early part of the process."¹⁰⁰ In that regard, TIC made a number of submissions concerning the events that occurred in the timeline leading up to the Notification. These events comprise

- the 'triage' by Contractor 2 of the bug report and the notification of same (in the JIRA ticket) by Contractor 2 to Twitter Inc. on 29 December 2018;
- the review by Twitter Inc. of the JIRA ticket submitted to it by Contractor 2 on 2 January 2019; and

¹⁰⁰ Submissions in relation to the Preliminary Draft, para 6.1

- the incident on 4 January 2019, whereby, due to a failure by a member of Twitter Inc.'s Information Security team to follow the protocol (as set out in the DART Runbook), the TIC DPO was not added to the Incident ticket, which, in turn, resulted in a delay in the TIC DPO (and therefore TIC as controller) being made aware of the Breach.

- 7.31 As set out above, TIC submitted, in its Submissions in relation to the Preliminary Draft, that the time period within which Contractor 2 had carried out its 'triage' of the issue – from its receipt of the bug report on 26 December 2018 to its notification of same to Twitter Inc. on 29 December 2018 – *“was in line with its contractual commitments so there was no delay in complying with the internal process requirement.”* In this regard, TIC confirmed that, at the relevant time, Contractor 2 was subject to a service level but did not confirm details of the service level¹⁰¹. TIC further submitted that *“Given the nature of the majority of bug reports, this target is a reasonable and appropriate standard, and is in line with other bug bounty programs.”*¹⁰²
- 7.32 TIC further submitted, in its Submissions in relation to the Preliminary Draft, that the time period that elapsed between 29 December 2018, when Contractor 2 notified Twitter Inc. of the issue, to the date of the commencement of the review of the issue by Twitter Inc.'s Information Security team on 2 January 2019, was reasonable. TIC contended that this was a reasonable time period given that the initial risk classification of the issue (by Contractor 2) was 'low risk' and also that *“...of the four preceding days (including the day on which the JIRA ticket was raised), three were holidays (a weekend, and New Year's Day).”*¹⁰³
- 7.33 TIC also made submissions regarding factual matters pertaining to the next stage of the timeline of the Notification, which, as set out above, at section 4, involved the assessment of the issue by Twitter Inc.'s Information Security team and the notification of the issue, by the Twitter Inc. Information Security team, to Twitter Inc.'s legal team.

In this regard, and as I have noted above, in all submissions made to this office by TIC during the course of the Inquiry (including its Submissions in relation to the Draft Report), TIC outlined that the notification of the incident by Twitter Inc.'s Information Security team to Twitter Inc.'s legal team took place on 3 January 2019. As discussed above, however, in its Submissions in relation to the Preliminary Draft, TIC stated that

*“The engineer reviewing the JIRA ticket identified the potential impact of the vulnerability on personal data and contacted the Twitter legal team on 2 January (i.e. on the same day as he reviewed it).”*¹⁰⁴

¹⁰¹ Ibid, para. 5.6

¹⁰² Ibid, para 6.2

¹⁰³ Ibid, para 6.3

¹⁰⁴ Submissions in relation to the Preliminary Draft, para 6.4

7.34 In the Submissions in relation to the Preliminary Draft, TIC also made further submissions in respect of the next step in the timeline, which took place on 4 January 2019. As outlined above at paragraph 4 this was when, following the assessment of the issue by Twitter Inc.’s legal team on 3 January 2019 as being likely to be a reportable personal data breach, the Information Security team initiated the incident response plan and opened an IM Ticket. However, due to a failure (by Twitter Inc. staff) to follow the internal incident management process as set out in the DART Runbook, the TIC DPO was not added to the IM Ticket, resulting in a delay in the DPO (who is the Global DPO for the Twitter group including for TIC) (and therefore, TIC) being notified of the issue.¹⁰⁵ TIC has acknowledged, both in its submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that, at this point, a divergence from the prescribed process occurred.¹⁰⁶

As set out above, TIC, in its Submissions in relation to the Preliminary Draft, made a number of submissions that are relevant to this stage of the process, which are set out below at paragraphs 7.35 to 7.39.

7.35 Firstly, TIC confirmed, as it had done in its submissions made during the Inquiry, that the relevant process for the internal management of incidents was that outlined in the DART Runbook.¹⁰⁷ In this regard, as set out above, TIC confirmed during the course of the Inquiry that a deviation from the prescribed process arose when

“The engineer opening the IM ticket failed to follow the process correctly so the TIC DPO was not immediately added to the ticket. This meant that TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.”¹⁰⁸

TIC also, during the course of the Inquiry, confirmed that this occurred when a particular step in the process, outlined at Step 5 of the DART Runbook, was not followed. As set out above, this step provided as follows:

Step 5 “Escalation to Legal”

“1. Add @[Name], @[Name] and @[Name] (DPO) as watchers to both the Investigation Ticket and the IM Ticket; 2. @mention both [Name] and [Name] (DPO) in the Investigation Ticket, making them aware of a possible GDPR in-scope Data Breach”¹⁰⁹ (Emphasis added).

7.36 In its submissions made during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, TIC confirmed that the reason the above step was not carried out, as required by the process set out in the DART Runbook, was that

¹⁰⁵ Ibid, para 6.5

¹⁰⁶ Ibid, para 6.5

¹⁰⁷ Ibid, para 5.11

¹⁰⁸ Submissions in relation to the Draft Report, para 3.10

¹⁰⁹ DART Runbook provided with TIC Submissions dated 25 January 2019

*"The Twitter Inc. legal team were already involved in the incident ... and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied."*¹¹⁰

- 7.37 In its Submissions in relation to the Preliminary Draft, TIC also made submissions regarding the efficacy of the DART Runbook and the process outlined therein.

In this regard, TIC stated that

*"The process requires that the legal team and DPO are added as watchers to the incident ticket. In summary, these processes are structured in such a way as to ensure that relevant experts triage and review issues and then ensure that the TIC DPO is notified by Twitter Inc of any GDPR impacting issues as quickly as possible and certainly "without undue delay" as required by Article 33(1) GDPR."*¹¹¹

*"It is evident from the DART Runbooks that Twitter Inc. had clear and effective processes and controls in place at the time of the report of the Underlying Bug which provided for the identification of vulnerabilities, the escalation of vulnerabilities to incidents if the vulnerability could lead to the exposure of 'high sensitivity' data, such as Protected Tweets; the documentation of all activities taking place in respect of incidents; involvement of the TIC DPO at an early stage."*¹¹²

- 7.38 TIC further submitted, in its Submissions in relation to the Preliminary Draft, that the incident whereby the prescribed process for notifying the TIC DPO was not followed by Twitter Inc. was *"an isolated one-off failure ... that occurred over the Christmas holiday season"*¹¹³. In addition, TIC submitted that its track record of notifying other incidents to the Commission (between May 2018 and June 2019) demonstrates that it had highly effective processes in place as regards appropriate technological and organizational measures for establishing personal data breaches had occurred and promptly informing the DPC and affected data subjects.¹¹⁴

- 7.39 TIC further submitted that, notwithstanding its track record of reporting breaches to the Commission within the timeframe prescribed by Article 33(1), it reviewed its processes in light of the issues arising in respect of its notification of the Breach to the Commission and made the following amendments:

"The service levels with [Contractor 2] were re-negotiated and it is now required to action all submissions within 24 business hours, unless it is granted an SLA extension for a particular report;

The Runbook was amended to make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly;

¹¹⁰ Submissions in relation to the Preliminary Draft, para 6.5

¹¹¹ Ibid, para 5.13

¹¹² Ibid, para 5.12

¹¹³ Submissions in relation to the Preliminary Draft, para 5.18

¹¹⁴ Ibid, para 5.18

The Twitter legal team provided additional training to the InfoSec team that receives the [Contractor 2] reports to ensure that they were better able to identify issues that are not security issues but may be privacy/data protection issues. The training also stressed the importance of @mentioning the DPO team in the JIRA ticket so that the DPO team receives email notices, and then specifically recording that in the incident document, including a time stamp.”¹¹⁵

Consideration of TIC’s submissions relating to timeline of events leading up to notification of the Breach

7.40 I have considered TIC’s submissions, relating to the timeline of events leading up to the Notification and, in particular, the issue of delay(s) during that time period, and I set out my views in respect of these matters below.

7.41 Firstly, regarding TIC’s submission in relation to the timing of the ‘triage’ of the incident by Contractor 2, which took place on the 29 December 2018 following the receipt by Contractor 2 of the bug report on the 26 December, I accept TIC’s submission that Contractor 2 was, at that time, subject to a service level (the timeframe for which has not been specified to the Commission in TIC’s Submissions in relation to the Preliminary Draft) and that the timing of Contractor 2’s review of the incident in this case was in line with its contractual requirements.

I note that TIC confirmed that this service level has since been re-negotiated with Contractor 2 to reduce the permitted timeframe and require it to action all such bug reports within 24 hours, unless otherwise stipulated.

7.42 In relation to TIC’s submission concerning the time period that elapsed between the notification by Contractor 2 of the issue to Twitter Inc. on 29 December 2018 and the commencement of Twitter Inc.’s review of same on 2 January 2019 by its Information Security team, for the reasons set out below, I do not accept the arguments advanced by TIC, in its Submissions in relation to the Preliminary Draft, that this timeframe was reasonable.

Firstly, I have considered TIC’s submission that, given the classification of the incident by Contractor 2 in the JIRA ticket as being ‘low risk’, it was reasonable for Twitter Inc. not to commence reviewing the matter until 2 January 2019. Having re-examined the JIRA ticket in light of TIC’s submission on this point, I note that whilst the JIRA ticket classifies the risk as being ‘Low’, it is also clear from the contents of the JIRA ticket that the issue is privacy-related, as it states, under the heading ‘Impact’ that

¹¹⁵ Ibid, para 5.17

“A user can accidentally disable the account privacy setting “Protect your tweets” by adding a new email on Twitter’s Android Mobile App.”¹¹⁶

I also note that the initial bug report, on 26 December, and which is contained within the JIRA ticket sent to Twitter Inc., had, as its subject line ‘*Privacy Violation*’, although I accept that this was contained in the original bug report and therefore pre-dates the ‘triage’ of the issue by Contractor 2.

I further note that when the matter was first reviewed on 2 January 2019, the Twitter Inc. Information Security personnel acknowledged that, although the issue was a low security risk, *“the privacy implications are pretty nasty”*.¹¹⁷

I am of the view, therefore, that, notwithstanding the classification by Contractor 2 of the issue as ‘low risk’, it was evident from the contents of the JIRA ticket as a whole that, by virtue of the nature of the bug / issue, it had significant data protection implications.

- 7.43 Furthermore, with regard to TIC’s contention that the four day intervening period between the Information Security team at Twitter, Inc. receiving the JIRA ticket from Contractor 2 on 29 December 2018 and actually reviewing it on 2 January 2019 was reasonable because three of the four preceding days were holidays, I do not accept this. (I note that, in a similar vein, TIC had previously, during the course of its submissions made during the Inquiry and in its Submissions dated 2 December 2019 (made following the commencement of the decision making process) outlined that the “winter holiday schedule” had led to the issue not being identified and escalated as it should have been). Potential risks to the data protection and privacy rights of data subjects cannot be neglected, even for a limited period of days, simply because it is an official holiday day/period or a weekend. Accordingly, I do not accept TIC’s claim that it was reasonable to have such a delay in the examination of a matter which was described in the JIRA ticket as a “privacy violation” with a clear explanation as to the nature of its effects on users. This is particularly in circumstances where TIC, in its Submissions in relation to the Preliminary Draft, specifically refers, amongst other things, to the independent review of Twitter’s Security Program as reflected in the 2017 third party audit report which noted that the Information Security [team] had a *“security on call rotation responsible for responding to incidents”*¹¹⁸. It is expected that the nature of such an on call rotation is that there are sufficient, allocated personnel available on a rota to ensure that the Information Security function is constantly staffed irrespective of weekends and public holidays given that Twitter’s services do not cease to operate during such times and users continue to use such services.

I also note, in this regard, that TIC has stated that Twitter Inc. has since provided additional training to its Information Security team that receives such reports from Contractor 2 to ensure that they are

¹¹⁶ Redacted JIRA Ticket provided with Submissions dated 1 February 2019

¹¹⁷ Ibid

¹¹⁸ Submissions in relation to the Preliminary Draft, para 5.21

*“...better able to identify issues that are not security related but may be privacy / data protection issues”.*¹¹⁹ I further note that TIC confirmed that this training also highlighted the importance of mentioning the DPO team (therefore TIC (as controller)) in the JIRA ticket so that the DPO team receives email notices in respect of the issue.¹²⁰

Accordingly, for all of the reasons set out above, I remain of the view that a delay of four days preceding the commencement by Twitter. Inc.’s Information Security team of its review of the report outlined in the JIRA ticket was not acceptable nor reasonable in the circumstances and that this did, in fact, constitute a delay in this stage of the process.

- 7.44 As I have referred to above, in its Submissions in relation to the Preliminary Draft, TIC outlined that the notification of the incident by Twitter Inc.’s Information Security team to Twitter Inc.’s legal team took place on 2 January 2019. As I have noted, this represents a deviation from all previous submissions made by TIC to this office, wherein it confirmed that this notification took place on 3 January 2019.

In light of TIC’s submission on this point, the relevant documentation (including, the JIRA ticket transmitted from Contractor 2 to Twitter Inc.; the Investigation and Incident Management tickets; and the Incident Report) furnished by TIC during the course of the Inquiry was re-examined. However, it is not possible, on the basis of the relevant documentation, to verify when this step took place. However, as the Submissions in relation to the Preliminary Draft are the most recent submissions made by TIC to the Commission, which have been made with the assistance of external legal expertise, on balance, I am prepared to accept that this represents the correct date in respect of the notification of Twitter Inc.’s legal team.

In any event, while noting it for the record, I do not consider that TIC’s change of position on this particular factual issue impacts upon my considerations of whether TIC complied with Article 33(1) and so I consider that nothing turns on it.

- 7.45 I now turn to the issue of TIC’s submissions made in respect of the incident whereby the prescribed process for notifying the TIC DPO was not followed by Twitter Inc.

As set out above, at paragraphs 7.35 – 7.37, TIC submitted that this occurred when the direction, contained in the DART Runbook at *Step 5 (‘Escalation to Legal’)* and which directs that members of Twitter Inc.’s legal team and the TIC DPO be added to the incident ticket *“making them aware of a possible GDPR in-scope Data Breach”*, was not followed as prescribed.

In its submissions made during the Inquiry, and in its Submissions in relation to the Preliminary Draft, TIC submitted that the reason the above step was not carried out arose in circumstances where

¹¹⁹ Ibid, para 5.17

¹²⁰ Ibid, para 5.17

“The Twitter Inc. legal team were already involved in the incident ... and as a result the DART team assumed that the legal steps (including notifying the DPO) of the Runbook were satisfied.”¹²¹

- 7.46 In essence, therefore, TIC acknowledged that Twitter Inc.’s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled ‘*Escalation to Legal*’ was not completed as prescribed.

As set out above, Step 5 of the protocol was essentially a combined step requiring that certain named members of the Twitter Inc., legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added to the Incident and Investigation tickets.

TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

- 7.47 TIC further submitted that

“The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate.”¹²²

I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team and / or individual Twitter Inc. engineer as to *who* had been informed of the issue when the legal team were already involved and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single composite step entitled ‘*Escalation to Legal*’.

I accept TIC’s submission that this was an isolated failure and that it was not indicative of a broader, systemic issue. However, despite the isolated nature of the incident underlying the Breach, I consider that the DART Runbook did not appear to have been as clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the Twitter Inc.

¹²¹ Submissions in relation to the Preliminary Draft, para 6.5

¹²² Submissions in relation to the Preliminary Draft, para 6.6

legal team **and** the DPO. Furthermore, I consider that the subsequent amendment of the Runbook and TIC's comments in respect of same are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

- 7.48 In this regard, I note that TIC confirmed, in its Submissions in relation to the Preliminary Draft, that it amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to “...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly”.¹²³

The updated DART Runbook was furnished to the Commission during the course of the Inquiry, specifically with TIC's Submissions dated 8 February 2019. Having re-examined the updated version of the DART Runbook in light of TIC's submission on this issue, I note that the relevant part of the DART Runbook, relating to Twitter Inc.'s notification of an incident or breach to TIC, now deals *separately* with the requirements to notify the TIC DPO, as distinct from the named members of Twitter Inc.'s legal team.

- 7.49 In respect of TIC's submission that the deviation from the agreed protocol in the earlier version of the DART Runbook was an isolated incident that occurred over the Christmas period, and its submission that it has a track record of successfully notifying the Commission of personal data breaches, I do not consider these to be factors which are directly relevant to the question of whether TIC complied with its obligation under Article 33(1). Rather I consider that such matters may be relevant in the context of the factors which must be taken into consideration insofar as I may find that an infringement has occurred and in considering the question of whether corrective powers should be exercised, including the question of whether any administrative fine should be imposed (and if so, the amount of same).

TIC's submissions in respect of Twitter Inc.'s Information Security Program

- 7.50 Before turning to address the various submissions which TIC made in respect of my provisional finding that it did not comply with Article 33(1), I note that TIC also, in its Submissions in relation to the Preliminary Draft, at paragraphs 5.1 – 5.18, made general submissions in relation to the Information Security program which Twitter Inc. had in place at the time of the Notification, (and as referenced at Paragraph 2(f) of its Submissions in relation to the Preliminary Draft). TIC also, at paragraphs 5.19 – 5.23 of its Submissions in relation to the Preliminary Draft, explained that the Twitter Inc. Information Security Program has been subject to biennial independent third party assessment, which has found that the Information Security Program “*was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality and integrity*

¹²³ Ibid, para 5.17

of non-public consumer information collected from or about consumers is protected and the program has so operated throughout the Assessment Period.”¹²⁴

TIC referenced the Twitter Inc. Information Security program, and the biennial independent audit of same, across the period from 2011 to 2019, in light of its submission that, in considering the obligation on a controller under Article 33(1) in the context of the other obligations on controllers under the GDPR, my provisional finding has the effect of implying obligations, specifically under Articles 24 and 32, into Article 33(1). TIC stated, in this regard, that

“While it is TIC’s view that the obligations to which the DPC is referring apply as obligations under Article 24 and 25 rather than being implied into Article 33(1), TIC nevertheless has extensive and robust processes in place to ensure that suspected breaches were identified and dealt with appropriately and its track record with respect to breach notification generally, and notifying the DPC when appropriate, in particular, demonstrates that these processes have been and continue to be effective.”¹²⁵

- 7.51 In its submission on these issues, TIC explained that, under Twitter Inc.’s Information Security program, all data is classified according to a Data Classification Standard and Data Handling Policy and that, in addition, Twitter Inc. has in place an Employee Security Handbook which all employees are required to read, and comply with, and which *“...includes specific instructions on reporting security incidents.”¹²⁶*

TIC also outlined that *“Twitter has a dedicated Detection and Response Team (“DART”) within the Enterprise Security Team responsible for handling security incidents at Twitter. The process of handling incidents is set out within the DART Runbook.”¹²⁷*

- 7.52 I have separately dealt below with TIC’s contentions as regards my approach towards the interpretation of the meaning and effect of the Article 33(1) obligation. As will be seen, I do not agree that, in considering Article 33(1), and in particular, the concept of controller awareness, in the context of the broader obligations on a controller under the GDPR, my provisional finding implies obligations arising under other Articles (and, specifically those arising under Articles 24 and 32), into Article 33(1).

- 7.53 Notwithstanding this, I carefully considered TIC’s submissions, as outlined above, in respect of:

- the Twitter Inc. Information Security program and the associated documents furnished (comprising the Data Handling Policy and Employee Security Handbook); and

¹²⁴ Submissions in relation to the Preliminary Draft, para 5.19

¹²⁵ Ibid, para 5.2

¹²⁶ Submissions in relation to the Preliminary Draft, para 5.9, 5.10

¹²⁷ Ibid, para 5.11

- the independent audit of Twitter Inc.'s Information Security Program and the associated third party reports on Twitter Inc.'s Information Security Program for the periods 2011-2013, 2013-2015, 2015-2017 and 2017-2019).

Having considered both the submissions from TIC and the supporting documentation furnished to me by way of the Submissions in relation to the Preliminary Draft, however, I do not consider TIC's submissions on these issues, or the related documentation, to have any direct bearing on my consideration as to whether TIC complied with its obligation under Article 33(1). In this regard, as outlined herein, the issue of Twitter Inc.'s Information Security program generally, and its compliance with Articles 24, 25 and 32 in respect of same, was not investigated during the course of the Inquiry, which was confined to examining TIC's compliance with its obligation under Article 33(1) and Article 33(5). (It should be noted, however, that I do consider that such matters may be relevant in the context of the factors which must be taken into consideration, insofar as I may find that an infringement has occurred and I proceed to consider the question of whether corrective powers should be exercised, including the question of whether any administrative fine should be imposed (and if so, the amount of same)).

However, as will be apparent from paragraphs 7.31-7.49 above, I have taken account of TIC's submissions on these matters insofar as they relate to factual issues, and the related internal protocol(s) as they pertain to those issues, concerning the timeline relating to the notification of the Breach to the Commission, and the factors which led to the acknowledged delay in TIC being informed about the Breach.

- 7.54 In its Submissions in relation to the Preliminary Draft, TIC also referenced (at paragraph 5.14 thereof) its Security Incident Management Workflow document. In this regard, TIC outlined that this document *"includes a general instruction ...to "Be aware, that for ANY breach of customer private data, we have 72 hours to notify our European Regulators from the time the issue was DISCOVERED BY A TWITTER EMPLOYEE. Move quickly and loop in our DPO if you believe you have a GDPR impacting issue."*¹²⁸

TIC further submitted that:

*"This internal standard does not distinguish between Twitter Inc. employees and TIC employees i.e. between the awareness of TIC and the awareness of its processor. As a result, this is a higher standard than that required by both Article 33(1) and the Breach Notification Guidelines."*¹²⁹

- 7.55 Having re-examined the version of the Security Incident Management Workflow document (revision July 2018) that was furnished to the Commission during the course of the Inquiry, the text referred to above by TIC is not included therein. In such circumstances, whilst I note TIC's submission to this

¹²⁸ Submissions in relation to the Preliminary Draft, para. 5.14

¹²⁹ Ibid, para 5.15

effect, I do not accept or reject it in circumstances where it is not reflected by the documentation provided to the Commission during the course of the Inquiry.

I also note, in this regard, that TIC, in any event, confirmed both during the course of the Inquiry and in its Submissions in relation to the Preliminary Draft, that the applicable process for the handling of incidents (such as the Breach), and the process that was followed in this regard, is that set out in the DART Runbook, the relevant aspects of which have been fully considered in this Decision in the course of the factual backdrop to the Breach.

TIC's submissions in relation to the provisional finding that it did not comply with Article 33(1)

7.56 TIC made a number of submissions in respect of my provisional finding in the Preliminary Draft that, in its notification of the Breach to the Commission, TIC did not comply with Article 33(1). TIC's submissions on these issues are as set out in its Submissions in relation to the Preliminary Draft at Paragraphs 7, 8 and 9 thereof, and, in summary, assert that, in making a provisional finding that TIC did not comply with Article 33(1), the Commission:

- (i) Incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and incorrectly applied a 'purposive interpretation' of Article 33(1);
- (ii) Implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1); and
- (iii) Failed to adhere to fair procedures.

I set out below, at paragraphs 7.57 to 7.69, the submissions made by TIC on these issues and which are summarized in the extract set out above from the Submissions in relation to the Preliminary Draft at points (a), (b), (c), (h), (i) and (j) thereof.

At paragraphs 7.70 to 7.128 below then, I set out my views, having carefully analysed and considered TIC's submissions on these issues.

- (i) Summary of TIC's submissions that the provisional finding incorrectly interpreted the concept of 'controller awareness' under Article 33(1) and its submissions that my provisional finding incorrectly applied a 'purposive interpretation' of Article 33(1)

7.57 TIC submitted that, in my provisional finding, I incorrectly interpreted the concept of 'awareness' on the part of the controller in Article 33(1). The main arguments, submitted by TIC on this issue, can be summarized as follows:

- (a) TIC asserted that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches.
- (b) TIC alleged that, in respect of how the provisional finding interprets the issue of controller awareness, it incorrectly applies a ‘purposive interpretation’ of Article 33(1);
- (c) TIC further contended that “[the] DPC’s proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach”. TIC submits that this, in turn, has the effect of making a controller vicariously liable for its processor/sub-processor’s failure to comply with Article 33(2).

(a) Outline of TIC’s assertion that the provisional finding departs from the Breach Notification Guidelines and is not suggested in guidance published by the Commission

7.58 In its Submissions in relation to the Preliminary Draft, TIC submitted that the interpretation of Article 33(1), and specifically the interpretation of controller ‘awareness’, as set out in the provisional finding, departs from the position as set out in the Breach Notification Guidelines¹³⁰.

In this regard, TIC contended that the approach adopted in the current version of the Breach Notification Guidelines differs to that adopted in the previous version of the Guidelines, which were adopted by the Article 29 Working Party on 3 October 2017. TIC pointed to the following paragraphs, from pages 13 and 14, respectively, of the current Breach Notification Guidelines, which address the matter of the relationship between the processor’s awareness and the controller’s awareness:

*“...the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. **The controller uses the processor to achieve its purposes; therefore in principle, the controller should be considered as “aware” once the processor has informed it of the breach.***

As explained above, the contract between the controller and processor should specify how the requirements expressed in article 33(2) should be met in addition to other provisions of the GDPR. This can include requirements for early notification by the processor that in turn support the controller’s obligation to report to the supervisory authority within 72 hours.”

¹³⁰ Article 29 Working Party *Guidelines on Personal data breach notification under Regulation 2016/679*, (As Adopted on 3 October 2017; as last revised and adopted on 6 February 2018)

TIC then set out, by way of comparison, the equivalent paragraph in the earlier version of the Breach Notification Guidelines (as adopted on 3 October 2017). (This was the original version of the Breach Notification Guidelines which were revised following an EEA-wide public consultation on them):

*“Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller “without undue delay”. **The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as “aware” once the processor has become aware.** The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1).”¹³¹*

- 7.59 TIC further contended that, in taking the view in the provisional finding that, had sufficient measures been in place and / or had they been followed, TIC would have been aware of the Breach at an earlier point in time (as it ought to have been), the concept of ‘awareness’ as set out in Article 33(1) had been incorrectly interpreted. In this regard, TIC submitted that

“The Breach Notification Guidelines state that “the controller uses the processor to perform its purposes; therefore in principle, the controller should be considered as “aware” once the processor has informed it of the breach.” Twitter, Inc. informed the TIC DPO of the Underlying Bug on 7 January. Therefore, TIC became aware of the Underlying Bug on 7 January.”¹³²

- 7.60 TIC further submitted that guidance published by the Commission in relation to the notification of personal data breaches in May 2018¹³³, August 2019 and October 2019¹³⁴ does not suggest the interpretation of Article 33(1), and in particular, the concept of controller awareness, adopted in the provisional finding.

In this regard, TIC stated that *“Neither piece of Guidance suggests a processor’s awareness being imputed to the controller where the controller has not been made aware.”¹³⁵*

¹³¹ Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, page 11

¹³² Submissions in relation to the Preliminary Draft, para 8.3

¹³³ Breach Notification Process under GDPR’, Data Protection Commission website

¹³⁴ ‘A Quick Guide to GDPR Breach Notifications’, Data Protection Commission, August 2019; ‘A Practical Guide to Personal Data Breach Notifications under the GDPR’, Data Protection Commission, October 2019

¹³⁵ Submissions in relation to the Preliminary Draft, para 3.10

(b) Outline of TIC's allegation that the provisional finding incorrectly applies a 'purposive interpretation' of Article 33(1)

- 7.61 TIC submitted that, in considering the obligation to notify under Article 33(1) in the context of controller obligations under the GDPR as a whole, the provisional finding in respect of Article 33(1) has misapplied a purposive interpretation to that provision.

TIC referred, in this regard, to the portion of my provisional finding, which was contained at Paragraph 7.20 of the Preliminary Draft and which outlined as follows:

"Having regard to the foregoing, and to the analysis which I have set out above at paragraphs 6.1 – 6.19, I am of the view that TIC's obligations under Article 33(1) cannot be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

*That this is the case is, as outlined above, supported by both the Recitals to the GDPR and the views of the EDPB, as set out in the Breach Notification Guidelines. **It also accords with the established principle of interpretation of EU law, applied by the CJEU in numerous decisions, whereby a provision of law is interpreted by reference not only to its wording but also to its purpose and the overall context in which it occurs.**"* (Emphasis added)

- 7.62 TIC submitted (at Paragraphs 8.10 to 8.12 of its Submissions in relation to the Preliminary Draft) that, in considering the obligation under Article 33(1) in the context of the controller obligations under the GDPR as a whole, the provisional finding has ignored the ordinary meaning of Article 33(1). In this regard, TIC asserted that:

"Contrary to the assertion in Paragraph 7.20 of the Draft Decision, the DPC's interpretation of Article 33(1) does not accord with the established principles of EU law. The CJEU's usual method of interpretation requires the application of literal, systematic and purposive criteria of interpretation...This means that the ordinary meaning of the words must be the starting point. The DPC's interpretation of Article 33(1) proceeds directly to a purposive interpretation ignoring the ordinary meaning of "after having become aware of it."¹³⁶

TIC further submitted that:

"It is not open to the DPC to apply a unique, national interpretation to the meaning of "after having become aware of it" in Article 33(1)."¹³⁷

¹³⁶ Submissions in relation to the Preliminary Draft, para 8.10

¹³⁷ Ibid, para 8.12

(c) *Outline of TIC's contention that the DPC's proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of a personal data breach*

- 7.63 Following on from its submission that the provisional finding incorrectly applied a purposive interpretation of Article 33(1), TIC further submitted that the approach adopted in the provisional finding has the effect of creating a strict liability obligation under Article 33(1), whereby a controller will be imputed with awareness of a personal data breach *at the same time* as its processor becomes aware.

In this regard, TIC submitted that my interpretation of Article 33(1), as set out in my provisional finding, “recasts TIC’s obligation as a strict liability obligation to have communication protocols in place with its processors that always lead to the controller becoming aware of the incident at the same time as its processor (or sub-processor).”¹³⁸

TIC further contended that:

*“In imputing Twitter Inc.’s awareness to TIC, the DPC is conflating TIC and Twitter Inc. and treating them as a single legal entity...The Breach Notification Guidelines make clear that awareness of the processor is not the same as awareness of the controller. Given this, it would not be appropriate to attribute the processor’s awareness to the controller in an arm’s length relationship. The DPC should not apply a higher standard merely because the entities are part of the same corporate group.”*¹³⁹

- 7.64 TIC further submitted that the interpretation, in my provisional finding, of the obligation under Article 33(1), and in particular, the concept of controller awareness, has the further effect that

*“...controllers will be held vicariously liable for a processor/sub-processor’s failure to comply with Article 33(2).”*¹⁴⁰

TIC further submitted that this interpretation could not have been anticipated by it, in view of the wording of Article 33(1) and Article 33(2).

(ii) *Summary of TIC’s submissions that the provisional finding implies obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1)*

- 7.65 As set out above, TIC submitted that my interpretation of Article 33(1) in the context of the broader obligations on controllers under the GDPR has the effect of implying into Article 33(1) other obligations, on a controller, and in particular those arising under Articles 24 and 32 of the GDPR.

¹³⁸ Ibid, para. 8.13

¹³⁹ Submissions in relation to the Preliminary Draft, para. 8.14

¹⁴⁰ Ibid, para 8.15

In this regard, TIC submitted that

“...the DPC has erred in making its [provisional] finding. The requirements to have appropriate measures in place to enable and demonstrate compliance with the GDPR and the data protection principles arise as separate obligations under Articles 24 and 32.”¹⁴¹

- 7.66 TIC further submitted that the provisional finding is incorrect as it holds TIC in breach of Article 33(1) *“...on the basis of an allegation that it failed to comply with obligations which arise under other Articles of the GDPR (which in any event Twitter strenuously denies) when the effectiveness of TIC’s security measures have been independently audited and benchmarked against the ISO requirements by a third party for almost ten years.”¹⁴²*

(iii) Summary of TIC’s submissions that in making the provisional finding, the Commission failed to adhere to fair procedures

- 7.67 Following on from its submissions that the effect of my interpretation of Article 33(1) is to imply into that provision the obligations that arise under Articles 24, 25 and 32 of the GDPR, TIC submitted that, in making my provisional finding, I extended the scope, or terms of reference, of the Inquiry. In this regard, TIC submitted, at Paragraphs 2(i) and (j) of its Submissions in relation to the Preliminary Draft, as follows:

“The DPC has not investigated, nor enquired of Twitter or TIC, whether TIC did in fact have appropriate processes in place. Indeed, the DPC’s Draft Decision expressly states in Paragraph 7.19 that “a detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic)”

“The terms of reference of the DPC’s inquiry were limited to Article 33(1) and Article 33(5) of the GDPR...The DPC, however, has de facto extended the scope of the inquiry by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice.”¹⁴³

- 7.68 TIC further submitted that the consequence of the provisional finding, which it submits has de facto extended the scope of the Inquiry without notice to TIC, is that TIC did not know the case it had to meet and was denied the opportunity to put its side of the case, as are the established requirements for fair procedures to be applied under Irish Constitutional and Administrative law.

In this regard, TIC contended that

¹⁴¹ Ibid, para 7.3

¹⁴² Ibid, para 7.4

¹⁴³ Submissions in relation to the Preliminary Draft, para 2(i) and (j)

“The DPC provided no notice to TIC that it was, de facto, extending the scope of its inquiry. By failing to (i) formally extend the scope of the inquiry and (ii) give TIC on notice of the extension, TIC was deprived of an opportunity to make submissions on the relevant issues.”¹⁴⁴

Consideration of TIC’s submissions in relation to the provisional finding that it did not comply with Article 33(1)

7.69 I have set out below my consideration of the three major aspects of TIC’s submissions and, specifically, its assertions that my provisional finding:

- (i) Incorrectly interpreted the concept of ‘controller awareness’ under Article 33(1) and incorrectly applied a ‘purposive interpretation’ of Article 33(1);
- (ii) Implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1); and
- (iii) Failed to adhere to fair procedures.

(i) Consideration of TIC’s submission that the provisional finding incorrectly interprets the concept of ‘controller awareness’ under Article 33(1) and incorrectly applied a ‘purposive interpretation’ of Article 33(1)

7.70 As set out above, the submissions made by TIC under this heading can be summarized as follows:

- (a) TIC asserted that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches.
- (b) TIC alleged that, in respect of how the provisional finding interprets the issue of controller awareness, it incorrectly applies a ‘purposive interpretation’ of Article 33(1);
- (c) TIC contended that “[the] DPC’s proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach”. TIC submitted that this, in turn, has the effect of making a controller vicariously liable for its processor/sub-processor’s failure to comply with Article 33(2).

I have considered TIC’s submissions below, in the order as summarized in this section.

¹⁴⁴ Ibid, para 9.3

(a) *Consideration of TIC's assertions that the interpretation of controller awareness in the provisional finding departs from the Breach Notification Guidelines and was also not suggested in guidance published by the Commission in relation to the notification of personal data breaches*

- 7.71 As set out above, I consider that a controller's obligation to notify a personal data breach under Article 33(1), and the prescribed timeframe within which this must take place, must be viewed *in the context of* its other obligations under the GDPR. Paragraphs 6.1 to 6.20 above set out the range of obligations imposed upon a controller that are relevant in this context.
- 7.72 The controller's obligation under Article 33(1) is to notify a personal data breach without undue delay and where feasible not later than 72 hours *after having become aware of it*. The timeframe for notification in Article 33(1), therefore, commences from when the controller 'becomes aware' of the breach. As such, the timeframe for notification of a breach under Article 33(1) is determined by the controller's ability, or readiness, to become aware of the breach.

As set out above, this is recognized by Recital 87, which provides that

*"It should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject."*¹⁴⁵

This is also clearly stated in the Breach Notification Guidelines, which provide that

*"...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. However...the GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subjects. **This 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.**"*¹⁴⁶ (Emphasis added)

- 7.73 Whilst it is the case, therefore, that Article 33(1) provides that a controller must notify a personal data breach within 72 hours *after having become aware of it*, the concept of the controller's 'awareness' under Article 33(1) and, more specifically, the timing of when this takes place, must be viewed in the context of the controller's ability to 'become aware' of the breach. The requirement under Article 33(1) that a controller notify a breach within 72 hours *after having become aware of it*,

¹⁴⁵ Recital 87, GDPR

¹⁴⁶ Breach Notification Guidelines, page 11

in other words, is predicated upon the controller's internal systems and procedures (and where applicable, those systems and procedures in place with any external parties including processors whether they are part of the same corporate structure or otherwise) being configured, and followed, so as to facilitate prompt awareness, and timely notification, of breaches.

This arises from the fact that the obligation to notify, under Article 33(1), is addressed to the controller, and from the fact that, under Article 5(2), the controller has overarching responsibility for ensuring compliance with the GDPR.

The necessary consequence of this (and the position that applies under Article 33(1)) can be seen in the following situation: where a personal data breach occurs in respect of personal data for which an organization is the controller but the controller either fails to detect, or become aware of, the breach or is delayed in detecting, or becoming aware of, the breach due either to its own failure to have effective processes in place, or due to an internal failure (by, for example, an employee) or an external failure (for example, on the part of a processor) to follow its own systems and procedures. In those circumstances, the controller cannot then seek to justify, or excuse, its consequent lack of compliance with Article 33(1) on the basis of the shortcomings in those failures (whether internal or external) which resulted in it not becoming aware of at all, or its delayed awareness of, the personal data breach in question.

- 7.74 Where a controller engages a processor to process personal data on its behalf and a personal data breach occurs in relation to the personal data processed by the processor, the timing of the controller's awareness of the personal data breach (for the purpose of Article 33(1)) will be dependent on when the controller is notified, or made aware, of the breach by its processor, unless the controller has some other independent method of becoming aware of such a breach outside of notification by the processor.

The only obligation on the processor, under Article 33, is that under Article 33(2) which requires that the processor *"...shall notify the controller without undue delay after becoming aware of a personal data breach."*¹⁴⁷

The controller, therefore, relies on the processor to make it aware of a breach without undue delay in order that it can, in turn, fulfil its obligation under Article 33(1) to promptly notify the breach to the supervisory authority.

- 7.75 Where a controller engages a processor to process personal data on its behalf, however, it remains the overall responsibility of the controller to ensure that the processing is carried out in compliance with the GDPR.

¹⁴⁷ Article 33(2) GDPR

As is outlined above, Article 28(1) provides that a controller must only use a processor that can provide “*sufficient guarantees*” to implement appropriate technical and organizational measures to ensure the processing complies with the GDPR and protects the rights of individuals. Article 28 also requires the controller to have a contract in place with its processor and to give the processor documented instructions to follow. As set out above in section 6, this will include a requirement, under Article 28(3)(f), that the processor is required to “[*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 responsibility for complying with those provisions is, however, solely that of the controller.

Furthermore, and pursuant to its accountability obligation under Article 5(2), the controller is responsible for overseeing the compliance of its processor. Article 28(3)(h), in this regard, makes provision for the processor to “...allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.”

- 7.76 Subject to the comments on constructive awareness further below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller’s *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor.

The Breach Notification Guidelines, in this regard, state as follows:

“The controller uses the processor to achieve its purposes; therefore in principle, the controller should be considered as “aware” once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). (Emphasis added)

The Guidelines go on to state that

“The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.”

- 7.77 As set out above, TIC contended that the analysis in the Preliminary Draft departed from the Breach Notification Guidelines in respect of the interpretation of the issue of controller ‘awareness’ for the purposes of the provisional finding in relation to Article 33(1).

In this regard, as set out above, TIC pointed to the change in wording between the earlier (2017) version of the Guidelines ('the earlier Guidelines') and the final version of the Breach Notification Guidelines dated February 2018 in respect of the issue of when the controller is considered to be 'aware' in the case of a breach of personal data by its processor. In particular, TIC pointed to the fact that the earlier Guidelines stated that:

*"The controller uses the processor to achieve its purposes; therefore, in principle, **the controller should be considered as "aware" once the processor has become aware.**"*

TIC pointed to the fact that this wording was amended in the (final) Breach Notification Guidelines to read as follows:

*"The controller uses the processor to achieve its purpose; therefore, in principle, **the controller should be considered as "aware" once the processor has informed it of the breach.**"*

- 7.78 Having considered TIC's submissions on this point (and as summarized above), I do not agree that my interpretation of the issue of controller awareness, for the purpose of Article 33(1), departs from the current Breach Notification Guidelines.

The Breach Notification Guidelines state that *"...in principle, the controller should be considered as "aware" once the processor has informed it of the breach."* However, the Guidelines further outline that, as the GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay", *"...WP29 recommends the processor **promptly** notifies the controller...This is in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours."* (Emphasis added)

The Guidelines further state, by specific reference to Recital 87, that in terms of when a controller is to be considered to be "aware" of a personal data breach, the controller is subject to an obligation *"...to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action."*¹⁴⁸

- 7.79 The controller's *awareness* of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor (unless there is some other method by which the controller can independently learn of the existence of a personal data breach other than from the processor).

Where that process – as agreed with the processor – is not effective in some respect, fails, or is not followed by the processor, such that, even in a once off or isolated situation the controller's awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own

¹⁴⁸ Breach Notification Guidelines, page 11

delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor's default.

- 7.80 As I set out in my provisional finding, I reiterate now that it is the controller's responsibility to ensure, by means of an effective process agreed with its processor, that its processor makes it aware of a personal data breach in such a manner so as to enable it (as controller) to comply with its own obligation to notify under Article 33(1).

Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails / is not followed correctly by the processor (as it ought to have been), and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

As I further outline below, I consider that such an interpretation of the concept of 'controller awareness' is necessary in order to ensure that the controller's obligation to notify under Article 33(1) remains effective. I also consider that this interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

- 7.81 TIC submitted, at paragraph 8.4 of its Submissions in relation to the Preliminary Draft, that

*"The DPC's rationale for departing from the position in the Breach Notification Guidelines (as set out in Paragraph 7.22 of the Draft Decision) is that if the performance by a controller of its obligation to notify is essentially contingent upon the compliance by its processor with the processor's obligations under Article 33(1), this would operate to render the Article 33(1) obligations on a controller ineffective. This logic is flawed. There are other obligations on the controller to ensure that the processor notifies it promptly, specifically the obligations referenced by the DPC to have technical and organizational measures in place to ensure that the processor notifies the controller without undue delay, notably, Articles 24 and 32...This ensures that the interpretation of "awareness" in the Breach Notification Guidelines does not render the obligation in Article 33(1) ineffective for ensuring notification, as the DPC asserts. It is not necessary to imply obligations arising under other Articles into Article 33(1)"*¹⁴⁹

TIC further contended that

"In addition to the other obligations on the controller to ensure prompt notification by the processor, Article 33(2) imposes a separate, direct obligation on the processor to notify the controller of personal data breaches without undue delay. This creates a statutory framework that, along with the

¹⁴⁹ Submissions in relation to the Preliminary Draft, para 8.4

measures that a controller has put in place, ensures controllers are informed of breaches at their processors.”¹⁵⁰

- 7.82 I do not agree with the arguments made by TIC in its submissions, and as set out above, to the effect that the rationale for the provisional finding is ‘flawed.’

The position adopted by TIC is that it was in compliance with Article 33(1) because it notified the Breach to the Commission within 72 hours of TIC becoming aware of it, notwithstanding the fact that there was a four day delay between its processor forming the view that the issue was a notifiable personal data breach and its notification of same to TIC as controller. While I have considered TIC’s submissions, as discussed above on this matter, I continue to hold the view, which was set out in the provisional finding, and as outlined above, that this interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor, Twitter Inc. and, in particular, for **ensuring** that its own processor made it aware of any data breach in a manner that would enable TIC to comply with its obligation to notify under Article 33(1). In this context, I would emphasise that, as referred to above, the Breach Notification Guidelines reinforce the principle that the processor must **“help the controller to meet the requirement of notification to the supervisory authority within 72 hours.”** For this reason, TIC cannot, as controller, seek to excuse its own delay in notifying the Breach on the basis that the protocol, which it had agreed with its processor, was not followed in this instance.

In this regard, and as set out above, I note that TIC acknowledged that there was a failure by the Twitter Inc. DART team (or an engineer on that team), to follow an element of the protocol in place with its processor. I further note that TIC confirmed that this arose because the DART team (or an engineer on that team) assumed that, because the relevant members of the Twitter Inc. legal team were already involved at that point in time, the relevant step (Step 5 ‘Escalation to Legal’) had been completed, including the requirement in that step that the DPO (and, therefore, TIC as controller) be notified.

As set out above, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team and / or individual Twitter Inc. engineer as to *who* had been informed of the issue when the legal team were already involved and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single composite step entitled ‘Escalation to Legal’.

¹⁵⁰ Ibid, para. 8.5

As I have stated above, I accept TIC's submission that this was an isolated failure and that it was not indicative of a broader, systemic issue. However, despite the isolated nature of the incident underlying the Breach, I consider that the DART Runbook, as it was at the relevant time, did not appear to have been clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the Twitter Inc. legal team **and** the DPO. As noted above, I consider that the subsequent amendment of the Runbook and TIC's comments in respect of same are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

In this regard, as I have also stated above, I note that TIC confirmed, in its Submissions in relation to the Preliminary Draft, that it amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to "...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly".¹⁵¹

The updated DART Runbook was furnished to the Commission during the course of the Inquiry, specifically with TIC's Submissions dated 8 February 2019. Having re-examined the updated version of the DART Runbook in light of TIC's submission on this issue, I note that the relevant part of the DART Runbook, relating to Twitter Inc.'s notification of an incident or breach to TIC, now deals *separately* with the requirements to notify the TIC DPO, as distinct from the named members of Twitter Inc.'s legal team.

- 7.83 I also continue to hold the view, as set out in the provisional finding in the Preliminary Draft, that the interpretation being advanced by TIC – whereby the performance by a controller of its obligation to notify is contingent upon the compliance by its processor with its own free-standing obligation under Article 33(2) – would undermine the effectiveness of Article 33 as an obligation on a controller. This is in circumstances where such an approach would effectively mean that the time for notification of a personal data breach to a supervisory authority would only start to run at the point when the processor had informed the controller of the breach (if at all).

Such an approach would give rise to a situation whereby notification would be delayed for an extended period of time, or never take place, and the controller would avoid its obligations under Article 33(1). As noted above, TIC argued in its Submissions in relation to the Preliminary Draft that this interpretation is flawed and that:

*"There are other obligations on the controller to ensure that the processor notifies it promptly, specifically the obligations referenced by the DPC to have technical and organizational measures in place to ensure that the processor notifies the controller without undue delay, notably, Articles 24 and 32..."*¹⁵²

¹⁵¹ Submissions in relation to the Preliminary Draft, para 5.17

¹⁵² Submissions in relation to the Preliminary Draft, para 8.4

However, the issue here is ultimately about ensuring that the controller *notifies* the supervisory authority so that the objectives behind the data breach notification system (as already discussed) concerning protection of data subjects are met. Importantly, those other obligations (under Articles 24 and 32) which TIC pointed to address the other ways of ensuring that the processor notifies the controller of a data breach. They do not address any other means of ensuring that the controller actually makes the data breach notification to the supervisory authority. Therefore, those other obligations do not address the gap in compliance which could arise based on the interpretation TIC advocates for, whereby notification of the data breach by the controller is entirely dependent upon having been notified in the first place by the processor.

- 7.84 In this regard, if a processor fails to notify its controller about a data breach, in the absence of any other method by which the controller can learn about the data breach, the consequence is that there will be no notification of the data breach to the supervisory authority (and potentially, therefore, affected data subjects will not benefit from the protections inherent in the GDPR's data breach notification system).

The fact, therefore, that the processor has obligations under Article 33(2) to notify the controller about the data breach, and obligations flowing from the technical and organizational measures which the controller has in place with the processor, pursuant to the controller's own obligations under Articles 24 and 32, does not ameliorate the obvious lacuna, arising from the consequence of TIC's interpretation of Article 33(1), which is that a controller will not have infringed Article 33(1) due to its own non-notification of a breach to the supervisory authority if it has not been told about the breach by its processor in the first place.

Furthermore, as I outlined in my provisional finding, such an approach is entirely at odds with the overall purpose of the GDPR and the intention of the legislator, which is clearly to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded (to the extent possible by mitigating the risks to them arising from a data breach), by action on the part of the supervisory authority – for example, by requiring the controller to notify data subjects about the breach under Article 34(4).

- 7.85 As I have set out above and further below, the controller's obligation under Article 33(1) and, in particular, the issue of controller awareness, must, in order to be effective, be considered *in the context of* those other obligations and, also, in the context of the controller's overall responsibility for ensuring the compliance of its processor. I do not accept TIC's submission, and which I address further separately below, that this has the effect of implying other obligations (such as those under Articles 24 and 32) into Article 33(1).
- 7.86 TIC further submitted that the potential consequence, which I had identified in my provisional finding (and which is set out above at paragraph 7.83), of the proposed approach by TIC to Article 33(1), being that *"...the time for notification of a personal data breach to a supervisory authority would*

*only start to run at the point when the processor finally informed the controller of the breach (if at all)”, was an issue of which the Article 29 Working Party was fully cognizant but that it “nevertheless determined that a controller’s awareness runs from the point at which the processor informs them of a breach.”*¹⁵³

I do not accept TIC’s submission in this respect. The current Breach Notification Guidelines clearly do not envisage, or endorse, the approach that is proposed by TIC, whereby a failure on the part of a processor to discharge its obligation to make a controller aware of a breach “without undue delay” under Article 33(2) effectively operates to release a controller from its obligations under Article 33(1).

The Breach Notification Guidelines state that “...*in principle, the controller should be considered as “aware” once the processor has informed it of the breach.*” However, this is clearly considered in the context (as per Recitals 85 and 87) of the controller having appropriate measures in place to ensure that it actually does become “aware” of a personal data breach, for the purposes of Article 33(1), promptly.

- 7.87 Having regard to the above, therefore, I do not accept TIC’s submission that my provisional finding departs from the current Breach Notification Guidelines.
- 7.88 In its Submissions in relation to the Preliminary Draft, TIC also submitted that my provisional finding and, in particular, my consideration of the controller’s obligation under Article 33(1) in the context of the broader obligations on a controller under the GDPR, is not suggested in the guidance relating to the notification of personal data breaches that has been issued to date by the Data Protection Commission.

As TIC outlined in its Submissions, the Commission issued guidance in August 2019 and in October 2019. Both guidance documents reflect the position that “*A controller should be regarded as having become ‘aware’ of the breach when they have a reasonable degree of certainty that a security incident has occurred and compromised personal data.*”¹⁵⁴ In addition, both documents outline that “*per Article 33(2) GDPR, a processor, processing personal data on the direction of a controller, must notify the controller of any personal data breach without undue delay after becoming aware of the breach. This is of key importance in enabling the controller to comply with its notification obligations.*”¹⁵⁵

TIC submitted that the approach adopted in the provisional finding in respect of Article 33(1) is not suggested in these guidance documents and that, in particular, the documents “...*did not provide guidance on the meaning of awareness.*”¹⁵⁶

¹⁵³ Submissions in relation to the Preliminary Draft, para 8.6

¹⁵⁴ ‘A Practical Guide to Personal Data Breach Notifications’, Data Protection Commission, page 4

¹⁵⁵ ‘A Practical Guide to Personal Data Breach Notifications’, Data Protection Commission, page 5

¹⁵⁶ Submissions in relation to the Preliminary Draft, para. 3.8

7.89 I have considered TIC's submissions on these points but I do not accept them for the following reasons. As guidance documents, these publications are intended to provide controllers and processors with practical guidance in respect of the handling of personal data breaches. The documents are not intended to be exhaustive statements of the law, nor are they intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR in specific factual matrices such as this one.

However, both documents are entirely consistent with the position adopted in the current Breach Notification Guidelines, and which is set out above. In this regard, neither document envisages, or endorses, the approach being suggested by TIC whereby a failure on the part of a processor to discharge its obligation to make a controller aware of a breach "without undue delay" under Article 33(2) effectively operates to release a controller from its obligations under Article 33(1). In addition, neither document envisages or endorses, a situation whereby a protracted delay on the part of the processor to inform the controller means that an equivalent protracted delay in the controller notifying the supervisory authority will have no consequence in terms of compliance with Article 33(1), despite the potentially very serious consequences for data subjects in not having been made aware and/or benefitted from advice from the supervisory authority, where required, on how to mitigate damage to their own position arising from the personal data breach.

7.90 Having regard to the foregoing, therefore, and in summary, I do not accept TIC's submission that, in interpreting the controller's obligation to notify a breach under Article 33(1), in the context of the controller's obligations under the GDPR as a whole, *my provisional finding departs from the current Breach Notification Guidelines or guidance* issued by the Commission. I summarize my reasons for this below:

- Subject to the further points below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller's *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor.
- The controller's *awareness* of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor (unless there is some other method by which the controller can independently learn of the existence of a personal data breach other than from the processor). It is the controller's overall responsibility to oversee the processing operations carried out by its processor and, as part of this, to ensure that its processor makes it aware of any data breach in a manner that will enable it to comply with its obligation to notify under Article 33(1).

- In such circumstances, where that process – as agreed with the processor – **is not effective in some respect, fails, or is not followed by the processor, such that even in a once off or isolated situation** the controller’s actual awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor’s default.
- This is recognized by the current Breach Notification Guidelines which state that “*...in principle, the controller should be considered as “aware” once the processor has informed it of the breach.*” However, this is clearly considered in the context (as per Recitals 85 and 87) of the controller having appropriate measures in place to ensure that it actually does become “aware” of a personal data breach, for the purposes of Article 33(1), promptly.

7.91 Therefore, a controller must ensure, by means of an effective process agreed with its processor, that its processor makes it aware of a personal data breach in such a manner so as to enable it (as controller) to comply with its own obligation to notify under Article 33(1).

Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails / is not followed correctly by the processor (**as it ought to have been**), and this results in a delay or failure in the processor making the controller aware of the breach even in a once-off situation, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

Such an interpretation of the concept of ‘controller awareness’ is necessary in order to ensure that the controller’s obligation to notify under Article 33(1) remains effective, and also reflects the responsibility and accountability of the controller in the GDPR scheme.

In the context of the above, I also do not consider that such an interpretation of controller awareness is inconsistent with the current Breach Notification Guidelines which clearly view the concept of controller ‘awareness’ in the context of the controller (as per Recitals 85 and 87) having appropriate measures in place to ensure that it becomes “aware” of a personal data breach, for the purposes of Article 33(1), promptly.

(b) Consideration of TIC’s allegation that the provisional finding incorrectly applies a ‘purposive interpretation’ of Article 33(1)

7.92 As set out above, TIC submitted that, in considering the obligation to notify under Article 33(1) (and, in particular, the issue of controller awareness), in the context of controller obligations under the GDPR as a whole, the provisional finding in respect of Article 33(1) has misapplied a purposive interpretation to that provision.

In that respect, TIC submitted (at paragraphs 8.10 and 8.11 of its Submissions in relation to the Preliminary Draft) that the provisional finding ignores the ordinary meaning of Article 33(1) and, in particular, the wording whereby a controller is required to notify a personal data breach to a supervisory authority not later than 72 hours “...*after having become aware of it.*” TIC cites a number of authorities in support of its submission.¹⁵⁷

TIC also submitted (at paragraph 8.12 of its Submissions in relation to the Preliminary Draft) that

“It is not open to the DPC to apply a unique, national interpretation to the meaning of “after having become aware of it” in Article 33(1).”

I have considered TIC’s submissions, in this regard, however I do not accept same for the reasons which I have set out below.

- 7.93 Firstly, contrary to the argument at paragraph 8.12 of TIC’s Submissions in relation to the Preliminary Draft (and as referred to above), the Commission is not seeking to apply a “*unique, national interpretation*” to Article 33(1). As a provision of EU law, Article 33(1) must be given an autonomous and uniform interpretation throughout the EU. In the absence of authority from the CJEU on this point, it falls to the Commission to give Article 33(1) such an interpretation consistent with the applicable principles of EU law.
- 7.94 As regards those principles, it is correct, as TIC submitted at paragraph 8.10 of its Submissions in relation to the Preliminary Draft, that the CJEU applies literal, systematic and purposive criteria of interpretation. The literal meaning is, however, the starting point only.¹⁵⁸ The purposive approach is “*the characteristic element in the Court’s interpretive method*”.¹⁵⁹ Thus, the literal meaning of the words takes no precedence over context and purpose. Indeed, in construing the relevant EU case law, the UK courts have held that “*of the four methods of interpretation – literal, historical, schematic and teleological – the first is the least important and the last the most important*”.¹⁶⁰
- 7.95 The corollary to the purposive or “*teleological*” method is the principle of *effet utile*. The doctrine provides that “*once the purpose of a provision is clearly identified, its detailed terms will be interpreted so “as to ensure that the provision retains its effectiveness”... [the Court will] seek above all, effectiveness, consistency, and uniformity in its case law and in the application of Community law. Consequently, the Court either reads in necessary provisions regarding cooperation or the furnishing of information to the Commission, or bends or ignores literal meanings. Most shockingly of all to the*

¹⁵⁷ Submissions in relation to the Preliminary Draft, para. 8.11 where TIC cites Egenberger (C-414/16), paragraph 44; Wightman and Others (C-621/18), paragraph 47; and *Rimšēvičs and ECB v Latvia* (C-202/18 and C-238/18)

¹⁵⁸ *CILFIT e.a.*, C-283/81, ECLI:EU:C:1982:335, §20

¹⁵⁹ N. Fennelly *Legal Interpretation at the European Court of Justice* Fordham Int LJ [1997] 656 at 664.

¹⁶⁰ *Shanning International Ltd v Lloyds TSB Bank plc* [2001] UKHL 31 [2001] 1 WLR 1462 per Lord Steyn at §34, to the same effect see O'Donnell J in *NAMA v The Commissioner for Environmental Information* [2015] 4 IR 626 at §13.

*common lawyer, the Court fills in lacunae which it identifies in legislative or even EC Treaty provisions.”*¹⁶¹

7.96 Accordingly, the CJEU has laid down a specific rule of construction that when a provision is open to more than one interpretation, and one interpretation will allow it to “achieve its purpose” and “ensure that [it] retains its effectiveness”, the court should prefer that interpretation over others that do not.¹⁶²

7.97 These principles are illustrated in one of the authorities cited in TIC’s Submissions in relation to the Preliminary Draft (at paragraph 8.11 thereof), *Rimšēvičs and ECB v Latvia*¹⁶³. That case concerned a decision by the Latvian Anti-Corruption Agency to remove from office the Governor of the Latvian Central Bank. This decision was challenged by the ECB before the CJEU. The Latvian government argued that, under the EU legislation in question, its decision could be reviewed by the CJEU only where the “legal and institutional link” between the individual and the national central bank had been completely severed. The Latvian decision was temporary and interim in nature, pending an investigation.

The CJEU, at paragraph 44, noted as follows:

“...it is true that, as the Advocate General noted in point 78 of her Opinion, the terms used in the second subparagraph of Article 14.2 of the Statute of the ESCB and of the ECB to define the subject matter of the review envisaged therein appear to evoke, in the Latvian version as in several other language versions of that provision, the definitive severing of the link between the national central bank and its governor”.

The CJEU held, however, that this literal meaning of the provision was superseded by an interpretation necessary to secure the objectives of the measure. In that case, the protection of the independence of Eurozone central bank governors (paragraphs 45-55).

7.98 Having regard to the above, therefore, the key questions are (1) what is the purpose of Article 33(1) GDPR; and (2) which available interpretation secures that purpose?

As set out above, the purpose of Article 33(1) is to ensure the prompt notification by controllers of personal data breaches to a supervisory authority so that a supervisory authority can assess the

¹⁶¹ N. Fennelly *Legal Interpretation at the European Court of Justice* Fordham Int LJ [1997] 656 at 674. See also, P. Lasok and T. Millett, *Judicial Control in the EU*, at §661: “the literal meaning of a provision must be discarded if it is inconsistent with the purpose, general scheme and the context in which it is to be applied”.

¹⁶² *Land de Sarre v Ministre de L’Industrie*, C-187/87, ECLI:EU:C:1988:439, §19

¹⁶³ C-202/18 and C-238/18, EU:C:2019:139

circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded.¹⁶⁴

The interpretation of Article 33(1) which ensures its effectiveness is one where, in appropriate circumstances, the controller is treated as having constructive awareness of a personal data breach through its processor. Such an interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

The effect of this is that whilst, in principle, a controller will be considered to be 'aware' of a breach from the time at which it is notified by its processor, the controller must ensure that it has sufficient measures in place to facilitate this awareness. A controller cannot seek to excuse its own delay in notifying a personal data breach (or a failure to notify a personal data breach) on the basis of shortcomings in, and/or a failure to follow, its own internal processes or those agreed with its processor, and which directly caused its delayed awareness of (or failure to notify) the breach.

Such an interpretation reflects the responsibility and accountability of the controller in all circumstances under the GDPR scheme.

- 7.99 The alternative interpretation in these circumstances, that a controller is only "aware" when informed by its processor, leaves a significant lacuna in the protection provided by the GDPR. Such an interpretation could result in the controller avoiding responsibility even in respect of very significant delays in notifying breaches to the supervisory authority (or failing to notify), provided that the controller could show that it satisfied its obligations in choosing a processor and ensuring that proper systems were in place. If those systems were disregarded by the processor, and significant harm caused to the data subjects, enforcement measures could not be taken by the supervisory authority in respect of the delayed notification or non-notification against the controller as there would be no infringement of Article 33(1).

In view of the importance of the provisions and the overriding need to secure the most rapid notification of breaches to the supervisory authority, it is necessary that **both** the controller and its appointed processor remain subject to live and continuing obligations in such circumstances.

- 7.100 That interpretation is not undermined by the fact that the GDPR requires a processor to notify the controller of any breach without undue delay (Article 33(2)). The obligations on the processor are supplementary to those on the controller. Even if the controller has constructive awareness of a

¹⁶⁴ This underlying objective is apparent from Recital 85 which states that "*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons... Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority...*" The role of the supervisory authority in overseeing the mitigation of risks to data subjects is also evident from Recital 86 which states that communication of data breaches which are likely to pose a high risk to data subjects should be made by a controller to data subjects "*as soon as reasonably feasible and in close co-operation with the supervisory authority, respecting the guidance provided by it...*"

breach and is subject to any enforcement action by a supervisory authority in the event of an infringement of Article 33(1), it is still nevertheless important that the processor communicate the breach rapidly on pain of being subject to separate enforcement action by the supervisory authority.

(c) Consideration of TIC's contention that "[the] DPC's proposed purposive interpretation amounts to imputing awareness to a controller at the same time as its processor became aware of [a] personal data breach"

7.101 As set out above, TIC also submitted that the interpretation of Article 33(1), and in particular, of the concept of controller awareness, in the provisional finding has the effect of creating a strict liability obligation, whereby a controller will be imputed with awareness of a personal data breach *at the same time* that its processor becomes aware. TIC also submitted that a further effect of this is that a controller would be held vicariously liable for a processor/sub-processor's failure to comply with Article 33(2).

I have set out my view below in respect of both of these contentions advanced by TIC.

7.102 Firstly, the issue of the purposive interpretation which is applied to Article 33(1) and the reasons based on EU law underpinning the legitimacy of same have been set out in detail from paragraph 7.92 to 7.100 above. In essence, as explained in those paragraphs, EU law and the principle of *effet utile* requires that "*once the purpose of a provision is clearly identified, its detailed terms will be interpreted so "as to ensure that the provision retains its effectiveness..."*

7.103 As already set out, I consider that the interpretation of Article 33(1) which ensures its effectiveness is one where, in appropriate circumstances, the controller is treated as having constructive awareness of a personal data breach through its processor. Such an interpretation reflects the responsibility and accountability of the controller in the GDPR scheme.

For the reasons described above, this approach is lawful and appropriate in accordance with the principles applying to interpretation of EU law. As also stated above, the effect of this is that whilst, in principle, a controller will be considered to be 'aware' of a breach from the time at which it is notified by its processor, the controller must ensure that it has sufficient measures in place to facilitate this awareness. A controller cannot, therefore, seek to excuse its own delay in notifying a personal data breach (or a failure to notify a personal data breach) on the basis of shortcomings in, or a failure to follow, its own internal processes or those agreed with its processor, and which directly caused its delayed awareness of (or failure to notify) the breach.

7.104 In such circumstances, where the process – as agreed with the processor – even in a once off or isolated situation, **is not effective in some respect, fails, or is not followed by the processor (as it ought to have been)**, and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having

constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

7.105 I do not agree that, as submitted by TIC, such an interpretation creates a strict liability obligation under Article 33(1) whereby a controller will automatically be imputed with awareness of a breach *at the same time* as its processor. My finding recognizes that it will usually be the case that a processor that 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, for the purposes of Article 33(1), in a manner that enables it to comply with its obligation to notify same under Article 33(1).

7.106 As set out above, TIC further submitted that a consequence of my interpretation of Article 33(1) is that controllers will be held ‘vicariously liable’ for a processor/sub-processor’s failure to comply with Article 33(2).

TIC submitted, in this regard, that *“That controllers are not intended to be vicariously liable for the actions of their processors is reinforced by Article 82(2) of the GDPR. It is clear from Article 82(2) that a processor will be liable for damage caused by processing only where it has not complied with its obligations under the GDPR.”*¹⁶⁵

I consider that TIC’s submission that my provisional finding on Article 33(1) has the effect of making it, as controller, ‘vicariously liable’ for the failure of its processor to comply with Article 33(2), is misplaced. Vicarious liability is a common law concept whereby a party who is not personally at fault is legally required to bear the burden of another’s tortious wrongdoing. This is not consistent with my provisional finding that TIC did not comply with Article 33(1) as it does not take account of the fact that the controller has primary, and overall, responsibility for ensuring compliance with the GDPR.

7.107 The primary responsibility of the controller is recognized by Article 82(2) which provides that *“Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.”* Article 82(2) then goes on to state, in respect of processors, that *“A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.”*

The only defence to liability under Article 82 is that under subsection (3), which provides that a controller or processor shall be exempt from liability if it proves that it is *“not in any way”* responsible for the event giving rise to the damage.

¹⁶⁵ Submissions in relation to the Preliminary Draft, para 8.15

Article 82 provides for a liability regime whereby the controller, as the party that carries primary responsibility for compliance, can be held liable for damages arising from *any* infringement of the GDPR. The processor can be held liable for damages in case of its failure to comply with an obligation of the GDPR specifically directed to the processor or where it has acted contrary to the lawful instructions of the controller.

Article 82, therefore, recognizes the controller's primary responsibility for compliance under the GDPR, both in respect of its own processing of personal data and in respect of processing carried out by a processor on its behalf.

7.108 Having regard to the above, therefore, I do not agree with TIC's submission that the interpretation of controller awareness followed in my provisional finding gives rise to a strict liability obligation under Article 33(1), whereby a controller will always be considered to be aware of a breach at the same time as its processor becomes aware.

As I have outlined above, I consider that, having regard to the controller's overall responsibility and accountability under the GDPR, the controller must ensure that, by means of an effective process agreed with its processor, it is made aware of personal data breaches in such a manner as to enable compliance with its own obligation under Article 33(1).

In such circumstances, where the process – as agreed with the processor – even in a once off or isolated situation, **is not effective in some respect, fails, or is not followed by the processor (as it ought to have been)**, and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, in these circumstances, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

(ii) Consideration of TIC's submissions that the provisional finding implied obligations arising under other Articles of the GDPR, in particular Articles 24 and 32, into Article 33(1)

7.109 I now turn to address TIC's submission that, in viewing Article 33(1), and the controller's obligation therein, in the context of the other obligations on a controller under the GDPR, my provisional finding 'implies' the obligations arising under those provisions into Article 33(1).

7.110 I do not agree with TIC's submission in this regard. As already set out above, the obligation to notify under Article 33(1) – and the issue of the controller's awareness of a breach - must be considered in the context of the other obligations on a controller under the GDPR, as I have done. I do not accept TIC's submission that my finding:

“...[held] TIC in breach of Article 33(1) on the basis of an allegation that it failed to comply with obligations which arise under other Articles of the GDPR...”¹⁶⁶

7.111 In considering the issue of TIC’s compliance with Article 33(1), it was necessary to consider the facts in relation to the timing of its notification of the Breach to the Commission. The timing of the notification to the Commission, and in particular, the factors that led to the delay in TIC being *made aware* of the Breach by its processor, were relevant issues that were considered during the Inquiry in order to assess TIC’s compliance, as a controller, with its obligation under Article 33(1).

Any consideration of TIC’s processes, as applied between TIC and Twitter Inc., both by the Investigator during the Inquiry or by me as decision maker, was solely for the purpose of examining the facts surrounding TIC’s notification of the Breach to the Commission and assessing TIC’s compliance with Article 33(1).

Furthermore, no provisional finding was made either expressly or by implication (and no such finding will be made) under any provision, other than under Article 33(1) and Article 33(5). Rather, TIC’s assertions in this regard arise from my consideration of the obligation under Article 33(1) in the context of the broader obligations on a controller under the GDPR as a whole.

7.112 The consideration given in the Preliminary Draft, and above, to the controller’s obligations arising under Articles 5(2), 24, 25, 28 and 32, was solely for the purpose of demonstrating that the obligation under Article 33(1) on a controller must be viewed in the context of the broader obligations on a controller under the GDPR and, in particular, must be understood by reference to the controller’s primary responsibility for ensuring compliance with the GDPR.

This is in circumstances where a controller is obliged to ensure that it has measures in place to facilitate timely ‘awareness’ and notification of breaches for the purpose of Article 33(1).

(iii) Consideration of TIC’s submissions that in making the provisional finding, the Commission failed to adhere to fair procedures

7.113 As set out above, TIC also submitted that, in making my provisional finding, under Article 33(1), I have, de facto, extended the terms of reference of the Inquiry *“...by relying on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1), which offends the principles of natural justice.”*

For the reasons which I have set out above and further below, I do not accept TIC’s submission in this respect.

¹⁶⁶ Submissions in relation to the Preliminary Draft, para 7.4

7.114 The terms of reference, or scope, of the Inquiry was outlined in the Notice (informing TIC of the commencement of the Inquiry) sent to TIC on 22 January 2019. Paragraph 12 of the Notice, headed ‘Scope of Inquiry’, in this regard outlined as follows:

“The Inquiry commenced by this Notice will examine whether or not TIC has discharged its obligations in connection with the notification of the Data Breach to the DPC by TIC and TIC’s compliance with Article 33(1) and Article 33(5) GDPR and determine whether or not any provision(s) of the Act and / or the GDPR has been, is being or are likely to be contravened by TIC in that context.”

7.115 The Inquiry was commenced in circumstances where, as set out above at paragraphs 2.11 and 2.12, on the basis of the information contained in the Breach Notification Form, the Investigator was of the initial understanding that TIC had become aware of the Breach either on 26 December 2018 or on 3 January 2019, which, in either case, meant that the notification to the Commission on 8 January 2019 had taken place outside of the 72 hour timeframe allowed by Article 33(1).

7.116 The purpose of the Inquiry was, therefore, to establish the facts relating to TIC’s notification of the Breach to the Commission and, in particular, the apparent delay in TIC making the notification, with a view to establishing whether TIC had complied with its obligations as a controller under Article 33(1).

As set out above, in order to establish whether TIC had complied with Article 33(1), it was necessary to consider the facts in relation to the *timing* of its notification of the Breach to the Commission. In doing so, the Investigator raised queries in relation to, *inter alia*, the factors that had led to the delay in TIC being *made aware* of the Breach by its processor and in relation to the timing of TIC’s *awareness* of the Breach relative to when TIC notified the Breach to the Commission.

For this purpose, the Investigator, therefore, sought and obtained information from TIC in respect of the relevant process which it had in place, and which it had agreed with its processor, Twitter Inc, for the management of incidents.

7.117 During the course of the Inquiry, TIC made five rounds of submissions to the Commission, arising from queries raised by the Investigator.

An outline of these submissions, and what they related to, is set out below. The outline below demonstrates that the issues that were raised and considered by the Investigator during the course of the Inquiry concerned the timeline of events leading up to TIC’s notification of the Breach to the Commission; the process (as outlined in the DART Runbook) that was followed; and the issue of when, and how, TIC (as controller) was made aware of the Breach.

- a. The Notice (dated 22 January 2019) requested TIC to provide to the Commission all information in TIC’s possession which, pursuant to Article 33(5), it had documented comprising the facts

relating to the Breach, its effects and the remedial action taken. The Notice also requested TIC to provide the Commission with all relevant supporting documentary evidence.

- b. TIC responded to the Notice by way of correspondence, with enclosed documentation, on 25 January 2019 (Submissions dated 25 January 2019). TIC's response set out a timeline in respect of its notification of the Breach to the Commission, which referred to delays having occurred in the early part of the process leading up to notification of the Breach. TIC also referred in this letter to the meeting that took place on 7 January 2019 and that "*members of TIC's and Twitter's executive teams were made aware of the incident*" on that date but did not specify when TIC (as controller) had been made aware of the incident.
- c. Arising from TIC's Submissions dated 25 January 2019, the Investigator raised further queries, seeking to establish, *inter alia*, the facts surrounding when TIC (as controller) had been made aware of the Breach; and how this notification to TIC (as controller) had taken place (by reference to *Step 5 'Escalation to Legal'* in the DART Runbook). Specifically, in this regard, the Investigator sought to clarify *when* the required action in that step, being the addition of the TIC DPO (and the member of Twitter Inc.'s legal team), had been completed.
- d. In response, TIC made a further submission on 1 February 2019 (Submissions dated 1 February 2019), wherein it outlined a further timeline relating to the notification of the Breach and, in that regard, confirmed, *inter alia*, that on 3 January 2019, Twitter Inc.'s Legal Team had determined that the issue may constitute a personal data breach. In its Submissions dated 1 February, TIC also confirmed that on 7 January 2019, Twitter Inc. notified TIC's Global Data Protection Officer.

TIC also noted, in its Submissions of that date, that "*...delays appear to have occurred in the triage of the[Bug bounty] report, execution of the Twitter Inc. incident response plan...and notification to TIC.*"

TIC further confirmed that, in respect of the query raised by the Investigator regarding when Step 5 in the DART Runbook had been completed, that the "*...the Investigation Ticket and IM Ticket were created on 4 January 2019 and Twitter Inc.'s legal team was also added at this time.*" TIC further confirmed that "*There is no notation of [notification to the DPO] in the ticket as the Global Data Protection Officer was notified orally on 7 January 2019...*"

- e. A further request for clarification was raised by the Investigator on 6 February 2019, seeking, *inter alia* documentary evidence from TIC in relation to when *Step 5* of the DART Runbook had been completed and documentary evidence demonstrating that the DPO had been notified on 7 January 2019.

In the correspondence of this date, the Investigator also directly cited the text of *Step 5/Escalation to Legal* and sought confirmation as to whether this was the correct step *..."for adding legal resources as outlined in the [DART Runbook] as submitted by TIC on 25 January*

2019". (*The Investigator's query in this regard was raised in light of the fact that TIC had referred in its previous response to Step 5 as being entitled 'Review by Legal' which prompted a concern by the Investigator that TIC was referring to a different document*).

- f. TIC responded on 8 February 2019 (Submissions dated 8 February 2019) and confirmed, *inter alia*, that 'Step 5/ Escalation to Legal' (as referenced by the Investigator) was the correct step.

TIC also confirmed that "*Please note, the DART Runbook (Exhibit C to our 25 January 2019 letter) has been updated based on our learnings from the incidents the company has reported since 25 May 2018*" and it provided a copy of the updated DART Runbook.

In relation to the question of when 'Step 5 'Escalation to Legal' in the DART Runbook had been completed, TIC confirmed that

"As noted in our 25 January 2019 letter, a member of the Twitter Inc. legal team – who would have been added pursuant to "5/Escalation to Legal" – was consulted by the Information Security team on 3 January 2018 after they had determined that the issue was not a security risk but may have been a potential privacy risk. As a result, this member of Twitter Inc.'s legal team who would have been added pursuant to "5/Escalation to Legal" was already involved in the incident. Thus "5/Escalation to Legal" was not followed as prescribed in the runbook, and resulted in a delay in notifying the Global DPO."

In addition, TIC furnished documentary evidence, in the form of a Calendar Invite, relating to the TIC DPO's attendance at an incident response meeting on 7 January 2019.

- g. Following consideration of all matters, as presented by TIC in the course of its submissions (and as summarised above), the Investigator issued a Draft Inquiry Report to TIC on 17 June 2019. The Draft Inquiry Report, *inter alia*, outlined (at section D.1.3.2) the Investigator's concerns during the Inquiry relating to the DART Runbook and, in particular, noted (at paragraph 116) that *"...TIC's awareness of the Breach was dependent on the successful execution of the procedure outlined therein. In this respect, the investigator also noted, and was concerned that the elements of the procedure outlined at phase 5 potentially represented a single point of failure in the notification process."* The Investigator, however, noted that, as a procedural document, the Runbook did not allow for verification of when the DPO was made aware of the Breach.

The Investigator's provisional finding, in respect of Article 33(1) was that TIC had not demonstrated that it complied with its Article 33(1) GDPR obligation to notify the Breach without undue delay or indeed within 72 hours of awareness.

- h. TIC's Submissions in relation to the Draft Report were furnished to the Commission on 17 June 2019. In addition to setting out a further overview of events leading to the notification of the Breach, TIC's submissions confirmed again that, while Twitter Inc.'s legal team determined the issue as being a potential personal data breach on 3 January, a failure by Twitter Inc. to follow the incident management process at that point meant that the TIC DPO was not added to the IM

ticket, which in turn “*meant TIC was not notified of the incident as rapidly as would usually happen under Twitter Inc.’s incident response process.*” TIC also made further submissions in relation to, *inter alia*, the issue of when the TIC DPO became aware of the Breach and in respect of the verification of this issue. In addition, TIC confirmed in its submissions that the DART Runbook, as a procedural document, did not verify the time at which the TIC DPO had become aware of the Breach.

- i. As set out above, the Investigator’s final Inquiry Report was issued on 21 October 2019. As set out above, the Investigator’s view, in respect of Article 33(1), was that it was not possible to establish whether TIC had complied with its obligation under Article 33(1). This was on the basis that TIC’s documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became ‘aware’ of the Breach, did not verify such compliance.

7.118 As the above demonstrates, during the Inquiry, the Investigator raised queries in respect of the timeline of events leading up to TIC’s notification of the Breach to the Commission; the process (as outlined in the DART Runbook) that was followed; and the issue of when, and how, TIC (as controller) was made aware of the Breach. It was both appropriate and necessary for the Investigator to seek to establish the facts in respect of these issues, as, in the absence of doing so, it would not have been possible for the Investigator to assess whether TIC had complied with Article 33(1).

TIC had the opportunity to make submissions in relation to all matters considered by the Investigator during the course of the Inquiry and, in that regard, made five rounds of submissions, including their Submissions in relation to the Draft Report.

7.119 At paragraph 9.3 of its Submissions in relation to the Preliminary Draft, TIC outlined its view that

“The terms of reference of the inquiry (as per the DPC notice dated 22 January 2019) were limited to Article 33(1) and Article 33(5). The DPC, however, de facto extended the scope of the inquiry to TIC’s compliance with Articles 5(2), 24, 25 and 32. It relies on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32 for the purpose of finding an infringement of Article 33(1).”¹⁶⁷

TIC’s submission, in this regard, is connected with its assertion, addressed above, to the effect that, in considering the controller’s obligation to notify under Article 33(1) in the context of the other obligations on a controller under the GDPR, my provisional finding in relation to Article 33(1) had the effect of implying, into Article 33(1), obligations on a controller arising under other Articles of the GDPR.

For the reasons that I have already set out above, I do not agree that this is the case, nor do I agree that my provisional finding has the effect of ‘de facto’ extending the scope of the Inquiry.

¹⁶⁷ Submissions in relation to the Preliminary Draft, para. 9.3

7.120 As decision-maker for the Commission, I am required to carry out an independent assessment of all materials that have been provided to me by the Investigator and further received by me during the course of the decision-making phase of the Inquiry (to include any submissions made to me by TIC).

In considering the materials provided to me by the Investigator and further received by me from TIC, for the purpose of preparing the Preliminary Draft, I considered the **same issues of fact** relating to TIC's notification of the Breach to the Commission as were considered by the Investigator during the Inquiry, and in respect of which TIC made submissions. In this regard, I considered:

- 1) the facts presented by TIC in relation to the timeline of the Notification, including the events leading up to 3 January 2019 (being the date on which Twitter Inc. assessed the matter as being a reportable data breach);
- 2) the relevant incident management process / procedure between Twitter Inc and TIC, that applied (i.e. the DART Runbook); and
- 3) the issue of how and when TIC (as controller) was made aware of the Breach.

All of these issues were considered by me, during my independent review of all of the materials before me, in the context of assessing the issue of TIC's compliance with its obligations under Article 33(1).

7.121 As set out above, the Investigator's view, as set out in the Final Report, was that it was not possible to establish whether TIC had complied with its obligation under Article 33(1), on the basis that TIC's documentation of the Breach and, in particular, its documentation in respect of the point in time at which TIC became 'aware' of the Breach, did not verify such compliance.

7.122 As also set out above, as decision-maker, I am not bound by the conclusion(s) of the Investigator. In this case, therefore, having independently reviewed and considered the materials provided to me by the Investigator and further materials received by me during the decision-making phase, including all of TIC's submissions, I formed the provisional view in the Preliminary Draft that TIC had not complied with its obligations as a controller under Article 33(1).

As set out above, in forming the provisional view that TIC did not comply with Article 33(1), I considered that the obligation on a controller to notify cannot be viewed in isolation and must be understood in the context of its broader obligations as a controller under the GDPR, including its overarching obligation of accountability under Article 5(2); its obligations under Article 28 in respect of its engagement of a processor; and its obligations in respect of the security of processing of personal data under Article 32.

In this regard, my provisional finding that TIC did not comply with Article 33(1) was made on the basis that, as controller, TIC had overarching responsibility for ensuring that its own processor made it aware of a data breach in a manner that would allow TIC to comply with the notification requirement in Article 33(1).

7.123 TIC submitted that, in my provisional finding that it infringed Article 33(1) on the basis outlined above, I have relied

“...on inferences to the effect that TIC has not complied with its obligations under Articles 5(2), 24, 25 and 32” and have “de facto extended the scope of the inquiry to TIC’s compliance with Articles 5(2), 24, 25 and 32.”

I do not agree that my provisional finding that TIC did not comply with Article 33(1), in circumstances where its own agreed process with its processor for the notification of personal data breaches failed, amounts to extending the scope of the Inquiry to Articles 5(2), 24, 25 and 32. As I clearly outlined in the Preliminary Draft, I consider that, in order to be effective, the obligation under Article 33(1) must be understood *in the context of* the other controller obligations under the GDPR. However, I have not, in any way, considered the substance of matters pertaining to the question of whether or not TIC complied with any or each of these obligations.

Furthermore, I do not agree that my provisional finding that TIC did not comply with Article 33(1) is based upon “inferences” or “adverse findings” in respect of TIC’s compliance with Articles 24, 25, 32 and 5(2). As I have already set out above, it was both necessary, and wholly appropriate, for me to consider the factors and factual matters that led to the delay in TIC being *made aware* of the Breach by its processor and in relation to the timing of TIC’s *awareness* of the Breach relative to when TIC notified the Breach to the Commission.

7.124 My consideration of those factors, and in particular, my consideration of the associated protocol which TIC had in place with its processor, Twitter Inc., was solely in the context of TIC’s compliance with Article 33(1). In this regard, as TIC has referenced in its Submissions, the Preliminary Draft (at paragraph 7.19) clearly outlined that *“a detailed examination of the technical and organizational measures is beyond the scope of the enquiry (sic).”*¹⁶⁸

In accordance with the scope of the Inquiry, it was not necessary, and would have been inappropriate, to consider TIC’s technical and organizational measures (or the efficacy of same) on a broader level for the purpose of assessing its compliance generally with, *inter alia*, Articles 24, 25, 32 and 5(2). No provisional findings were made in the Preliminary Draft, whether expressly or impliedly, in respect of those provisions, and no findings are made in this Decision in respect of those provisions. TIC’s assertion in this regard, therefore, arises from my consideration of the obligation

¹⁶⁸ Paragraph 7.19 of the Preliminary Draft

under Article 33(1) in the context of the broader obligations on a controller under the GDPR as a whole.

7.125 The fact that, in making my provisional finding that TIC did not comply with Article 33(1), I departed from the conclusion reached by the Investigator, does not mean that TIC did not know the case it had to meet or that it was denied a reasonable opportunity to put its side of the case. TIC was afforded fair procedures at all times throughout the currency of the Inquiry and during the decision-making process as is outlined below:

- The scope of the Inquiry, being to assess TIC's compliance with Articles 33(1) and 33(5) in relation to its notification of the Breach, was clearly set out at the outset of the Inquiry.
- Queries were raised by the Investigator during the course of the Inquiry, for the purpose of considering the timeline of the notification and the factors which led to TIC's delayed awareness of the Breach, and TIC was afforded the right to be heard in respect of **all** matters raised. As outlined above, in this regard, TIC made five rounds of submissions during the course of the Inquiry.
- TIC was then afforded a further opportunity, following the commencement of the decision-making process, to make submissions in respect of certain matters that it wished to clarify. TIC did so in its Submissions dated 2 December 2019.
- The **same issues of fact**, as were considered by the Investigator during the Inquiry, were considered by me during the decision making process and for the purpose of making my provisional findings.
- The Preliminary Draft, setting out my provisional findings, was issued to TIC on 14 March 2020 for the purpose of enabling TIC to make any submissions it wished to in respect of the provisional findings. TIC was allowed until the 3 April 2020 to make its submissions, and this period was then extended (on TIC's request) to double the original timeframe for its response until 27 April 2020.
- TIC made comprehensive submissions in respect of the Preliminary Draft. As is reflected above and in the section of this Decision below wherein I set out my decision in respect of the corrective powers to be imposed, I have taken full account of the submissions made by TIC in respect of the Preliminary Draft in making this Decision.

7.126 Having regard to the above, even it were the case, which I do not accept, that the Preliminary Draft addressed matters that had not already been considered during the course of the investigative stage of the Inquiry, or any matters in respect of which TIC had not been afforded the right to be heard during the course of the investigative stage of the Inquiry, TIC had an opportunity to make comprehensive submissions in respect of the full contents of the Preliminary Draft and indeed it

made detailed and extensive submissions in that regard, which I further note were made with the assistance of external legal experts.

I do not, therefore, accept TIC's submission that it was "...deprived of an opportunity to make submissions on the relevant issues."

7.127 Nor do I accept TIC submission, at Paragraph 9.5 of its Submissions in relation to the Preliminary Draft to the effect that

"Even if it was permissible for the DPC to extend the scope of the inquiry without formal notice, TIC has not been afforded a proper opportunity to respond to these provisional findings."

TIC's submission in this regard also appears to be misplaced in circumstances where it is made in the very context of TIC's comprehensive submissions in relation to the Preliminary Draft.

7.128 Having regard to the above, therefore, I do not accept TIC's submission that my provisional finding and, in particular, my interpretation therein of the obligation under Article 33(1) in the context of the GDPR as a whole, de facto extends the scope of the Inquiry.

Nor do I accept TIC's submission that, either during the course of the Inquiry or during the decision-making stage, it has been denied fair procedures.

FINDING - Article 33(1)

7.129 On the basis of the above, I have found that TIC did not comply with its obligations under Article 33(1). I have set out below, in summary form, my reasons for this finding. In doing so, I set out firstly at (i) to (v) below the legal principles underpinning my finding. I then set out at (vi) to (x) the application of those principles having regard to the particular facts of this case:

- (i) Compliance with Article 33(1) requires that a controller must notify a personal data breach within a prescribed timeframe *after having become aware* of the breach. The concept of the controller's 'awareness' under Article 33(1) and, more specifically, the timing of when this takes place, must be viewed in the context of the controller's ability to 'become aware' of the breach. The requirement under Article 33(1) that a controller notify a breach within 72 hours *after having become aware of it*, in other words, 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.
- (ii) This arises from the fact that the obligation to notify, under Article 33(1), is addressed to the controller, and from the fact that, under Article 5(2), the controller has overarching responsibility

for ensuring compliance with the GDPR. It is the controller's responsibility, therefore, having regard to its obligations under the GDPR, to ensure that it becomes aware of a breach in a timely manner so that it can comply with its obligation under Article 33(1).

- (iii) Subject to the further points below, where a controller engages a processor to process personal data on its behalf, and the processor suffers a personal data breach, the controller's *awareness* of the breach (for the purpose of Article 33(1)) will commence when it is notified of the breach by the processor unless it has some other independent method of becoming aware of such a breach outside of notification by the processor. The controller's *awareness* of the breach (and when this takes place) is, therefore, dependent on the efficacy of the process for the notification of breaches which it has agreed with its processor.
- (iv) It is the controller's overall responsibility to oversee the processing operations carried out by its processor and, as part of this, to ensure (by means of an effective process) that its processor makes it aware of any data breach in a manner that will enable it to comply with its obligation to notify under Article 33(1).

In such circumstances, where the process – as agreed with the processor – **is not effective in some respect, fails, or is not followed by the processor**, such that even in a once off or isolated situation, the controller's actual awareness, and notification, of the breach is delayed, the controller cannot seek to excuse its own delayed notification, or complete failure to notify, under Article 33(1) on the basis of the processor's default.

- (v) Where a controller does not ensure that it has an effective process with its processor whereby its processor makes it aware of a personal data breach, and/or where such a process fails/ is not followed correctly by the processor (**as it ought to have been**), and this results in a delay or failure in the processor making the controller aware of the breach, I consider that the controller must, *in these circumstances*, be considered as having constructive awareness of the personal data breach through its processor, such that its obligation to notify under Article 33(1) continues to apply.

I consider that such an interpretation of the concept of 'controller awareness' is necessary in order to ensure that the controller's obligation to notify under Article 33(1) remains effective, and also reflects the responsibility and accountability of the controller in the GDPR scheme.

- (vi) In this particular case, TIC has confirmed that Twitter Inc., its processor, assessed the issue as potentially being a personal data breach on 3 January 2019. I consider that this is the point at which TIC should have been made aware of the issue by its processor. However, for reasons of the ineffectiveness of the process in *the particular circumstances which transpired here* and/or a failure by Twitter Inc. staff to follow its incident management process (which is admitted by TIC), this led to a delay in the DPO being informed of the potential data breach, which resulted in TIC (as controller) not being notified by its processor of the Breach until 7 January 2019.

In this regard, TIC has acknowledged that there was a failure by the Twitter Inc. DART Team (or an engineer on that team), to follow a particular element of the protocol in place with the processor.

- (vii) I have observed that an earlier delay arose during the period from when the incident was first notified by 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*”. For the reasons set out above, I do not accept that this delay was reasonable in the circumstances.
- (viii) TIC has asserted that “*Twitter Inc. informed TIC of the Breach on 7 January 2019 so it was at this point that TIC became “aware” of the breach for the purposes of Article 33(1). As TIC submitted the notification on 8 January 2019, its notification to the DPC was within the required time period...*”
- (ix) Notwithstanding TIC’s actual ‘awareness’ of the breach on 7 January 2019, however, I am of the view that, having regard to the issues set out above, TIC did not comply with its obligations as a controller to notify the Breach within the prescribed timeframe. **I consider that TIC *ought to have been aware of the Breach at an earlier point in time, and in this case, at the latest by 3 January 2019 and that even in the particular circumstances of this situation, any arrangements in place with Twitter, Inc. should have enabled this.*** This is taking into account that 3 January 2019 is the date on which Twitter Inc. first assessed the incident as being a potential data breach and also taking into account the earlier delay in the process up to this point (as set out above at (vii)).
- (x) The alternative application of Article 33(1), and that being 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. Such an approach would be at odds with the overall purpose of the GDPR and the intention of the EU legislator.

8. ISSUE II - ARTICLE 33(5)

- 8.1 As set out above, the second issue, in respect of which I am required to make a determination, relates to whether TIC complied with Article 33(5) in terms of how it documented the Breach. In considering this issue, I have had regard to the requirements of Article 33(5) and the guidance relating to its application, as set out in the Breach Notification Guidelines.

I also carried out a full review and analysis of the documentation furnished by TIC to the Commission during the course of the Inquiry for the purpose of assessing whether TIC had met the requirement in Article 33(5) to document the Breach.

Having done so, my provisional finding, as set out in the Preliminary Draft, was that TIC had not complied with Article 33(5), for the following reasons:

- *On the basis of my assessment of the documentation furnished by TIC during the course of the Inquiry, by which TIC claimed that it 'documented' the Breach, I did not consider that this documentation contained sufficient information so as to enable the question of TIC's compliance with the requirements of Article 33 to be verified.*
- *In particular, I did not consider that the Incident Report - which is identified by TIC as being the primary record in which it documented the facts, effects, and remedial action taken in respect of the Breach - comprised a sufficient record or documenting of the Breach in circumstances where it did not contain all material facts relating to the notification of the Breach to the Commission. In particular, I noted that the report did not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, I noted that the Incident Report did not address how TIC assessed the risk, arising from the Breach, to affected users.*
- *With regard to the other documents furnished by TIC, including the JIRA tickets, whilst I noted that these contained disparate items of limited information relating to the facts of the Breach and its impact on users, I did not consider that (either individually or collectively) they contained sufficient information for the purposes of verifying TIC's compliance with Article 33.*
- *Having reviewed all of the documentation furnished by TIC, I considered that it did not comprise a record or document of, specifically, a 'personal data breach' within the terms of Article 33(5), but rather was documentation of a more generalised nature, including reports and internal communications, that were generated in the context of TIC's management of the incident.*
- *I also considered it to be significant that the deficiency of the documentation furnished by TIC, as a 'record' of the Breach, was demonstrated by the fact that, during the course of the*

Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach. ¹⁶⁹

8.2 In its Submissions in relation to the Preliminary Draft, TIC made a number of submissions concerning my provisional finding that it had not complied with Article 33(5). TIC set out a summary of its submissions in relation to the Preliminary Draft, as follows:

“

- (a) Article 33(5) sets out a closed list of the matters a controller shall document in respect of a personal data breach, namely, the facts relating to the breach, its effects and the remedial action taken. The Breach Notification Guidelines do not extend these categories.*
- (b) The DPC’s May 2018 Guidance, which was relevant at the time that the Underlying Bug was discovered, did not specify a requirement for controllers to demonstrate when and how they became aware of a personal data breach. The recommendation to do so, along with the recommendation to document a risk assessment, was only added in the DPC’s August 2019 Guidance, which was published after the Underlying Bug had already been notified.*
- (c) The DPC is not entitled to interpret Article 33(5) of the GDPR in a way that unilaterally increases the documentation requirement.*
- (d) Neither Article 33(5), nor the Breach Notification Guidelines require controllers to maintain a separate register of data breaches. TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines.*
- (e) TIC met the requirements of Article 33(5) of the GDPR, and in the event that the DPC concludes that it did not, any deficiencies in the documentation created are minor.* ¹⁷⁰

TIC’s submissions above can be broadly separated into two categories, comprising:

- (i) TIC’s submissions regarding the interpretation and application of Article 33(5) (this captures the matters as summarised by TIC set out at (a), (c) and (d) above); and
- (ii) TIC’s submissions to the effect that it complied with the requirements of Article 33(5) in respect of the documentation maintained by it (this captures the matters as summarised by TIC set out above at (b) and (e)).

I have considered and responded to TIC’s submissions on point (i) in this section 8 while I deal with TIC’s submissions in relation to point (ii) in sections 9 and 10. Specifically, section 9 contains an outline

¹⁶⁹ Preliminary Draft, para. 10.30

¹⁷⁰ Submissions in relation to the Preliminary Draft, para. 13

of the documentation furnished by TIC to the Commission during the course of the Inquiry. I have analysed whether this documentation complied with the requirements of Article 33(5) at section 10.

Requirements of Article 33(5)

- 8.3 Before turning to address TIC's submissions concerning the interpretation and application of Article 33(5), it is necessary to briefly consider the terms of this provision. Article 33(5) provides that

*"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*¹⁷¹

As is outlined in the Breach Notification Guidelines, this provision is linked to the accountability principle in Article 5(2) of the GDPR.¹⁷²

- 8.4 The requirement to 'document' under Article 33(5) applies to 'any *personal data breach*'. The documentation requirement is, therefore, specific to incidents that fall within the definition of being a 'personal data breach', within the meaning of Article 4(12), and it applies to 'any' such breach, irrespective of whether it is notifiable or non-notifiable. As the Breach Notification Guidelines outline, this requirement to record non-notifiable as well as notifiable breaches relates to the controller's obligation, under Article 24, to "*be able to demonstrate that processing is performed in accordance with [the GDPR]*".¹⁷³
- 8.5 The precise format in which a controller is required to 'document' a personal data breach is not prescribed by the GDPR. The requirement, as set out in the first statement of Article 33(5), is simply that a controller 'shall document' certain information relating to the personal data breach. In terms of the information that must be documented, this comprises details in respect of three broad categories of information, being the *facts* of the breach, its *effects* and the *remedial action* taken, as indicated by the first sentence in Article 33(5).
- 8.6 The second sentence of Article 33(5), however, explains that the purpose of "*that documentation*" is to enable the supervisory authority to *verify* the controller's compliance with the requirements of "this Article".

¹⁷¹ Article 33(5), GDPR

¹⁷² Breach Notification Guidelines, page 26

¹⁷³ Breach Notification Guidelines, page 26

TIC's submissions regarding the interpretation and application of Article 33(5)

TIC's position that Article 33(5) should not be read as requiring documentation to enable verification with Article 33 as a whole

- 8.7 In the Preliminary Draft, I set out my view that the requirement to 'document' the information, falling under the three broad categories (facts, effects and remedial action), in relation to the personal data breach must be carried out in such a way as to enable a supervisory authority to verify whether there has been compliance with the requirements of Article 33. As will be considered further below, TIC objects to this interpretation whereby Article 33(5) is read as enabling verification of compliance with Article 33 as a whole. (TIC's contentions in this regard related to the summary points at (a) and (c) referred to above in paragraph 8.2). In particular, TIC submitted that there is no basis for maintaining that Article 33(5) obliges a controller to document all matters relating to compliance with Article 33(1), as was the position outlined in the Preliminary Draft. TIC's contentions in this regard were as follows:

*"The DPC argues that the documentation required by Article 33(5) is to enable verification of compliance with Article 33 as a whole and that therefore "the documentation must address all salient facts that relate to the notification of the Breach." This implies obligations into Article 33(5) which are not there and which are not mentioned in the Breach Notification Guidelines."*¹⁷⁴

TIC further submitted, in this regard, that:

*"Article 33(5) prescribes a closed list of items to be documented, namely those "comprising" (i) the facts relating to the personal data protection breach; (ii) its effects, and (iii) the remedial action (and the records kept by TIC address these points). The final sentence of Article 33(5) that refers to "that documentation" cannot be interpreted as increasing the documentation requirement, but must be read as indicating the purpose behind why those three specific items are to be documented. The DPC cannot insert requirements beyond those three items: the use of the word "that" limits the documentation requirement."*¹⁷⁵

- 8.8 I do not accept TIC's submissions on this point in circumstances where Article 33(5) explicitly states that the purpose of documenting the personal data breach by the controller is to *"enable the supervisory authority to verify compliance with this Article."*
- 8.9 As discussed earlier in this Decision, the purpose of Article 33 is to ensure the prompt notification by controllers of personal data breaches to a supervisory authority so that a supervisory authority can assess the circumstances of the breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded.

¹⁷⁴ Submissions in relation to the Preliminary Draft, para 14.10

¹⁷⁵ Ibid, para 14.11

Equally, a supervisory authority must be facilitated to assess a controller's compliance with Article 33 by reference to the controller's documentation of the breach. The categories of documentation specified in Article 33(5), being the *facts relating to the personal data breach*, its *effects* and the *remedial action taken* are deliberately described in broad terms so as to capture all such documentation which would, upon production, facilitate a supervisory authority's verification of the controller's compliance with all of the elements of each paragraph in Article 33.

- 8.10 TIC contended that the wording of Article 33(5) and, in particular, the use of the word "that" in the second sentence has the effect of confining the extent of the documenting which must be done under this obligation to the "closed list" of the three specific items described in Article 33(5).¹⁷⁶ However, I do not agree that these categories of documentation are limited by the terms of Article 33(5), and neither do I agree that they should not be interpreted by reference to the other obligations in paragraphs 1 to 4 of Article 33. In particular, I note that TIC objected to the view expressed in the Preliminary Draft that the obligation in Article 33(5) requires that the documented information must address all salient facts that relate to the notification of the breach. TIC contended that this amounts to implying obligations into Article 33(5) which are not there (and which are not mentioned in the Breach Notification Guidelines – an issue which I deal with separately below)¹⁷⁷. Furthermore, TIC argued that there is no basis for maintaining that Article 33(5) obliges a controller to document all matters relating to compliance with Article 33(1).¹⁷⁸
- 8.11 Contrary to TIC's submissions on these issues, I consider that, as a matter of interpretation, it is clear from the construction of the second sentence in Article 33(5) that the words "this Article" refer to all of the paragraphs of Article 33 as a whole – including Article 33(1). This is because, throughout the text of the GDPR, where specific reference is made to a sub-article or a paragraph of an article, specific phraseology is used to identify that sub-element of the article, for example, the use of the words "paragraph"¹⁷⁹ and "subparagraph"¹⁸⁰. Therefore, if the EU legislators had intended to confine the obligation to document in Article 33(5) so that it was narrowly confined only for the purposes of enabling verification of compliance with just the obligation in the first sentence of Article 33(5), as TIC contended, the words "this Article" would instead read "this paragraph".

Furthermore, if the interpretation of Article 33(5) being proposed by TIC was applied, a controller that delayed in notifying a breach, or that decided not to notify a breach, would not have to document the reasons for its delay or failure to notify and would still comply with Article 33(5), provided that it had recorded the bare facts, effects and remedial action relating to the breach itself. This would, in effect, mean that a supervisory authority would potentially not be able to verify whether the controller's delay

¹⁷⁶ Submissions in relation to the Preliminary Draft, para 14.11

¹⁷⁷ Ibid, para 14.10

¹⁷⁸ Ibid, para 14.11

¹⁷⁹ See for example the use of the word "paragraph" in Articles 5, 6, 8 and 9 amongst others. This word appears 178 times in the text of the GDPR.

¹⁸⁰ See for example the use of the word "subparagraph" in Article 13(1)(f) amongst others. This word appears 12 times in the text of the GDPR.

or failure to notify the breach was justified. Such an outcome is clearly not the intention of Article 33(5), given the overall objective of Article 33.

- 8.12 Connected to the above arguments concerning the scope and extent of the documenting obligation in Article 33(5), TIC also submitted that:

“It is clear....that the Article 29 Working Party did not consider Article 33(5) to require the documentation of all notification decisions and their timing...”

TIC further cited, in support of this contention, that the Breach Notification Guidelines do not specifically identify “*notification*” as being one of the key elements that should be recorded in all cases about a breach; and that the Guidelines use the word “*recommended*” in relation to “*documenting the reasoning behind decisions*.”¹⁸¹

I do not accept TIC’s submission in this regard in circumstances where, as outlined above, Article 33(5) provides that the record of the personal data breach maintained by the controller “*...shall enable the supervisory authority to verify compliance with this Article.*”

- 8.13 The timing of the notification of a breach to the supervisory authority will not always be an issue that a supervisory authority requires to examine or inquire into. However, Article 33(5) provides the basis for enabling a supervisory authority to conduct such an examination or inquiry where it sees fit – for example, where it has doubts as to whether a controller has notified a breach in line with the time requirements in Article 33(1) or whether a breach was notifiable or not. The obligation in Article 33(5), therefore, positions a supervisory authority to be able to assess compliance where it decides that such examination of compliance needs to be undertaken. The only objective means by which a supervisory authority can do this is by examining the controller’s record of the breach.

This is clearly envisaged by the Breach Notification Guidelines, which state that

“In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals.”

Furthermore, and as set out above, the Guidelines state that, where a controller delays in notifying a breach, its record of the breach may assist it in demonstrating that the delay is valid:

“...the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.”¹⁸²

¹⁸¹ Submissions in relation to the Preliminary Draft, para 14.13

¹⁸² Breach Notification Guidelines, page 27

TIC's position on what the "documenting" obligation in relation to Article 33(5) means

- 8.14 This section relates to the points made by TIC as summarised at (d) in paragraph 8.2 above.
- 8.15 The GDPR (and indeed the 2018 Act) does not elaborate as to what is meant by the requirement 'to document' as set out in the first part of Article 33(5).

The ordinary meaning of this term, as set out in dictionary definitions, is 'to record information about something by writing about it...' and 'to record the details of an event, a process etc'.¹⁸³ Applying such an interpretation would mean that where a requirement 'to document' exists, it gives rise to an obligation to actively make and maintain a record of certain information relating to a particular incident or event.

Applying this interpretation in the context of the requirement 'to document' in Article 33(5) would, necessarily, mean that a controller is required to engage in some type of systematic recording of personal data breaches that includes the key components of the specified information (facts, effects and remedial action). Whilst such an approach is not specifically articulated within the GDPR, it is in keeping with the interpretation of Article 33(5) advanced in the Breach Notification Guidelines, which state that

*"Controllers are encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not."*¹⁸⁴

- 8.16 Such an approach to the documenting of personal data breaches is also in keeping with the requirement, under Article 24, that a controller *"shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]."*¹⁸⁵

In this respect, the Breach Notification Guidelines state that

*"The controller may choose to document breaches as part of its record of processing activities which is maintained pursuant to Article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request."*¹⁸⁶
(Emphasis added)

- 8.17 In the Preliminary Draft, I noted that it was of significance that Article 33 has its own requirement 'to document', which is distinct from the general obligation on a controller under the GDPR (under, *inter alia*, the accountability provision at Article 5(2) and also under Articles 30 and 31) to maintain records

¹⁸³ Cambridge Dictionary, online version

¹⁸⁴ Breach Notification Guidelines, page 26

¹⁸⁵ Article 24, GDPR

¹⁸⁶ Breach Notification Guidelines, page 26, footnote 43

in relation to its processing activities, and to provide such records to a supervisory authority upon request.

As I stated, that the EU legislators opted to include a specific obligation ‘to document’ in Article 33, in my view, lends further support to the interpretation of this provision as requiring a targeted approach to the recording of incidents that fall within the definition of being ‘a personal data breach’.

8.18 In the Preliminary Draft, I expressed the provisional view that the distinct nature of the documenting requirement under Article 33(5) is also indicated by the fact that it applies to *any* breaches, whether they are notifiable or not. The obligation applies, therefore, once an incident has been determined as comprising a personal data breach. This means that records that are held out by a controller as comprising ‘documentation’ of a personal data breach may be assessed, based on the time and purpose of their creation, as to whether they amount to the documenting of the ‘breach’, or whether they comprise incident-related documents of a more generalised nature, which, for example, track the occurrence of an identified data or IT security issue.

8.19 However, in its Submissions in relation to the Preliminary Draft, TIC submitted that it did not agree that Article 33(5) requires a separate, or distinct, record or documenting of a personal data breach. In this regard, TIC submitted that

“Whether a general incident response-related document is sufficient to meet the requirements of Article 33(5) is a question of substance, not form. One cannot exclude the possibility that a controller has recorded the relevant information about an incident simply because those records are part of its generalised incident management process. Neither Article 33(5) nor the Breach Notification Guidelines require controllers to maintain a separate register of data breaches.”

TIC further submitted that:

“Article 33(5) does not require a separate record of the personal data breach provided the controller has recorded the required information in some form.”¹⁸⁷

8.20 I do not agree with TIC’s interpretation of the requirement in Article 33(5) and, specifically, its submission that Article 33(5) does not require a separate record of a personal data breach and that recording the information “*in some form*” is sufficient.

As referred to above, neither the Breach Notification Guidelines nor the GDPR impose a specific requirement on a controller to maintain a separate ‘register’ of breaches. However, it is clearly envisaged by both that the record (i.e. the documentation) maintained by a controller pursuant to Article 33(5) should be specific to a ‘personal data breach’ rather than being comprised of more generalised documents that the controller has generated in the context of its general day-to-day

¹⁸⁷ Submissions in relation to the Preliminary Draft, para 14.17

operations, including, for example, records in relation to actual or potential security incidents/breaches. In this context, it is notable that, for example, while not all breaches of security will constitute personal data breaches within the meaning of Article 4(12) GDPR, conversely, all personal data breaches will constitute security breaches¹⁸⁸.

The requirement in Article 33(5) is that a controller ‘document’ a ‘personal data breach’. It is, therefore, a documenting requirement that applies specifically to ‘personal data breaches’ as they are defined under the GDPR. In that regard, it can be distinguished from the other documenting requirements to which controllers are subject under the GDPR, such as those under Article 5(2) and Article 30.

8.21 In its Submissions in relation to the Preliminary Draft, TIC further submitted, on this point, that

“The Breach Notification Guidelines say that controllers are “encouraged to establish an internal register of breaches (p.26) but that “it is up to the controller to determine what method and structure to use when documenting a breach.” When considering whether a controller might keep such information as part of the Article 30 records, the Breach Notification Guidelines say that “a separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.”¹⁸⁹

As TIC pointed out, the Breach Notification Guidelines provide that a controller “*may choose to document breaches as part of its record of processing activities which is maintained pursuant to Article 30.*” The Breach Notification Guidelines go on to outline, in that regard, that “*a separate register is not required*”.

Contrary to what TIC contended, I consider that this reference in the Breach Notification Guidelines to the record of a breach forming part of the controller’s ‘record of processing activities’ clearly envisages that some form of register, or composite record, similar to the ‘record of processing activities’, in respect of personal data breaches should be maintained.

8.22 TIC submitted (at Paragraph 13(d) of its Submissions in relation to the Preliminary Draft) that “***TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines.***” (Emphasis added).

However, as set out below, no such ‘record’ was provided to the Commission during the course of the Inquiry. The documents provided by TIC, as purported to be its ‘record’ of the Breach, comprised a collection of documentation of a more generalised nature, including various reports and internal communications, that were generated in the context of TIC’s management of the bug / incident underlying the Breach.

¹⁸⁸ Breach Notification Guidelines, page 7

¹⁸⁹ Submissions in relation to the Preliminary Draft, para 14.17

- 8.23 In terms of the information that a controller is obliged *to document* under Article 33(5), this falls into three broadly defined categories comprising the *facts relating to the breach*, its *effects* and the *remedial action taken*. As the purpose of documenting is stated to be to enable the supervisory authority to verify compliance with the requirements of Article 33, the information recorded within the required broad categories must meet that standard. In other words, it must be possible, on the basis of the information documented, to verify whether there has been compliance with the requirements under Article 33(1) – 33(4).

In that regard, the Breach Notification Guidelines, in elaborating as to what information a controller should document in order to comply with Article 33(5) has stated that:

“As is required by Article 33(5), the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.”¹⁹⁰

The Breach Notification Guidelines also recommend that:

“...the controller also document its reasoning for the decisions taken in response to a breach.”¹⁹¹

The Guidelines further state that

“Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.”¹⁹²

- 8.24 The above clearly indicates that, whilst the contents of the information that a controller will need to document, in respect of the breach, will depend on the circumstances, in order to be effective as a means of verifying compliance with Article 33, the documented information must address all salient facts that concern the notification of the breach. In this regard, for example, where the notification of the breach is delayed, or the controller decides not to notify, the record maintained by the controller in respect of the breach must address the reasons for the delay and / or the decision not to notify.

As set out above, the role of the documented information as a means to ‘verify’ compliance also indicates a requirement that a controller maintain evidence, in the form of relevant records or documents, as to the steps it took in relation to the breach and, more particularly, in relation to the notification of same to the supervisory authority. In this regard, the Breach Notification Guidelines state that

¹⁹⁰ Breach Notification Guidelines, page 27

¹⁹¹ Ibid, page 27

¹⁹² Ibid, page 27

*"[The controller] will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority."*¹⁹³

- 8.25 Connected to its contention concerning the scope and meaning of the "documenting" requirement, in its Submissions in relation to the Preliminary Draft, TIC also submitted that, at the time of the Breach, it was not aware of the requirement that a controller should, as part of its record of a personal data breach, document how and when it became aware of the breach. TIC also submitted that it was not aware of the requirement that a controller should, as part of its record of a personal data breach, document its assessment of the risk posed by the breach.

TIC's submissions, in this regard, are made on the basis that guidance in relation to breach notifications issued by the Commission in May 2018¹⁹⁴, and which therefore predated the Breach,

"...did not specify a requirement for controllers to demonstrate to the DPC when and how they became aware of a personal data breach. It was also not explicit on controllers' internal breach procedures recording how and when they become aware of personal data breaches. In relation to the recording of risk assessments it stated:

*"Please note even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded."*¹⁹⁵

The guidance to which TIC referred appears to be that published on the Commission website, relating to 'Breach Notification Process Under GDPR' and is referred to hereinafter as the 'May 2018 Commission Guidance'. An updated version of the May 2018 Commission Guidance is now contained on the Commission web site on the 'Breach Notification'¹⁹⁶ page, and comprises a brief guide in relation to notifying the Commission of a personal data breach.

- 8.26 TIC further posited that, in further guidance relating to breach notifications published by the Commission in August 2019¹⁹⁷ ('August 2019 Guidance') and in October 2019¹⁹⁸ ('the October 2019 Guidance'), it is stated that *"controllers should be able to demonstrate to the DPC when and how they became aware of a personal data breach"* and also *"how they assessed the potential risk posed by the*

¹⁹³ Ibid, page 27

¹⁹⁴ 'Breach Notification Process under GDPR', Data Protection Commission website

¹⁹⁵ Submissions in relation to the Preliminary Draft, para 14.5

¹⁹⁶ 'Breach Notification', Data Protection Commission, <https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification>

¹⁹⁷ 'A Quick Guide to GDPR Breach Notifications', Data Protection Commission, August 2019

¹⁹⁸ 'A Practical Guide to Personal Data Breach Notifications under the GDPR', Data Protection Commission, October 2019

breach.”¹⁹⁹ TIC’s complaint, in this regard, was that this “guidance which introduces a recommendation that controllers document risk assessments and when they become aware of personal data breaches was not published until after the report of the Underlying Bug.”²⁰⁰ In addition, TIC contended that:

*“The fact that both sets of guidance include a recommendation that controllers keep records of when they became aware of a data breach and how they assessed the risk suggests that controllers had not generally understood this to be a requirement previously.”*²⁰¹

- 8.27 I do not accept TIC’s submissions that it was not, or could not have been, aware of the requirement to document / record when and how it (as a controller) became aware of a breach or the requirement to document its assessment of risk posed by a breach – simply because these issues were not explicitly addressed by the Commission in the breach notification guidance which it had published (in May 2018) and which, therefore, predated TIC’s notification of the Breach to the Commission.

As set out above, the May 2018 Commission Guidance to which TIC refers was intended to provide a short guide in relation to notifying the Commission of a personal data breach. As is the case with all guidance published by the Commission, it was not intended to be an exhaustive statement of the law, nor was it intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR.

The fact that the May 2018 Commission Guidance did not explicitly reference the requirement that a controller must document how and when it became aware of a breach is irrelevant, as the requirement to do so arises under Article 33(5).

In respect of the requirement that a controller must document its assessment of the risk posed by the breach, the wording of the May 2018 Commission Guidance (contained on the Commission’s web site), in so far as it relates to this requirement, clearly indicates that such documenting should take place irrespective of whether the breach is to be notified or not. In this regard, it states

“...even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.” (Emphasis added)

- 8.28 As set out above, the requirement for a controller to record when and how it became aware of a breach, and to record its assessment of the risk posed by a breach, is clear from Article 33 and, in particular, from the stated purpose of the documentation referred to in Article 33(5) as a means of verifying a controller’s compliance with Article 33.

¹⁹⁹ Submissions in relation to the Preliminary Draft, para 14.7

²⁰⁰ Ibid, para 14.9

²⁰¹ Ibid, para 14.8

Moreover, the controller's obligation to document these matters is encompassed by the required broadly termed categories of information outlined in Article 33(5) of the '*facts relating to the personal data breach*' and '*its effects*'.

In relation to the requirement that a controller document when and how it became aware of the breach, this will clearly form part of the controller's recorded information as to the '*facts relating to the personal data breach*'. In addition, and as set out above, where a breach occurs by a processor, in order for the controller to enable verification by the supervisory authority as to whether the processor complied with the requirement, in Article 33(2), to notify the controller of the personal data breach "*without undue delay*", the information documented by the controller should include details of when and how the processor became aware of the breach and of when the processor notified the controller, thereby making the controller aware of the breach, including reasons for any delay in doing so.

With regard to the requirement that a controller must document its assessment of risk posed by the breach, this will clearly form part of the controller's recorded information as to the '*effects*', or consequences, of the breach. In addition, and as set out above, it is necessary for a controller to *document* its risk assessment in order to enable verification by a supervisory authority of the controller's compliance with the requirement in Article 33(1) that a controller carry out an assessment of the risk posed by a breach to affected data subjects.

The Breach Notification Guidelines support this, stating that, in documenting the breach, the controller must record "*...**details concerning the breach**, which should include **its causes, what took place** and the personal data affected. It should also include **the effects and consequences** of the breach, along with the remedial action taken by the controller.*"

- 8.29 I also do not accept TIC's submission to the effect that the fact that the August 2019 Guidance and October 2019 Guidance issued by the Commission makes specific reference to the requirements for a controller to record when and how it became aware of a breach, and to document its assessment of risk posed by a breach, "*... suggests that controllers had not generally understood this to be a requirement previously.*"

Aside from the fact that this statement is entirely speculative, it does not take account of the fact that the requirements, in terms of what a controller must document, are clear from Article 33(5) which requires controllers to record, *inter alia*, the 'facts' and 'effects' relating to the personal data breach. Furthermore, Article 33(5) states that the purpose of the record which the controller is required to maintain is to enable a supervisory authority to verify the controller's compliance with Article 33. The requirements in terms of what a controller must document, in order to comply with Article 33(5), are, therefore, clear from that provision and from the contents of Articles 33(1) to 33(4).

TIC cannot, therefore, seek to argue that it was ignorant of those requirements on the basis that they were not explicitly stated in the May 2018 Guidance issued by the Commission which was in being at the time of the Breach.

Documentation requirements to enable verification of compliance with Article 33, in accordance with Article 33(5)

- 8.30 I have set out below an outline of what information should be documented by a controller, under Article 33(5), in order to enable a supervisory authority to verify the controller's compliance with Article 33. This is set out by reference to each of the sub-articles of Article 33. The table below, at Paragraph 8.41, then sets out a synopsis of the requirements in this regard, again by reference to each of the sub-articles of Article 33. (It should be noted that this analysis was set out in the Preliminary Draft by way of explanation and precursor to the assessment of the adequacy of the documentation maintained by TIC in the context of the Breach).

Article 33(5) documentation pertaining to verification of compliance with Article 33(1)

- 8.31 Article 33(1) requires a controller to notify a personal data breach *"without undue delay and, where feasible, not later than 72 hours after having become aware of it...unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."* Article 33(1) further requires that *"Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay"*.

As Article 33(1) relates to the notification of a 'personal data breach', a controller or processor, upon becoming aware of an incident or event must assess whether it comprises a breach of 'personal data'. In this regard, the Breach Notification Guidelines state that

*"What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches."*²⁰²

- 8.32 Any assessment of an incident, for the purpose of Article 33(1), must, therefore, include details of whether it involves 'personal data', within the meaning of Article 4(1) of the GDPR and the categories of personal data involved. As set out below, this is also one of the required categories of information to be provided to the supervisory authority under Article 33(3).

The assessment of the incident must also include details of whether, having regard to Article 4(12), it led to one of the events described in the definition of a 'personal data breach' arising – that is, whether it led to the *"...accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data..."*

²⁰² Breach Notification Guidelines, page 7

- 8.33 Article 33(1) also requires that a controller must notify a personal data breach to the supervisory authority, *unless it is unlikely to result in a risk to the rights and freedoms of natural persons*. In this regard, a controller is required to undertake an assessment of the level of risk posed by the breach to affected data subjects. The purpose of this is to ascertain firstly, whether the breach presents a *risk* to affected data subjects, such that notification to the supervisory authority is required. Such assessment must also then consider whether the breach presents a *‘high risk’* to affected data subjects, such that notification to data subjects is required under Article 34.

In this regard, the Breach Notification Guidelines outline that there are two reasons for the risk assessment under Article 33(1), being:

– *“firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned”²⁰³.*

- 8.34 In terms of the factors to be considered when assessing the risk, these are referenced at Recitals 75 and 76 of the GDPR, which state as follows:

“The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage...”²⁰⁴

“The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing...”²⁰⁵

- 8.35 The Breach Notification Guidelines comment that a risk assessment in the context of a personal data breach can be distinguished from an assessment of the risk arising more generally from data processing (and as recorded in a DPIA). In this regard, the Breach Notification Guidelines state that *“...when assessing risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.”²⁰⁶*

The Breach Notification Guidelines go on to recommend the criteria that such a risk assessment should take into account, including the type of breach, the nature, sensitivity and volume of personal data, the ease of identification of individuals and the severity of consequences for individuals.

²⁰³ Breach Notification Guidelines, page 23

²⁰⁴ Recital 75

²⁰⁵ Recital 76

²⁰⁶ Breach Notification Guidelines, page 24

- 8.36 A further requirement of Article 33(1) is that where a controller notifies a breach to the supervisory authority outside of the 72-hour timeframe, the notification must be accompanied by reasons for the delay. This provision recognises that it may not always be possible for a controller to notify a breach within the 72-hour timeframe and that there may be circumstances where a delayed notification may be permissible.

The requirement that a controller provide reasons for the delay is to ensure that any delay in notifying the breach to the supervisory authority is justifiable. In this regard, the Breach Notification Guidelines outline that documentation retained by the controller may assist the controller in demonstrating to a supervisory authority that a delay in notifying a personal data breach was justified.²⁰⁷

- 8.37 Having regard to the above, in order to verify compliance with Article 33(1), a controller will need to record the following information (relating to the ‘facts’ ‘effects’ and ‘remedial action taken’) in respect of the personal data breach:

- Information relating to the controller’s assessment of whether the incident / event comprised a personal data breach within the meaning of Article 4(12). This will include information relating to the personal data breached, including the categories of same and the purposes for which it was processed; and details of the event / incident that occurred and consideration as to whether it led to the *“accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...”*;
- Information relating to or outlining the controller’s assessment of risk posed by the personal data breach, to incorporate its assessment of the level of risk posed and the factors considered in this regard; and
- In the case of a delayed notification, information in relation to the reasons for the delay, including details of the factors that caused the delay, for the purpose of demonstrating that the delay in notifying was justified.

Article 33(5) documentation pertaining to verification of compliance with Article 33(2)

- 8.38 Article 33(2) requires that a processor *“...shall notify the controller without undue delay after becoming aware of a personal data breach.”*

As set out above, Article 33(2) imposes a requirement on a processor, which has been engaged by a controller to carry out processing on the controller’s behalf, to notify the controller *“without undue delay”* of a personal data breach. In this regard, and as set out above, the processor is required to *“assist”* the controller in meeting its obligation under Article 33(1), to notify the breach. However, the

²⁰⁷ Breach Notification Guidelines, page 27 – *“...the controller must be able to provide reasons for [the] delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.”*

responsibility to notify in compliance with Article 33(1), and to ensure that it has sufficient measures in place to facilitate such compliance, remains that of the controller.

In order for the information documented by a controller, under Article 33(5), to enable a supervisory authority to verify that there has been compliance with Article 33(2), it should include details of the processor's notification of the breach to the controller. In order to enable verification by the supervisory authority as to whether the processor complied with the requirement, in Article 33(2), to notify the controller of the personal data breach "*without undue delay*", the information documented should include details of when and how the processor became aware, and of when the processor notified the controller, including reasons for any delay in doing so.

Article 33(5) documentation pertaining to verification of compliance with Article 33(3)

- 8.39 Article 33(3) provides that when a controller notifies a breach to a supervisory authority, the notification must, "*at least*", contain certain information. As set out in Article 33(3), the notification must:

"(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

Article 33(3) relates to the controller's notification of the personal data breach to the supervisory authority and what this should contain. In order for the information documented by the controller, under Article 33(5), to enable the supervisory authority to verify compliance with Article 33(3), the contents of the notification should be reflected in the information documented under the other sub-articles of Article 33. This will include, as set out above, the information which is already required to have been documented in relation to Article 33(1) in relation to: the controller's assessment of the nature of the personal data breached; and the controller's assessment of the risk posed by the breach to affected data subjects, including the measures identified to contain and address the breach.

Article 33(5) documentation pertaining to verification of compliance with Article 33(4)

8.40 Article 33(4) provides that

“Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.”

Article 33(4), therefore, make provision for a controller to provide information on a phased basis in circumstances where it is not possible to provide all of the information, required in Article 33(3), in the initial notification. The Breach Notification Guidelines state that this phased approach to notification,

“...is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on.”²⁰⁸

As set out above in respect of delayed notifications, where a notification is carried out in phases pursuant to Article 33(4), the requirement, or reasons, for adopting this phased approach should be reflected in the documentation maintained by the controller in accordance with Article 33(5). For example, the documentation should reflect the timing of the investigations carried out by the controller and the timing at which further information is received by the controller and then provided to the supervisory authority.

8.41 The table below is for the purpose of summarising the above analysis and outlines, by reference to each of the paragraphs (1) to (4) of Article 33, the information that, as detailed above, should be documented in respect of a personal data breach under Article 33(5) in order that compliance with Article 33 can be verified by a supervisory authority.

²⁰⁸ Breach Notification Guidelines, page 15

Subsection of Article 33	Information to be documented
Section 33(1)	<ul style="list-style-type: none"> • <i>The controller’s assessment of whether there was a personal data breach within the meaning of Article 4(12) to include</i> <ul style="list-style-type: none"> - <i>details of the event / incident that occurred and assessment of whether it led to the ‘accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...’</i> - <i>assessment of the personal data breached, describing the categories and types of personal data and the purposes for which it was processed;</i> • <i>The controller’s assessment of the risk posed by the data breach to data subjects upon discovery of the incident, to incorporate assessment of the level of risk - i.e. whether the incident was unlikely / likely to pose a risk and also whether it was likely to pose a high risk to data subjects. This information is necessary to enable verification of compliance with the notification requirement under Article 33(1) (or indeed under Article 34). The assessment of risk should also consider such factors as nature and volume of personal data; ease of identification of individuals; consequences for data subjects and severity of same; number of affected data subjects.</i> • <i>In the case of a delayed notification, information in relation to the reasons for the delay, to include details of the factors that caused the delay.</i>
Section 33(2)	<ul style="list-style-type: none"> • <i>Information to enable assessment of whether the processor complied with the requirement to notify the breach to the controller. In view of the requirement that the processor notify the controller ‘without undue delay’, this should evidence when the processor became aware and how, and when it notified the controller and any reasons for any delay in doing so.</i>
Section 33(3)	<ul style="list-style-type: none"> • <i>Article 33(3) relates to the required contents of the notification by the controller to the supervisory authority. However, the Commission would expect to see the information set out at Article 33(3)(a), (c) and (d) documented in a record of the personal data breach or, preferably, in a Register of personal data breaches.</i>
Article 33(4)	<ul style="list-style-type: none"> • <i>Information relating to the availability, and timing, of how knowledge and information on the breach evolved – this is necessary to assess whether, for example, if there was phased information provided outside of the 72 hour timeframe, that this phased approach was justified by reference to, for example, the investigations carried out and the timing of same; the timing of further information being received by the controller or processor; and the level of complexity of the breach.</i>

9. ISSUE II – TIC’S DOCUMENTATION IN RELATION TO THE BREACH

- 9.1 Before outlining my findings on the issue of whether TIC complied with its obligation under Article 33(5) to document the Breach, I set out below, in summary form, an outline of the documentation furnished by TIC during the course of the Inquiry.
- 9.2 In advance of doing so, I consider that it is important to note that, in relation to my finding that TIC did not comply with its obligations as a controller under Article 33(1), that finding has been reached on the basis of *all* of the materials provided to me by the Investigator **and** any further materials received by me during the course of the decision-making phase. These materials include the documentation provided by TIC and, in addition, the information and explanations which TIC has provided, during the course of the Inquiry including during the decision-making phase, by way of submissions and responses to this office.

For the purpose of assessing whether TIC complied with its obligations under Article 33(5), however, I am required to consider whether the ‘documentation’ furnished by TIC, and in which it asserts that it ‘documented’ the Breach, meets the requirements of that provision.

Summary of documentation furnished by TIC

- 9.3 The documentation provided by TIC was furnished with its various submissions to this office on the following dates: 25 January 2019, 1 February 2019, 8 February 2019 and 17 June 2019 (Submissions in relation to the Draft Report).

An overview, in terms of the documentation provided by TIC during the course of the Inquiry, is set out below at paragraphs 9.4 to 9.10. This does not exhaustively reference every document provided by TIC but instead deals with the documents by category and by reference to the date on which they were provided to this office.

Documents provided with TIC submissions / response dated 25 January 2019

- 9.4 In the Notice initiating the Inquiry, the Investigator requested TIC to provide

“all information in TIC’s possession which it, pursuant to Article 33(5) GDPR, documented comprising the facts relating to the personal data breach, its effects, and remedial action taken including, but not limited to, meeting agendas, minutes of meetings, email correspondence and risk assessments conducted by TIC or otherwise.”²⁰⁹

- 9.5 In its response, dated 25 January 2019, TIC set out an overview of the incident and it also provided a series of documents in support of same. The principal document provided by TIC on this date was the

²⁰⁹ Notice of Commencement of Inquiry dated 22 January 2019

Incident Report at (i) below. The documents listed at (ii), (iii), (iv), (v) and (vi) below were furnished as exhibits to the Incident Report and, therefore, were considered to form part of that Report.

i. Incident Report

TIC confirmed during the course of the Inquiry that the commencement of the incident management process resulted in the creation of an incident report (the 'Incident Report'). A copy of this document, which is entitled 'IM-3080 SEV1', was provided by TIC with its response dated 25 January 2019. As is set out below, TIC has identified this document as being the primary record in which it has documented the Breach.²¹⁰

ii. Contractor 1's Bug Bounty Report

TIC furnished a copy of Contractor 1's bug bounty report received by Contractor 2 on 26 December 2018 (referenced at 4.7(i) above) and wherein the incident was first identified to Contractor 2.

iii. Twitter Inc. incident response / incident management process documents

TIC confirmed during the course of the Inquiry, as set out above at 4.7(iv), that Twitter Inc.'s legal team was consulted on 3 January and, following this, the incident response plan was initiated. *(I have already noted above that, in its Submissions in relation to the Preliminary Draft, TIC outlined that this consultation with Twitter Inc.'s legal team took place on 2 January. However, it did not change its position that the Twitter Inc. legal team assessed the incident as being likely to be a notifiable personal data breach on 3 January 2019²¹¹).* In this regard, TIC provided (with its letter dated 25 January 2019) copies of two internal procedural documents which relate to Twitter Inc.'s incident management process - the '*Data Breach Investigation through Vulnerability Disclosure*' Runbook ('the DART Runbook') and the '*Security Incident Management Workflow*'. These are standard incident response documents and do not relate specifically to the Breach, although TIC confirmed, in its letter dated 25 January 2019, that these reflect the processes that were adopted following the review of the incident by Twitter Inc.'s legal team.

iv. Incident creation (JIRA) ticket

The commencement of the incident management process led to the generation of an Incident Creation Ticket. A copy of this ticket was provided by TIC with its letter dated 25 January 2019.

v. Documents relating to remediation of the issue

With its response dated 25 January 2019, TIC also provided copies of various documents relating to the technical measures taken to rectify the bug which gave rise to the Breach. These include a document relating to the 'patch' applied (entitled '*Fix hardcoded*

²¹⁰ Submissions in relation to the Draft Report

²¹¹ Submissions in relation to the Preliminary Draft, para 6.4

protectedUser params for settings updates’) and a number of JIRA tickets which relate to the application of the fix.

- vi. Document containing EU and EEA numbers of affected users

TIC provided a document comprising a country-by-country list of affected EU / EEA users.

Documents provided with TIC submissions / response dated 1 February 2019

- 9.6 In addition to the request made in the initial Notice, a follow up request was made by the Investigator, in the letter to TIC dated 29 January 2019, to be provided with “...the record of the data breach made pursuant to Article 33(5) GDPR”.²¹² (Emphasis added)

The Investigator also, in that correspondence, again requested that TIC would provide “*relevant supporting documentary evidence of any risk assessments conducted by TIC regarding the risk to the rights and freedoms of natural persons in respect of the Data Breach.*”²¹³ (Emphasis added)

- 9.7 In its response, dated 1 February 2019, TIC made the following submission in relation to the request that it provide a record of the data breach:

*“Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This (and other information) is recorded by Twitter Inc. at the direction and request of TIC, in its incident management reports (copies of which have already been provided), which are centrally stored in Google Drive, which are shared with TIC.”*²¹⁴

In respect of the request that it provide documentary evidence of any risk assessment carried out for the purpose of the Breach, TIC did not provide any documentation in this regard but outlined as follows:

*“TIC and Twitter Inc take the safety and security of the people that use our services very seriously. Thus, while TIC believes that people who were impacted by this issue would have immediately realised that their account had been unprotected by virtue of the disappearance of the “lock” from their account profile (as discussed in detail in our 25 January 2019 letter) and thus, would have been able to immediately reprotect their account should they have chosen. TIC decided to provide notice to impacted persons upon becoming aware of the issue.”*²¹⁵

- 9.8 In terms of the documentation furnished by TIC with its response of 1 February 2019, an outline of this is set out below:

²¹² Letter from DPC to TIC dated 29 January 2019, Appendix, Query 9

²¹³ Ibid, Query 11

²¹⁴ Submissions dated 1 February 2019, Annex, point 9

²¹⁵ Ibid, Annex, point 11

i. The JIRA Ticket – Contractor 2 to Twitter Inc.

TIC confirmed that once Contractor 2 had “triaged” the report from Contractor 1, it issued notification of same to Twitter Inc. in the form of a JIRA ticket, a copy of which was included by TIC in its submissions dated 1 February 2019.

This document is dated between 26 December 2018 and 29 December 2018 and, therefore, pre-dates the point at which the incident was assessed by Twitter Inc.’s legal team as comprising a personal data breach (which, as noted above, occurred on 3 January 2019).

In its submissions dated 25 January 2019 to the Commission, TIC had referred to this document but had not provided a copy of same on the basis that it “*contains privileged and confidential advice of counsel...*”²¹⁶ The version of this document provided with its response dated 1 February 2019, therefore, includes a redacted portion. TIC confirmed, in later submissions to this office, that the information redacted relates to “*...the exchange which took place on 3 January between Twitter Inc.’s Information Security and legal teams.*”²¹⁷

In terms of the remainder of this document, this sets out various exchanges between Contractor 2 and Twitter Inc. concerning the incident and arising from Contractor 2’s assessment of same. It also contains a number of comments exchanged between Twitter Inc.’s IT security personnel (dated 2 January 2019) relating to the severity of the incident and noting, in particular, that while it comprised a low security risk, “*the privacy implications are pretty nasty*”.

ii. Investigation and Incident Management (JIRA) tickets

TIC also provided, with its submissions dated 1 February 2019, a copy of the Incident Management (IM) ticket and a copy of the Investigation ticket. These documents were provided by TIC in response to queries raised by the Investigator concerning whether the process as outlined in the DART Runbook - which identified that the correct step at that point in time in the incident management process was to add the DPO (in addition to other personnel) as a ‘watcher’ to the incident management ticket – had been followed (as referenced above also).

TIC also provided a list of ‘watchers’ in respect of the Investigation and IM Tickets. These documents, which take the form of two lists of various personnel, were provided by TIC in response to a request by the Investigator to be provided with “*...a list of the individuals that were added as watchers to both the Investigation Ticket and the IM ticket.*”²¹⁸

²¹⁶ Submissions dated 25 January 2019, Annex, footnote 4

²¹⁷ Submissions in relation to the Draft Report, para 4.5.3

²¹⁸ Letter from DPC to TIC dated 29 January 2019, Appendix, Query 2(ii)

iii. Calendar invites

The balance of the documentation provided by TIC with its response dated 1 February 2019 comprised a series of calendar invites, relating to the involvement of the DPO in the incident management process from the 7 January 2019, that being the date on which the DPO was notified of the Breach.

Documents provided with TIC's submissions / response dated 8 February 2019

9.9 Arising from further queries raised by the Investigator, regarding the notification by Twitter Inc. to TIC of the Breach on 7 January 2019, and in particular, seeking documentary evidence of same, TIC provided a limited volume of additional documentation in its response dated 8 February 2019. This comprised the following:

i. Calendar invite dated 7 January 2019 (3:30pm - 4pm)

A further copy of this document, which had already been provided on 1 February 2019, was provided by TIC by way of documentary evidence as to the time of notification of the Breach by Twitter Inc. to the DPO (and, therefore, TIC).

ii. Updated DART Runbook

TIC also furnished a copy of an updated version of the DART Runbook, which it stated (in its response) *"has been updated based on our learnings from the incidents the company has reported since 25 May 2018."*²¹⁹ This DART Runbook is, therefore, a different version of the document which TIC had furnished with its submissions / response dated 25 January 2019.

Documents provided with TIC submissions dated 17 June 2019

9.10 The final document provided by TIC accompanied its Submissions in relation to the Draft Report. It comprises a copy of an internal ('Slack'²²⁰) message, dated 7 January 2019 at 11:23 am between the DPO and Twitter Inc., and wherein the DPO requests to be added to the *"IM-3080 materials"*.

This document was provided by TIC by way of further documentary evidence as to the point in time at which the DPO (and, therefore TIC) was notified of the Breach by Twitter Inc.

²¹⁹ Submissions dated 8 February 2019, Annex, point 2(i)

²²⁰ 'Slack' is an instant messaging / chatroom facility designed to replace email. It is described as *"a collaboration hub that can replace email to help you and your team work together seamlessly...so you can collaborate with people online as efficiently as you do face-to-face"* <https://slack.com/help/articles/115004071768-What-is-Slack->.

10. ISSUE II - ANALYSIS OF DOCUMENTATION FURNISHED BY TIC FOR THE PURPOSES OF ASSESSING COMPLIANCE WITH ARTICLE 33(5)

- 10.1 I now turn to consider whether, having regard to the documentation provided, TIC complied with its obligations as a controller under Article 33(5).
- 10.2 In considering whether TIC complied with Article 33(5), I have assessed whether the documentation provided by TIC during the course of the Inquiry, and in which it has asserted that it recorded the Breach, meets the requirements of Article 33(5), particularly in terms of whether it enabled the Commission to verify TIC's compliance with Article 33.

In this regard, TIC made specific submissions, in relation to the Draft Report, in which it set out how it considers that certain documentation which it furnished to the Commission in the context of the Inquiry met the requirements of Article 33(5).

- 10.3 Additionally, in its Submissions in relation to the Preliminary Draft, TIC made further submissions in relation to the documentation which it had furnished during the course of the Inquiry. I have addressed TIC's submissions in that regard at the relevant paragraphs below. Having considered those sets of submissions, together with all of the documentation which TIC furnished during the course of the Inquiry, I have set out below my analysis of the documentation in question in which TIC has asserted it recorded the Breach with regard to whether it meets the requirements of Article 33(5), and particularly in terms of whether it enabled the Commission to verify TIC's compliance with Article 33.

There are two aspects to my analysis in this regard – firstly, I have considered the contents of the documents furnished by TIC with a view to assessing whether they **record** the information required by Article 33(5), in terms of the facts, effects and remedial action taken, in respect of the Breach, as specifically referenced in Article 33(5). Secondly, and in so doing, I have also considered whether the documents meet the requirement, set out in the second sentence of Article 33(5), of enabling a supervisory authority to **verify** compliance with Article 33.

- 10.4 As referred to above, the requirement in Article 33(5) is that a controller shall “*document*” a “*personal data breach*.” Whilst the GDPR does not prescribe the format in which a controller must do this, the Breach Notification Guidelines provide that controllers are “*encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not.*”²²¹

Such an approach to the documenting of personal data breaches is also in keeping with the requirement, under Article 24, that a controller “*shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]*”.

²²¹ Breach Notification Guidelines, page 26

In this respect, the Breach Notification Guidelines state that

“The controller may choose to document breaches as part of its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.”²²²

- 10.5 As I have set out above, the obligation ‘to document’ in Article 33(5) is specific to personal data breaches and it can, therefore, be distinguished from the general obligation on controllers, under, *inter alia*, Article 5(2) and Article 30 and 31, of the GDPR to maintain records in relation to their processing activities and to furnish such records to a supervisory authority upon request.

Furthermore, the controller must ensure that the information documented by it, in respect of a personal data breach, is sufficient so as to enable its compliance with Article 33 to be verified.

- 10.6 As set out above, in its Submissions dated 1 February 2019, in response to the Investigator’s request that it provide “...*the record of the data breach made pursuant to Article 33(5) GDPR*”,²²³ TIC outlined as follows:

“Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This (and other information) is recorded by Twitter Inc. at the direction and request of TIC, in its incident management reports (copies of which have already been provided), which are centrally stored in Google Drive, which are shared with TIC.”²²⁴ (Emphasis added)

In its Submissions in relation to the Draft Report, TIC reiterated the above explanation, as to how it documents data breaches. In this regard, TIC stated as follows:

“TIC explained to the DPC in its response of 1 February how it documents breaches...”

TIC then outlined its view “*in more detail how the incident management report and JIRA ticketing system meet the requirements of Article 33(5).*”²²⁵ (Emphasis added)

The ‘incident management report’ referred to in the extract above from TIC’s submissions is the Incident Report (referenced above at 9.5 (i) and provided by TIC with its Submissions dated 25 January 2019. TIC has, in this regard, identified this report as essentially comprising the primary record of where it ‘documented’ the facts, effects and remedial action in relation to the Breach. Similarly, in its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of how it considers the Incident Report meets the requirements of Article 33(5). I have, therefore, firstly set out

²²² Ibid, 26, footnote 43

²²³ Letter from DPC to TIC dated 29 January 2019, Appendix, Query 9

²²⁴ Submissions dated 1 February 2019, Annex, point 9

²²⁵ Submissions in relation to the Draft Report, para 5.8

my analysis of this specific document below having also considered TIC's various submissions on this document.

Analysis of the Incident Report for the purposes of assessing compliance with Article 33(5)

- 10.7 The Incident Report (entitled IM-3080) was provided by TIC with its response to this office dated 25 January 2019. In terms of its contents, this document outlines, in an introductory section, that

"A Whitehat reporter...identified a bug in the Twitter Android client whereby users can unknowingly disable the 'protect my account' setting when adding a new email to their account using Android Mobile App."

The document then sets out certain information under the following headings –

- 'Contacts and Roles', wherein it sets out a list of (staff) points of contact and their roles;
- 'Current Status', wherein it contains a number of statements in relation to the status of the incident management process with the most recent stating *"Incident resolved, post mortem to be schedule"*;
- 'Event Details', wherein it outlines, by reference to code examples, the 'Android Client Flaws';
- 'Action Summary', wherein it sets out actions *"being taken to mitigate, contain, and react to the discovery of this problem"*, being *"Android client fix complete"* and *"Macaw-users mitigation complete"*;
- 'Open Items', wherein it sets out an exchange of internal messaging / communications between relevant staff members in relation to certain actions taken in respect of the incident.

The document also contains a Timeline in which, by reference to dates and times, it sets out certain steps taken in respect of the incident from 26 December 2018 to 16 January 2019.

- 10.8 In the Preliminary Draft, I noted, by way of general comment, that the 'Action Summary' and 'Timeline' sections of the Incident Report make specific reference to 'exhibits' that were included with TIC's correspondence to this office of 25 January 2019. I outlined, in this regard, that it was not clear whether those portions of the Report were created for the purpose of that correspondence or whether they formed part of the original Incident Report.

In its Submissions in relation to the Preliminary Draft, TIC clarified that the Incident Report (as created) included a number of attachments, including the JIRA ticket whereby the bug was notified by Contractor 2 to Twitter Inc., as hyperlinks. TIC submitted, in this regard, that *"As these hyperlinks were not available to the DPC, TIC included the documents as exhibits when sharing the Incident Report with the DPC."*²²⁶ On that basis, I have considered those documents referred to as 'exhibits' as forming part

²²⁶ Submissions in relation to the Preliminary Draft, para. 15.1 in first row of table therein under 'Additional Comment'

of the Incident Report itself. However, as set out above, I have also considered these documents individually in terms of their compliance with the requirements of Article 33(5).

The documents that were exhibited as part of the Incident Report comprise the following:

- Exhibit A – The original bug bounty report from Contractor 1 wherein the incident / bug was first disclosed on 26 December 2018 (as referenced above at Paragraph 9.5(ii));
- Exhibit E – Copy of JIRA ‘Incident Creation’ ticket (as referenced above at Paragraph 9.5(iv));
- Exhibit G – Copy of JIRA ticket entitled ‘Copy of fix for code review’ and relating to the application of a fix to the bug (as referenced above at Paragraph 9.5(v));
- Exhibit H – Copy of JIRA ticket for partial server side fix (as referenced above at Paragraph 9.5(v));
- Exhibit I – Copy of JIRA ticket for validation that issue is resolved in client side fix (as referenced above at Paragraph 9.5(v));
- Exhibit J – Copy of JIRA ticket for localisation team preparation of user notice;
- Exhibit K – Copy of document containing EU/EEA country-by-country breakout of impacted users ((as referenced above at Paragraph 9.5(vi));
- Exhibit L – Copy of JIRA ticket to identify user accounts that will be re-protected alongside issuance of user notice ((as referenced above at Paragraph 9.5(v));
- Exhibit M – Copy of JIRA ticket for start of work to re-protect accounts (as referenced above at Paragraph 9.5(v));
- Exhibit N – Copy of JIRA ticket affirming that Android client fix is complete (as referenced above at Paragraph 9.5(v));
- Exhibit O – Copy of JIRA ticket affirming server side work and fix (as referenced above at Paragraph 9.5(v)).

10.9 TIC has asserted that the Incident Report meets the requirements of Article 33(5) on the basis of TIC’s view that it documents the *facts* relating to the Breach (in the introductory and Event Details section); the *effects* of the Breach (in the introductory section and Timeline sections); and the *remedial action* taken (in the Timeline and Action Summary sections). In this regard, TIC has stated as follows:

“Facts relating to the breach

The introductory text at the start of IM-3080 outlines the way the breach came to light i.e. via a “Whitehat reporter” and the original report is attached as an exhibit. The “Event Details” section of the IM report details the changes which introduced the Android client flaws, citing the relevant change-IDs, with their dates and authors.

Effects of the breach

The introductory text explains the potential effect: “users can unknowingly [sic.] disable the “protect my account” setting when adding a new email to their account using Android Mobile App.”

Further detail of actual impact is given in the Timeline section (“Jan 7 7.53pm [Name] upgraded to SEV1 after reviewing the potential impact numbers (approx. 500k for 6 mos of logs)” Further detail on this can also be seen in the discussions in the section headed “open items”.

Remedial action taken

The detailed timeline sets out the actions taken to resolve the breach with dates and times. There is also an action summary of the actions being taken to mitigate, contain and react to the discovery of the problem (for example “Android client fix complete”). Exhibits to the IM report provide more details of these actions.”²²⁷

- 10.10 Having considered the contents of the Incident Report, and the various exhibits that were attached with the Incident Report, together with the submissions made by TIC in relation to its content, I consider that, while it does set out, in very basic terms, the facts relating to the incident or bug that led to the Breach, its impact upon users and the remedial action taken, it is deficient in a number of important respects from the point of view of enabling TIC’s compliance with Article 33 to be verified. My conclusions in this regard have been reached by reference to the requirements arising from each of the sub-articles of Article 33, which have already been considered above at paragraphs 8.31 – 8.40 and the table at paragraph 8.41.
- 10.11 Firstly, in respect of the obligations arising under Article 33(1), the Incident Report (and / or the exhibits attached thereto) does not contain any information relating to TIC (or Twitter Inc.’s) assessment of the incident / bug as a ‘personal data breach’ within the meaning of Article 4(12). In that regard, whilst the Incident Report contains one reference, in an entry in the Timeline section, that the incident “...*could likely be a reportable breach*”, the report does not contain any details of the personal data breached or the categories, or nature, of such personal data.

Furthermore, whilst the Incident Report refers to the nature of the incident as follows “...*users can unknowingly disable the ‘protect my account’ setting when adding new email to their account using Android Mobile App*”, there is no information relating to the assessment of how this event led to one of the vulnerabilities described in the definition of a personal data breach at Article 4(12) – i.e. “...*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...*” In other words, the Incident Report does not make any reference to how the bug was assessed as satisfying the criteria for being a personal data breach within the meaning of that term under the GDPR.

In its Submissions in relation to the Preliminary Draft, TIC objected to the provisional findings which I made to the above effect in the Preliminary Draft.

²²⁷ Submissions in relation to the Draft Report dated 17 June 2019, Paras 5.9.1 – 5.9.3

- 10.12 Firstly, TIC submitted that it did not accept my view that the Incident Report was deficient in not including any details of the personal data breached, or the categories or nature of such personal data.²²⁸ In this regard, TIC submitted that

“The original JIRA ticket forms a part of the Incident Report. The “impact” section of the details of the JIRA ticket says “this can lead to a user’s private tweets being exposed to the public...” The details of the personal data potentially breached, and the categories or nature of the data are inherent within the word “tweet”.”

TIC then goes on to explain in its submission that

“A tweet is a free text field. By its very nature it may potentially contain any type of data, depending on how the user uses their account. If only one account were exposed, it might be worthwhile carrying out a specific review to determine, for example, whether the account belonged to a business or a private individual, or what type of tweets the account contained, as one might then determine the breach was unlikely to result in a risk. With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data. Therefore the Incident Report was not deficient in not providing further details of the personal data affected by the Underlying Bug.”²²⁹

- 10.13 I do not accept TIC’s submission set out above. I accept that, by its nature, a ‘tweet’ could potentially contain any kind of personal data and that the word ‘tweet’ is commonly understood in this way. TIC’s submission does not take account of the fact that a controller is obliged, under Article 33(1), to carry out an assessment of the risk posed by a breach and to document that assessment. Any assessment of risk must, by necessity, be conducted by reference to the categories of personal data breached.

In the case of a breach such as that in the instant case, and as TIC has alluded to in its above submission, such an assessment of risk might include, for example, an analysis of the type of user accounts breached, with a view to ascertaining whether they belonged to business or private individuals. This would, in turn, determine what level of personal data and special category data was likely to have been involved.

- 10.14 No such assessment appears to have been conducted in this case as reflected in the Incident Report and in the original JIRA ticket attached thereto. This is borne out by TIC’s comment in the above extract that *“With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data.”* (Emphasis added) Even if one accepts TIC’s submission in this respect that, in view of the volume of potentially exposed accounts and the likelihood that all categories of personal data were involved, some form of analysis in respect of the personal data involved was not necessary (or was futile), the Incident Report (or the exhibits attached) does not make

²²⁸ Submissions in relation to the Preliminary Draft, para 16.3

²²⁹ Ibid, para 16.3

any reference to this. In any event, I do not accept this contention and I do not consider that the fact that the data involved “tweets” - no matter how self-evident TIC may consider the nature of same to be – was sufficient in terms of containing any details of the personal data breached or the categories, or nature, of such personal data.

- 10.15 In its Submissions in relation to the Preliminary Draft, TIC further submitted that, in circumstances where the Investigator did not specifically raise queries about the type of data impacted by the Breach, or the categories and nature of such personal data, during the course of the Inquiry, this “...demonstrates that the information [TIC] recorded and provided was not deficient in this area.”²³⁰ I do not accept TIC’s submission in this regard for the reasons which I set out below.
- 10.16 Firstly, it is the case that, by the time the Inquiry had commenced, TIC had already provided information to the Commission, in the Breach Notification Form and Updated Breach Notification Form, regarding the nature of the Breach, the number of data subjects impacted and the severity of impact. Given the circumstances which led to the commencement of the Inquiry – being the apparent delay in TIC’s notification of the Breach - the primary focus of the Investigator’s queries during the course of the Inquiry related to the timeline for the notification and, in particular, the reason for the delay in TIC becoming aware of the Breach.

Secondly, the Investigator raised queries, on a far broader level, in respect of the format and / or quality of TIC’s documentation of the Breach under Article 33(5). In this regard, the Investigator made two separate requests to be provided with TIC’s ‘record’ of the Breach and the documentary evidence in respect of the risk assessment which it had carried out in respect of the Breach. This request was first made in the Notice (commencing the Inquiry) and, having not received these items from TIC in its first response to the Commission, the Investigator then repeated the request in correspondence dated 29 January 2019. As already set out above, in its response, dated 1 February 2019, TIC confirmed that its ‘record’ of the Breach was contained within the “*incident management reports (copies of which have already been provided)*...”²³¹ TIC did not provide any documentary evidence of a risk assessment.

As I have outlined above, it is the controller’s ‘record’ of the Breach and / or its documented risk assessment in relation to the Breach that would usually contain details of the categories and nature of the personal data affected. TIC did not provide either of these.

The fact that the Investigator did not raise specific queries about the nature or categories of personal data impacted certainly does not demonstrate that TIC’s documenting of the Breach in the Incident Report (or in the other documentation furnished) was sufficient in so far as it addressed these issues. Furthermore, I as decision-maker, having carried out a full and independent review of the materials furnished by TIC, have determined that the documents retained by TIC as the ‘record’ of the Breach were deficient in relation to these matters.

²³⁰ Submissions in relation to the Preliminary Draft, para 16.5

²³¹ Submissions dated 1 February 2019, Annex, point 9

- 10.17 TIC also submitted (in its Submissions in relation to the Preliminary Draft) that it did not accept my view (again set out at paragraph 10.11 above and which was expressed on a provisional basis in the Preliminary Draft) that the Incident Report was deficient, as a ‘record’ of the Breach, in circumstances where it did not contain any information relating to the assessment of how the event led to one of the vulnerabilities described in the definition of a personal data breach, that, is “...accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.”

In this regard, TIC submitted that

“Given the level of knowledge, experience and expertise of the individuals involved in incident management at Twitter, there would have been no formal assessment process necessary in this instance. The nature of the risk would have been immediately obvious to them from the statement in the initial bug report “this can lead to a user’s private tweets being exposed to the public.”²³²

As I set out above, the requirement that a controller document whether an incident gives rise to one of the vulnerabilities listed in Article 4(12) is simply a requirement that a controller confirm whether, having assessed the incident, it satisfies the criteria for being a personal data breach (as defined under the GDPR). The fact of the level of knowledge / experience / expertise amongst those individuals assessing such an incident is irrelevant, because what is required here is that a record is made for the purpose of facilitating any later review / examination by a supervisory authority of the matter in question. It does not matter that it may have apparently been obvious to any such individuals that the matter was high risk, or even that they considered that it met the criteria of a data breach. Rather, the core issue was whether such an assessment was committed to writing / documented so that it could be later consulted by a supervisory authority. Further, while, as TIC submitted, the Incident Report sets out the Information Security team’s assessment of the potential impact of the bug, it does not contain any data-protection specific assessment of whether the bug was a personal data breach within the meaning of that term under the GDPR. (As I set out in further detail below, this is indicative of the fact that the Incident Report was not specifically a record of a ‘personal data breach.’)

- 10.18 In its Submissions in relation to the Preliminary Draft, TIC made further submissions in respect of the view I set out at paragraph 10.11 above - and which was also expressed in provisional terms in the Preliminary Draft - that the Incident Report did not set out any assessment of the incident/bug as a ‘personal data breach’. In this regard, TIC submitted that

“TIC’s understanding of its obligations under Article 33(5) at the time it reported the Underlying Breach was that it was not necessary to record a risk assessment where a personal data breach was reported to the relevant supervisory authority. This interpretation was consistent with both the available guidance quoted above and the stated purpose of the documentation.”²³³

²³² Submissions in relation to the Preliminary Draft, para. 16.6

²³³ Submissions in relation to the Preliminary Draft, para 14.15

- 10.19 I have already outlined above, at section 8, that I do not accept TIC's submission to the effect that it could not have known, at the time of the Breach, that it was required to document an assessment of the risk posed by the Breach. In summary, and as set out in those paragraphs, this requirement is clear from the wording of Article 33(5) and from the obligation therein to document the 'effects' of the breach. In addition, given that the stated purpose of the record referred to in Article 33(5) is that it is a means of verifying the controller's compliance with Article 33, a controller must document its assessment of the risk presented by a breach in order to demonstrate its compliance with the requirement, under Article 33(1), to carry out such an assessment.

Furthermore, and as I set out above at section 8, the requirement to document the assessment of risk in all circumstances, irrespective of whether the breach is to be notified to the supervisory authority or not, is clearly contemplated by the wording of the Commission's guidance that was published at the time of the Breach and which states:

"...even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded."²³⁴ (Emphasis added)

- 10.20 I also consider the Incident Report to be deficient in terms of verifying TIC's compliance with its obligation as controller (under Article 33(1)) and the obligation on Twitter Inc. as processor (under Article 33(2)) to notify the Breach.

In this regard, the Incident Report contains no reference to, or explanation of, the issues that led to the delay in TIC, as controller, being notified of the Breach. Whilst the Timeline section of the document contains an entry relating to 7 January 2019, there is no reference to this being the date on which notification of the DPO (and, therefore TIC) of the Breach took place.

- 10.21 Whilst there is no explicit requirement in Article 33(5) that a controller must 'document' the details relating to a delayed notification, the requirement 'to document' in Article 33(5) is stated to be for the purpose of enabling verification of a controller's compliance with Article 33. This will necessarily include, as set out above at section 8, verification of compliance with the express requirement in Article 33(1) that, where notification to the supervisory authority is delayed, the controller must provide reasons for the delay.

It therefore follows that any documentation by a controller of a personal data breach where notification has been delayed should make reference to this fact and to any factors leading to the delay. This information should, logically, form part of the controller's documentation of the 'facts relating to the personal data breach'. It should also form part of the controller's record or assessment of the 'effects' of the breach in view of the fact that a delay in notification may impact negatively on the affected data subjects.

²³⁴ May 2018 Commission Guidance

10.22 In its Submissions in relation to the Preliminary Draft, TIC outlined that

*"[it] does not agree that Article 33(5) requires reasoning relating to the notification process to be documented, unless a decision not to notify is made."*²³⁵

TIC's submission, in this respect, is made on the basis that "[the] notification process is distinct from the personal data breach, so information about it does not form part of the facts about the breach."²³⁶

I do not accept TIC's assertion in this respect. To the contrary, I consider that the notification process and the facts of the breach are intrinsically connected, such that information relating to the circumstances of notification (or failure to notify) will inevitably overlap with the facts of the breach.

As I have noted above, the three categories of information to be documented under Article 33(5) are broadly defined and there is no limitation in place on what they are required to capture. The facts of the breach will, therefore, as a matter of logic, encapsulate **all** of the circumstances of the breach, including how it occurred, how it came to light and how it was dealt with. Further, and as I have already set out above, in circumstances where the stated purpose of the record under Article 33(5) is to enable the controller's compliance with Article 33 (in all of its parts) to be verified, the recorded information relating to the breach must verify compliance with Articles 33(1) and 33(2).

In particular, where a controller delays in making a breach notification, the supervisory authority must be able to verify, by reference to the controller's documentation or record of the breach, whether or not the delay was justified having regard to the nature of the notification obligations in Article 33(1).

10.23 I note, in this regard, that TIC acknowledged in its Submissions in relation to the Preliminary Draft that, in this case, the Incident Report did not meet the requirement of verifying when TIC became aware of the Breach in circumstances where *"the engineer failed to follow the process correctly. However, its processes were designed to meet this requirement, so this was not a systemic failure, and in all other aspects the documentation is sufficient."*²³⁷

The issue of the process, as agreed between TIC and Twitter Inc., for the notification of breaches has already been addressed above in the context of Article 33(1).

TIC has accepted that the Incident Report does not verify when the TIC DPO was made aware of the Breach. However, and, perhaps more fundamentally, the Incident Report does not provide any information as to *how* the delay in TIC becoming aware of the Breach arose – that is, a failure by Twitter Inc. to follow the agreed protocol with TIC regarding the notification of personal data breaches. In this regard, I consider that the Incident Report is deficient as a record of TIC's compliance with Articles 33(1) and 33(2).

²³⁵ Submissions in relation to the Preliminary Draft, para. 16.10

²³⁶ Ibid

²³⁷ Ibid

10.24 TIC submitted, in this respect, that

“...[the] Incident Report is a contemporaneous record of events. It is clear from the documentation when Twitter Inc. became aware of the Underlying Bug. TIC has informed the DPC when it was notified by its processor. This makes it evident that there was a delay in informing TIC. As TIC has explained, the delay in notification to TIC arose from a failure to add the TIC DPO as a watcher on the Incident Report...It is difficult to see what additional information TIC could have included in the documentation which would have enabled the DPC to verify that an engineer had made a mistake.”²³⁸

TIC’s submission, in this regard, is again made on the basis that the controller’s ‘record’ of the breach does not have to include information relating to a delay in notification, such that it would enable a supervisory authority to verify the controller’s compliance with Articles 33(1) and 33(2). As I have already set out above, I do not accept TIC’s submission in this regard.

The requirement in Article 33(5) is that a controller must ‘document’ a breach and that this documentation “*shall enable the supervisory authority to verify compliance*” with Article 33. The record(s) maintained must, therefore, include all of the salient facts in relation to the breach so as to verify compliance with the requirements under Articles 33(1) to 33(4). This will include information relating to the circumstances of a controller’s delay in notifying a breach (including any reasons for such delay), where this arises. The Incident Report did not contain this information.

TIC sought to argue, in its above submission, that “*...as [it] has explained, the delay in notification to TIC arose from a failure to add the TIC DPO as watcher on the Incident Report.*” I do not accept, as submitted by TIC, that a controller can seek to remedy the deficiencies in the documentation which it says constitutes its ‘record’ of the breach, for the purposes of Article 33(5), by furnishing further information to the supervisory authority in response to queries *ex post facto*, which themselves arise from those very deficiencies in the information provided to the supervisory authority.

10.25 I also consider that the Incident Report is deficient as to how it addresses the issue of the ‘effects’ of the Breach. The requirement in Article 33(5) that a controller must document the ‘effects’, or consequences, of a personal data breach is linked to the requirement, under Article 33(1), that a controller must assess the risk that could result from a personal data breach.

As outlined above, TIC has asserted that the ‘effects’ of the Breach are addressed in the Incident Report by way of a statement, contained in the introductory section of the document, that “*users can unknowingly disable the ‘protect my account’ setting when adding a new email to their account using Android Mobile App.*” There is also reference, in the Timeline section of the Incident Report, to the issue being upgraded in terms of its severity following a review of potential impact numbers; and some

²³⁸ Submissions in relation to the Preliminary Draft, para. 16.11

discussion of the issue, set out in exchanges of communications between relevant personnel, in the 'Open Items' section of the Incident Report.

- 10.26 In the Breach Notification Form, TIC confirmed the impact upon affected users as being “significant” and also stated, in respect of the reasons for the delayed notification to the Commission, that

“The severity of the issue – and that it was reportable – was not appreciated until 3 January 2018 at which point Twitter’s incident response process was put into action.”²³⁹

Arising from this, in the course of the Inquiry, the Investigator requested that TIC would provide, as part of its documentation in accordance with Article 33(5), a copy of any risk assessments. This request was first made by the Investigator in the Notice and was repeated in the correspondence to TIC dated 29 January 2019.

In its response, dated 1 February 2019, TIC did not furnish any documentation pertaining to its assessment of risk, but it outlined as follows:

“..while TIC believes that people who were impacted by this issue would have immediately realized that their account had been unprotected by virtue of the disappearance of the “lock” from their account profile...and thus would have been able to immediately reprotect their account should they have chosen, TIC decided to provide notice to impacted persons upon becoming aware of this issue.”²⁴⁰

- 10.27 Having considered the contents of the Incident Report (as being the primary document in which TIC recorded the Breach), I do not consider that it demonstrates, or reflects, how TIC assessed the risk arising from the Breach.

In this regard, the Incident Report makes only very brief reference to the severity of the impact of the Breach upon users, but there is no further evidence in this document of the assessment of the risk to users in the context of the Breach, or of the factors considered by TIC, for this purpose.

In that regard, the above statement, made by TIC in its submissions dated 1 February 2019 to this office by way of explanation as to how it assessed the risk arising from the Breach, is not supported by the documentation furnished.

- 10.28 In its Submissions in relation to the Preliminary Draft, TIC submitted that

“It is not clear from the Draft Decision whether the DPC expects a controller to document a risk assessment that it can provide to the DPC to demonstrate that it carried out an appropriate risk

²³⁹ Breach Notification Form dated 8 January 2019, Section 3.2

²⁴⁰ Submissions dated 1 February 2019, Annex, 11

assessment or whether it is sufficient for the controller to provide sufficient details to the DPC so that it can form its own view of the risk (Para 10.15).”²⁴¹

TIC further submitted that

“In either case, this was not an issue in the case of the Underlying Bug....a verification exercise could have served no useful purpose in this instance, since TIC had already fixed the Underlying Bug, notified the DPC and decided to notify the data subjects. Therefore, Article 33(5) did not require documentation of a risk assessment in this instance.”²⁴²

As already set out above and at section 8, I do not accept TIC’s submission that it could not have known that it was required to document its assessment of the risk posed by the Breach. The requirement to carry out a risk assessment is clear from Article 33(1). In addition, the requirement, under Article 33(5), that a controller document the ‘effects’ (or consequences) of the breach clearly encompasses a requirement to document the risk posed by the breach.

I also do not accept TIC’s submission above to the effect that, as by the time of the Investigator’s request to be provided with a copy of TIC’s risk assessment, *“TIC had already fixed the Underlying Bug, notified the DPC and decided to notify the data subjects”* TIC was not required, *“in this instance”*, to document the risk assessment. This argument ignores the fact that TIC’s documentation of the risk assessment relating to the Breach should have taken place at least at the same time as it fixed the bug, and, in any event, immediately upon becoming aware of it, because such a risk assessment is an inherent aspect of making a breach notification. The notification of the Breach to the Commission and affected data subjects should have been informed by TIC’s prior assessment of the risk posed by the Breach. In this regard, TIC is incorrect to say that it did not have to document its assessment of risk *“in this instance.”*

- 10.29 Having regard to the foregoing, and in summary, I do not consider that the Incident Report comprises a sufficient record or document of the Breach in circumstances where it does not contain all material facts concerning the notification of the Breach to the Commission. In this regard, the Incident Report does not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, the Incident Report does not address how TIC assessed the risk, arising from the Breach, to affected users.
- 10.30 Arising from the above deficiencies, in terms of verifying compliance with the requirements of Article 33(1) and 33(2), I do not consider that the Incident Report contains sufficient information to enable TIC’s compliance with the requirements of Article 33(3) to be verified.
- 10.31 In the context of the requirements of Article 33(4), and the provision therein for phased notification by the controller, I note that the Timeline section of the Incident Report refers (in the entry for 15 January

²⁴¹ Submissions in relation to the Preliminary Draft, para. 14.16

²⁴² Ibid

2019) to the number of affected EU/EEA users, which information was communicated to the Commission on 16 January 2019.

In the Preliminary Draft, I noted, however, that the Incident Report did not contain any reference to the Updated Notification Form which was sent to the Commission, and wherein the affected number of EU/EEA Users was confirmed, on 16 January 2019. However, I did not make any conclusion as to whether this represented a deficiency in terms of the recording of the Breach for the purpose of Article 33(5).

- 10.32 In its Submissions in relation to the Preliminary Draft, TIC outlined (at paragraph 16.4) how, following its initial notification to the Commission on 8 January 2019 in the Breach Notification, it provided information to the Commission in phases. In this regard, TIC outlined that it “...*provided an updated cross-border notification form on 16 January which included the numbers affected, in so far as it was able to assess this..*”

TIC further submitted that “*Providing information in phases as it becomes available is expressly permitted by Article 33(4) so this was not a deficiency.*”²⁴³

TIC’s submission on this point appears to be misplaced. As I have set out above, Article 33(4) makes provision for phased notification by a controller of a breach so there is no question that TIC was permitted to notify the Breach in phases. Any assessment by me of this section of the Incident Report was not for the purpose of assessing whether TIC had complied with Article 33(4) but was for the purpose of assessing whether its record of the Breach (as contained in the Incident Report) verified its compliance with Article 33(4) (as is required by Article 33(5)).

Insofar as the Incident Report reflects, in the timeline section, that TIC collated the additional information regarding the number of affected EU/EEA users on 15 January 2019, which was then provided to the Commission on 16 January in the Updated Notification Form, I consider that the Incident Report was satisfactory as to how it evidenced TIC’s compliance with Article 33(4).

- 10.33 For the reasons set out above, therefore, I have concluded that the Incident Report does not meet the requirement, set out in Article 33(5), of enabling verification of TIC’s compliance with Article 33.
- 10.34 However, in considering TIC’s compliance with the requirements of Article 33(5), I have also considered the other documentation furnished by TIC during the course of the Inquiry. This can, broadly speaking, be broken into two categories, comprising

- The various JIRA tickets; and
- The calendar invites and internal ‘Slack’ message

²⁴³ Submissions in relation to the Preliminary Draft, para. 16.4

Analysis of the JIRA²⁴⁴ tickets

- 10.35 During the course of the Inquiry, TIC furnished copies of a number of ‘tickets’, relating to the incident. TIC has also made specific submissions in respect of these documents, as contained in its Submissions in relation to the Draft Report.

In this regard, TIC stated as follows:

“Article 33(5) also requires that the documentation shall enable the supervisory authority to verify compliance with the other requirements of Article 33, which amount to the notification obligations placed on the processor and controller by Articles 33(1) and 33(2). We consider that TIC’s documentation meets this requirement, subject to the limitations in relation to oral notifications discussed earlier in this submission.”²⁴⁵

(TIC’s reference, in the above extract, to “...the limitations in relation to oral notifications..” is a reference to the fact that, as TIC has itself confirmed, it did not document the notification of the Breach by Twitter Inc. to TIC, which was communicated orally to the DPO during the course of a meeting on the 7 January 2019).

- 10.36 In terms of the ‘ticket’ documents provided by TIC, I consider that these fall into three categories:

- i. The initial “triage” ticket from Contractor 2;
- ii. The Incident Management and Investigation tickets; and
- iii. Tickets relating to the remediation of the issue.

I have set out below, in brief, an outline of what these documents contain before outlining my view as to whether they meet the requirement, in Article 33(5), as a means of verifying TIC’s compliance with Article 33.

- i. The initial “triage” ticket from Contractor 2

TIC has confirmed that once Contractor 2 had triaged the report from Contractor 1, it issued notification of same to Twitter Inc. in the form of a JIRA ticket. This document, which is dated between 26 December 2018 and 29 December 2018, therefore, pre-dates the point at which the incident was determined by Twitter Inc’s legal team as comprising a personal data breach. It comprises the communication of the incident by Contractor 2 to Twitter Inc.

²⁴⁴ JIRA is a “work management tool, from requirements and test case management to agile software development”. It facilitates the creation of tickets to manage incidents and cases in a workplace. <https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for>.

²⁴⁵ Submissions in relation to the Draft Report, para 5.10

As set out above, this document was provided by TIC in redacted format, and TIC has confirmed that the redacted portion relates to *“the exchange which took place on 3 January between Twitter Inc.’s Information Security and legal teams.”*²⁴⁶

ii. Incident Management and Investigation tickets

As set out above, these documents were provided by TIC in response to queries raised by the Investigator concerning whether the process as outlined in the DART Runbook - which identified that the correct step at that point in time in the incident management process was to add the DPO (in addition to other personnel) as a ‘watcher’ to the incident management ticket – had been followed (as referenced above in section 7).

TIC also provided, with its letter dated 1 February 2019, a list of ‘watchers’ in respect of the Investigation and IM Tickets. These are set out in two separate documents, listing various personnel. They were provided by TIC in response to a request by the Investigator to be provided with *“...a list of the individuals that were added as watchers to both the Investigation Ticket and the IM ticket.”*²⁴⁷

iii. Documents (including tickets) relating to remediation of the issue

TIC also, during the course of the Inquiry, provided copies of various documents relating to the ‘patch’ applied to rectify the bug which gave rise to the Breach. These documents include a document relating to the ‘patch’ applied (entitled *‘Fix hardcoded protectedUser params for settings updates’*) and a number of JIRA tickets which relate to the application of the fix.

10.37 I have considered the contents of the three types of documents, set out above at paragraph 10.36, in the context of the requirements of Article 33(5), and in particular, having regard to the requirement that the ‘documentation’ of the Breach *“...shall enable the supervisory authority to verify compliance with this Article.”*

I consider that, whilst the JIRA tickets contain disparate items of limited information relating to the facts of the Breach and its impact on users, I do not consider that (either individually or collectively) they contain sufficient information for the purposes of verifying TIC’s compliance with Article 33.

In particular, the tickets do not contain information relating to the delay in Twitter Inc.’s notification of the Breach to TIC, or information relating to the date on which TIC was made aware of the Breach. In addition, one of the tickets, the initial assessment ticket from Contractor 2 (at (i) above) pre-dates the assessment of the incident (by Twitter Inc.) as being a personal data breach.

²⁴⁶ Submission in relation to the Draft Report, para 4.5.3

²⁴⁷ Letter dated 29 January 2019 from DPC to TIC, Appendix, 2(ii)

Analysis of the calendar invites and internal 'Slack' message

- 10.38 As set out above, TIC also provided, during the course of the Inquiry, copies of a series of calendar invites, which relate to the involvement of the DPO in the incident from 7 January 2019, being the date on which the DPO was notified of the Breach.

In terms of their contents, these comprise internal communication / invite documents, which set out, by reference to a date and time, a list of persons invited to a meeting / event. They also set out, in very basic terms, the purpose of the meeting. The earliest of these documents is a calendar invite dated 3:30 pm – 4 pm on Monday 7 January 2019 and constitutes a record of the first involvement of the DPO in meetings relating to the Breach (following the oral notification to him on that date).

TIC also furnished (with its Submissions in relation to the Draft Report) a copy of an internal ('Slack') message, dated 7 January 2019 at 11:23 am between the DPO and Twitter Inc., wherein the DPO requested to be added to the "IM-3080 materials". This document was provided by TIC by way of further documentary evidence as to the point in time at which the DPO (and, therefore TIC) was notified of the Breach by Twitter Inc.

- 10.39 I have considered whether the documents, set out above, at 10.38, meet the requirements of Article 33(5). It is important to note, in this regard, that these documents were provided by TIC by way of documentary evidence in respect of the point in time at which the DPO (and by extension, TIC) was made 'aware' of the Breach on the 7 January 2019.

As I have set out above, the question of when TIC became 'aware' of the Breach informed the Investigator's provisional finding in respect of both Article 33 and Article 33(5). In relation to Article 33(5), the Investigator's provisional finding was that, as TIC did not document the point in time at which it became aware of the Breach, it did not comply with its obligation pursuant to Article 33(5) to document the Breach.

As I have also set out above, in my role as decision-maker, I have carried out an independent review of all of the documentation furnished by TIC during the course of the Inquiry including during the decision-making phase. In that regard, whilst I agree with the Investigator's assessment that TIC did not document the point in time at which it became aware of the Breach, I am of the view that TIC's documentation of the Breach was deficient in a number of other, significant respects, which I have set out above.

- 10.40 As I have already outlined above, having reviewed all of the documentation furnished by TIC, I consider that it does not comprise, specifically, a record or document of a *personal data breach* which meets the requirements of Article 33(5) but is, rather, documentation of a more generalised nature, including various reports and internal communications that were generated in the context of TIC's management of the incident.

- 10.41 Connected to the above view, which was also expressed on a provisional basis in the Preliminary Draft, TIC submitted, in its Submissions in relation to the Preliminary Draft, that it did not agree that Article 33(5) requires a separate record of a personal data breach and that recording the information “*in some form*”²⁴⁸ is sufficient.

I have already addressed TIC’s submission on this point above. As I have outlined, in this regard, neither the Breach Notification Guidelines nor the GDPR impose a specific requirement on a controller to maintain a separate ‘register’ of breaches. However, it is clearly envisaged by both that the record maintained by a controller must be specific to a ‘personal data breach’, rather than being comprised of a disparate collection of records that the controller has generated in the context of its general day-to-day operations or in the context of the application of its internal processes for security / technical incident management.

TIC submitted (at paragraph 13(d)) of its Submissions in relation to the Preliminary Draft) that “***TIC keeps a record of all incidents which have privacy implications so it is easily able to extract all relevant records on request, as required by the Breach Notification Guidelines***” (Emphasis added). However, no such ‘record’ was provided to the Commission during the course of the Inquiry. The documents provided by TIC as comprising its ‘record’ of the Breach were made up of a collection of documentation of a generalised nature, including various reports and internal communications, that were generated in the context of TIC’s management of the incident.

- 10.42 I also consider that the deficiencies of the documentation provided by TIC as a ‘record’ of the Breach, and which I have outlined above, are demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple queries in order to gain clarity concerning the facts and sequencing surrounding the notification of the Breach.

This is, in particular, exemplified by the lack of clarity in relation to the issue of when TIC (through the DPO) was notified of the Breach by Twitter Inc. and the facts surrounding this issue.

In this regard, I note that TIC provided, in its Submissions dated 25 January 2019 and 1 February 2019, copies of the Incident Report and IM Ticket and Investigation Ticket. In addition, as set out above, TIC provided (with its response dated 1 February 2019) a list of ‘watchers’ to those tickets.

However, notwithstanding the provision of these documents by TIC on 25 January and 1 February 2019, it was not until after further queries had been raised by the Investigator that TIC actually clarified, in its submissions dated 8 February 2019, that the delay in Twitter Inc.’s notification of the Breach to TIC had arisen due to a deviation from the process set out in the DART Runbook, whereby the DPO was not added as a ‘watcher’ to the IM Ticket.

²⁴⁸ Submissions in relation to the Preliminary Draft, para 14.17 (relating to Paragraph 10.26 of the Preliminary Draft)

- 10.43 In the Submissions in relation to the Preliminary Draft, TIC submitted that it did not agree with my view, outlined above and which was set out on a provisional basis in the Preliminary Draft, that the deficiencies in the documentation which it furnished as being the ‘record’ of the Breach were demonstrated by the level of queries which the Investigator had to raise during the Inquiry in order to clarify the facts surrounding the notification of the Breach and, in particular, the facts surrounding the delay in TIC being made aware of the Breach.

TIC’s submission in this regard was made on the basis that my finding on this issue “...is only relevant to whether TIC breached Article 33(5) if Article 33(5) requires documentation of the timing and process around breach notification rather than of the breach.”²⁴⁹

I have already outlined above that I do not accept TIC’s interpretation of Article 33(5) to the effect that the requirement to document a breach does not include a requirement that a controller record the reasons for a delay in notifying a breach. As I have outlined above, such an interpretation is inconsistent with the wording of Article 33(5) and the overall objective of Article 33, which is to ensure the timely notification of breaches to a supervisory authority.

TIC’s offer to provide supplemental information by way of sworn affidavit

- 10.44 Before setting out my findings in respect of Article 33(5), I consider that it is important to note that, in the course of its submissions to this office, TIC offered to provide supplemental information, by way of a sworn affidavit, in relation to the issue of the point in time at which it, as controller, was made aware of the Breach. This is in circumstances where TIC did not maintain documentation recording the notification by Twitter Inc. of the Breach to the DPO, which took place orally during a meeting on 7 January 2019.²⁵⁰

Similarly, TIC also submitted, in respect of the issue of the delay in Twitter Inc. notifying TIC of the Breach and how this arose, as follows:

*“TIC has been transparent about its process and the failure to follow it properly when opening the IM ticket. We are aware that the DPC has statutory tools available to it by which it can require TIC to answer questions under oath. If this process had been used, TIC would have provided the same information about the way in which it became aware as it has already provided. In view of this we believe that it is unreasonable for the DPC to find that TIC’s written submissions with respect to the timeline and notification of the TIC DPO are insufficient evidence.”*²⁵¹

²⁴⁹ Submissions in relation to the Preliminary Draft, para 16.12

²⁵⁰ Submissions in relation to the Draft Report, Paragraph 4.7

²⁵¹ Submissions in relation to the Draft Report, para 4.6

- 10.45 In the Submissions in relation to the Preliminary Draft, TIC submitted that “[it] wished to clarify the purpose of the offered affidavit...the offer to provide an affidavit was not connected to the record keeping requirements of Article 33(5).” TIC further submitted, in this regard, that

“The purpose of the offered affidavit was to confirm the point at which TIC became aware of the Underlying Bug, which would enable the investigator to establish whether TIC had complied with its obligation to notify under Article 33(1). The offer did not relate to Article 33(5).”²⁵²

I accept that TIC’s purpose in offering to provide a sworn affidavit was to verify the time at which the DPO, and therefore TIC, became aware of the Breach and was not directly connected to the record keeping requirement of Article 33(5). However, it is the case that, had TIC properly documented the Breach, including the reasons for its delay in notifying same, this information would have been contained within its record of the Breach.

As the requirement in Article 33(5) is that a controller must ‘document’ a breach and that this documentation “shall enable the supervisory authority to verify compliance” with Article 33, the record(s) maintained must, by necessity, include all of the salient facts in relation to the breach. As set out above, therefore, I do not consider that a controller can remedy the deficiencies in the documentation which it says constitutes documentation for the purposes of Article 33(5) by furnishing further information to the supervisory authority in response to queries, which themselves arise from those very deficiencies.

- 10.46 In conclusion, for all of the reasons set out above, I do not consider that the documentation maintained by TIC amounts to the documentation, or recording, of, specifically, a ‘personal data breach’ as is required under Article 33(5).

FINDING – Article 33(5)

- 10.47 **Having regard to the foregoing issues, therefore, and having considered and taken account of all submissions made by TIC in relation to the Preliminary Draft, I have found that TIC did not comply with its obligations under Article 33(5) to ‘document’ the Breach, for the reasons I set out below:**

- On the basis of my assessment of the documentation furnished by TIC during the course of the Inquiry, and wherein it claims that it ‘documented’ the Breach, I do not consider that this documentation contains sufficient information so as to enable the question of TIC’s compliance with the requirements of Article 33 to be verified.

²⁵² Submissions in relation to the Preliminary Draft, para 15.2, 15.3

- In particular, I do not consider that the Incident Report - which is identified by TIC as being the primary record in which it documented the facts, effects, and remedial action taken in respect of the Breach - comprises a sufficient record or documenting of the Breach in circumstances where it does not contain all material facts relating to the notification of the Breach to the Commission. In particular, the report does not contain any reference to, or explanation of, the issues that led to the delay in TIC being notified of the Breach. In addition, the Incident Report does not address how TIC assessed the risk, arising from the Breach, to affected users.
- With regard to the other documents furnished by TIC, including the JIRA tickets, whilst these contain disparate items of limited information relating to the facts of the Breach and its impact on users, I do not consider that (either individually or collectively) they contain sufficient information for the purposes of verifying TIC's compliance with Article 33.
- Based on a review of all of the documentation furnished by TIC, I do not consider that, either collectively or individually, it comprises a record or document of, specifically, a '*personal data breach*' within the terms of Article 33(5), but is documentation of a more generalised nature, including reports and internal communications, that were generated in the context of TIC's management of the incident.
- The deficiencies in the documentation furnished by TIC as a 'record' of the Breach are further demonstrated by the fact that, during the course of the Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

11. DECISION UNDER SECTION 111(2) OF THE 2018 ACT

- 11.1 I have set out above, pursuant to Section 111(1)(a) of the 2018 Act, my decision to the effect that TIC has infringed both Article 33(1) and Article 33(5) of the GDPR.

Under Section 111(2) of the 2018 Act, where the Commission makes a decision (in accordance with Section 111(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised.

For the reasons set out above, and as outlined below, I have decided to exercise corrective powers under Section 111(2) of the 2018 Act.

- 11.2 As I have set out above at paragraph 1, this Decision is made by the Commission in accordance with Section 111 of the 2018 Act and the GDPR. A Preliminary Draft of this Decision was furnished to TIC on 14 March 2020 for the purpose of enabling TIC to make any submissions it wished to make in relation to the provisional findings and corrective powers that were set out in the Preliminary Draft. I have taken account of TIC's submissions in respect of the specific corrective powers at the relevant sections below.

- 11.3 Before turning to address the corrective powers, and TIC's submissions in respect of same, I wish to address a general submission which TIC made at Paragraph 10 of its Submissions in relation to the Preliminary Draft, and which relates to the Commission's exercise of its discretion in commencing the Inquiry.

- 11.4 In this regard, in its Submissions in relation to the Preliminary Draft (at paragraphs 10.1 – 10.6), TIC made the following submissions:

- *"The DPC has discretion on whether to open an investigation. It should have exercised its discretion and not opened an investigation in this instance. The DPC's own guidance on when it will consider commencing an inquiry provides that*

*"[g]enerally speaking, the DPC will only consider commencing an inquiry where the matter raised indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing within the organisation in question."*²⁵³

- TIC submitted that *"the alleged breach in relation to Article 33(1) is not a potential exposure of private data, nor the underlying bug which TIC identified in its systems, but TIC's alleged*

²⁵³ Submissions in relation to the Preliminary Draft, para. 10.1 referring to Data Protection Commission, online guidance on 'Complaints handling, Investigations and Enforcement For Organisations' at <https://www.dataprotection.ie/en/organisations/resources-organisations/complaints-handling-investigations-and-enforcement-organisations>

failure to notify the DPC without undue delay and in any event within 72 hours of when the DPC considers it ought to have been aware of a notifiable personal data breach.” TIC further submitted that *“Defined in this way, the alleged breach does not meet the thresholds for either a data breach (as the term is used in the guidance referred to [above] that is “extremely serious” or “indicative of a systemic” failure within TIC.*

- TIC further submitted that, in accordance with guidance previously issued by the Commission, *“in relation to the risk thresholds for reporting personal data breaches pursuant to Articles 33 and 34”,* neither of the two thresholds referenced there of “high risk” or “severe risk” have been met in this case.
- TIC further submitted that *“[there] was no evidence of any actual harm suffered by affected individuals at the time TIC notified the DPC, and TIC had already identified and was in the process of remedying the bug at the time it notified the Underlying Bug to the DPC”*
- TIC further submitted that *“It is not appropriate for the DPC to sanction TIC for non-compliance with Article 33(1) when its concerns are actually based around whether or not TIC fulfilled its obligations under Articles 24 and 32, the investigation of which the DPC has stated is outside the scope of its investigation.”²⁵⁴*

11.5 I have considered TIC’s submissions, as set out above, to the effect that the Commission should not have opened an Inquiry in this matter and I do not accept same for the reasons which I outline below.

11.6 The Inquiry in this case was commenced pursuant to Section 110 of the 2018 Act.

Section 110(1) of the 2018 Act provides that the Commission may, for the purpose of Section 109(5)(e) or Section 113(2) of the 2018 Act, or of its own volition, **cause such inquiry as it thinks fit to be conducted**, in order to ascertain whether an infringement has occurred or is occurring of the GDPR or a provision of the 2018 Act, or regulation under the Act, that gives further effect to the GDPR.

11.7 In this regard, the Commission saw fit to commence an Inquiry (on 22 January 2019) for the purpose of examining and assessing the circumstances surrounding the notification by TIC to the Commission of the Breach. The Inquiry was commenced in circumstances where TIC had, in its notification of the Breach to the Commission, confirmed that the number of affected EU/EEA data subjects was 88,726 and where TIC had, in the Breach Notification Form, identified the potential impacts for affected individuals, as assessed by TIC, as being “significant”.²⁵⁵

²⁵⁴ Submissions in relation to the Preliminary Draft, paras 10.1-10.6

²⁵⁵ Breach Notification Form, Section 5.6

- 11.8 Furthermore, the Inquiry was commenced in circumstances where, on the basis of the information contained within the Breach Notification Form, and in particular, arising from the language usage therein, it initially appeared to be the case that TIC (as controller) had become aware of the Breach on 26 December 2018 or on the 3 January 2019, which in either case, meant that the notification to the Commission on 8 January 2019 was outside the 72 hour timeframe permissible under Article 33(1).
- 11.9 Therefore, on the basis of the nature of the Breach, the high number of EU/EEA data subjects affected and TIC's assessment of the impact as being "significant", and in circumstances where it appeared that the Breach had been notified to the Commission outside of the timeframe permitted under Article 33(1), the Commission properly exercised its discretion to commence an Inquiry.
- 11.10 I further do not accept TIC's submissions to the effect that, on the basis of guidance published by the Commission, the Commission did not have a valid basis for commencing the Inquiry in this case.
- 11.11 Firstly, in this regard, as is the case with all guidance published by the Commission, the specific guidance referred to by TIC is not intended to be an exhaustive statement of the law, nor is it intended to provide legal advice regarding the interpretation of the relevant provisions of the GDPR. The guidance in question is contained within a section on the Commission's website that is intended to provide **an overview** of the complaint handling, investigation and enforcement procedures conducted by the Commission.
- 11.12 Secondly, and in any event, I do not accept that, having regard to the circumstances of this particular case, the Commission acted inappropriately in commencing an Inquiry by reference to the thresholds outlined in the guidance in question and which is referenced by TIC. The guidance, as referenced by TIC, states that

"[g]enerally speaking, the DPC will only consider commencing an inquiry where the matter raised indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing within the organisation in question."²⁵⁶

In this respect, as outlined above, based on the information communicated to the Commission by TIC in the Breach Notification Form and Updated Breach Notification Form, wherein TIC confirmed the nature of the Breach, the high number of affected data subjects and the fact that it, itself, had assessed the impact as being "significant", the Breach in this instance clearly potentially fell within the category of being "of an extremely serious nature."

²⁵⁶ Submissions in relation to the Preliminary Draft, para. 10.1 referring to Data Protection Commission, online guidance on 'Complaints handling, Investigations and Enforcement For Organisations' at <https://www.dataprotection.ie/en/organisations/resources-organisations/complaints-handling-investigations-and-enforcement-organisations>

11.13 Having regard to the above, therefore, I am satisfied that in this case, the Commission properly exercised its discretion to commence the Inquiry.

11.14 With regard to TIC's submission, outlined above, that "[it] is not appropriate for the DPC to sanction TIC for non-compliance with Article 33(1) when its concerns are actually based around whether or not TIC fulfilled its obligations under Articles 24 and 32, the investigation of which the DPC has stated is outside the scope of its investigation", I have already addressed TIC's submission in this respect above in Section 7.

12. CORRECTIVE POWERS – ARTICLE 58(2) GDPR

12.1 Article 58(2) of the GDPR sets out the corrective powers which supervisory authorities may employ in respect of non-compliance by a controller or processor. In the Preliminary Draft, I proposed, on a provisional basis, that I would exercise both the corrective power at Article 58(2)(b) – a reprimand to TIC as the controller – and the corrective power at Article 58(2)(i), being the imposition of an administrative fine on TIC pursuant to Article 83.

The Reprimand

12.2 With regard to the reprimand, Article 58(2)(b) provides that a supervisory authority shall have the power to "issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation." Additionally, Recital 129 states that:

"The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular, each measure must be necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case..."

Recital 148 is also relevant in this regard, in that it provides that:

"In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine." (Emphasis added)

12.3 Accordingly, it is clear from the GDPR that a reprimand does not have to be issued in isolation to the exercise of any other corrective power. Furthermore, where there is a *minor infringement* or if the controller is a *natural person*, and the imposition of a fine on that controller would be a

disproportionate burden upon them, then it is clear that it *may be* appropriate to issue a reprimand as the only corrective power.

In the Preliminary Draft, I set out my reasons for deciding to impose a reprimand, in addition to an administrative fine, noting that, in accordance with Recital 129, each measure that I decided to impose by way of the exercise of a corrective power for the infringements I had provisionally found must be “...*necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case...*” In summary, my reasons for proposing to impose a reprimand related to the nature of the infringement and the objective of the obligation under Article 33(1) in particular. In this regard, I indicated the importance of ensuring that full effect was given to this obligation, insofar as compliance directly affects the ability of a supervisory authority to consider a breach and whether action needs to be taken to protect individuals affected by the breach. In this context, I also noted that the provisions in respect of communication of a personal data breach to data subjects as set out in Article 33(4), would also potentially be rendered ineffective were it the case that a controller’s obligation to notify a breach, under Article 33(1), was contingent upon the compliance by its processor with its obligations, as had been advocated for by TIC. Having regard to all of those issues, and taking into account the circumstances of this individual case, my provisional view was that the imposition of a reprimand in this case was both necessary and proportionate.

- 12.4 In its Submissions in relation to the Preliminary Draft, TIC strongly objected to my provisional decision to issue a reprimand (and also the proposed imposition of an administrative fine which I deal with separately below). In this regard, TIC submitted that “*..the nature of the alleged infringements are such that a reprimand under Article 58(2)(b) is not an appropriate sanction.*”²⁵⁷

TIC further contended that:

“Article 58(2)(b) provides that each supervisory authority shall have a corrective power: “To issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation.”

TIC’s submission, in this regard, was that the infringements in question, being an infringement of Article 33(1) and Article 33(5), do not comprise “processing operations” for the purpose of the GDPR:

*“The alleged infringements relate to (i) an alleged delay of two days in notifying the supervisory authority of a personal data breach and (ii) a failure to keep appropriate records about the notification process. Neither of these alleged infringements involve actual processing of personal data. The activities concerned are not processing operations, so they do not fall within the scope of the power to issue reprimands.”*²⁵⁸

²⁵⁷ Submissions in relation to the Preliminary Draft, para. 11.1

²⁵⁸ Ibid, para 11.1

- 12.5 The term ‘*processing operations*’ (taking both the singular and the plural) appears 50 times in the GDPR. While the term ‘processing operations’ is not independently defined in the GDPR, the term ‘processing’ is so defined. As will be seen from the definition below, it includes a reference to “an operation or set of operations”, as follows:

“any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”²⁵⁹

Having considered how the term “processing operations” appears in the context of specific obligations on controllers throughout the GDPR, for example in Article 35 concerning Data Protection Impact Assessments, it appears that the term is used in many contexts to denote the treatment or use of - in other words, things that are done to - personal data controlled by a controller. At the same time, I do consider that the definition of the term “processing”, within which the word “operations” appears, is very broadly construed. It is, therefore, arguable that, in the context of a breach notification under Article 33(1), 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 (i.e. under Article 33(1)) is intrinsically connected to one or more processing operations. While I do not consider it necessary to definitively conclude on the meaning and effect of the term “processing operations” as it appears in Article 58(2)(b) for the purposes of this Decision, on balance, I consider that TIC’s legal argument supporting their contention that a reprimand should not be issued in the context of infringements under Articles 33(1) and 33(5) is a stateable one. I have, therefore, decided not to proceed with the issuing of a reprimand to TIC in relation to the infringements which I have found in this Decision.

- 12.6 I also note that TIC made further, separate arguments in its Submissions in relation to the Preliminary Draft outlining other reasons as to why it considered that it was not appropriate to issue a reprimand in the circumstances of this case.²⁶⁰ However, given my decision, as outlined above, not to proceed with issuing a reprimand, I do not consider it necessary to separately consider these arguments.
- 12.7 However, notwithstanding my decision not to proceed to issue a reprimand to TIC, I have nonetheless decided that it is appropriate to proceed, as outlined on a provisional basis in the Preliminary Draft, with imposing an administrative fine on TIC. I have set out the reasons for this decision in section 13 below.

²⁵⁹ Article 4(2), GDPR

²⁶⁰ Submissions in relation to the Preliminary Draft, paras 11.2 to 11.4

13. ADMINISTRATIVE FINE – ARTICLE 58(2)(i)

- 13.1 In the Preliminary Draft, I proposed to impose to impose an administrative fine upon TIC under Article 58(2)(i). I explained that, in determining that it was appropriate to impose an administrative fine, and the value of that fine, I had had due regard to the criteria set out in Article 83(2) GDPR, which is set out below. Thereafter, in the Preliminary Draft, I proceeded to consider each of the below criteria, having regard to the facts of this particular case, outlining how I had applied those criteria to this case.

“Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) 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;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

TIC's general submissions on the proposed imposition of an administrative fine

13.2 In its Submissions in relation to the Preliminary Draft, TIC made a number of general submissions in relation to my decision to issue a fine in respect of the infringement of both Article 33(1) and Article 33(5). In addition, TIC made specific submissions regarding my consideration and assessment of each of the factors under Article 83(2). I have considered TIC's submissions on these specific matters under the relevant factors at Articles 83(2) (a)-(k) below. For completeness, I have set out below a summary of the general submissions made by TIC in respect of my decision to impose a fine in relation to Article 33(1) and Article 33(5). Given that the decision as to whether to impose an administrative fine (and if so, the amount of the fine) must be a cumulative decision which is taken having had regard to each (where applicable) of a range of factors (as set out in Article 83(2)(a) to (k)), it is appropriate that I do not consider the below general submissions independently, but instead that I also consider these submissions in the context of my evaluation of the matters set out in Article 83(a) to (k).

13.3 In respect of my proposed decision to impose an administrative fine in relation to the infringement under Article 33(1), TIC made the following general submissions:

- that it complied with Article 33(1) on the basis that TIC, as controller, notified the Breach to the Commission within 72 hours after having become aware of it. TIC asserts this notwithstanding the fact that Twitter Inc., its processor, had assessed the issue as being a personal data breach on 3 January 2019 but a failure by Twitter Inc. staff to follow its incident management process led to a delay in TIC (as controller) being notified of the Breach, which did not occur until 7 January 2019. TIC submitted, in this regard, that

*"TIC's notification occurred comfortably within this notification time window, based on the interpretation in the Breach Notification Guidelines of when a controller becomes "aware" of a breach. Therefore, TIC complied with Article 33(1)."*²⁶¹

(The issues raised by TIC above have been already addressed in this Decision in section 7 above).

²⁶¹ Submissions in relation to the Preliminary Draft, para 12.1

- that *“It is not appropriate for the DPC to fine TIC for non-compliance with Article 33(1) when its concerns are based around whether or not TIC fulfilled its obligations under other articles of the GDPR.”*²⁶²

The issue raised by TIC in this respect relates to its submission that, in viewing Article 33(1), and the controller’s obligation therein, in the context of the other obligations on a controller under the GDPR, my provisional finding ‘implies’ the obligations arising under those provisions into Article 33(1). (TIC’s submissions in respect of this have already been addressed in this Decision in section 7 above.)

- that the application of the factors under Article 83(2) *“need to be considered in the light of the alleged infringement. In this instance, the nature of the alleged infringement is a two day delay in notifying the DPC of a bug which TIC was already in the process of fixing.”*²⁶³

In this regard, TIC further submitted that *“...on the available evidence the Underlying Bug did not result in any significant damage or distress to users (or indeed any damage or distress to users)...On the contrary, the absence of complaints suggests that there was no significant impact on users in relation to the underlying bug and thus even more so in relation to any alleged delay in notifying the DPC.”*²⁶⁴

As I have already set out above in section 7, and further below, I have taken account of both the nature and duration of the infringement, and the remedial action taken by TIC, in my consideration and application of the factors under Article 83(2). I have also taken into account the issue of damage arising from the infringement.

- that, *“Even if the DPC is correct in finding that TIC infringed Article 33(1), which TIC strenuously denies, it is wrong to conclude that a fine, and particularly, a fine potentially as high as \$500,000 is appropriate in this case.”*²⁶⁵

(The administrative fine imposed in this case is as set out below).

13.4 In respect of my proposed decision (as set out on a provisional basis in the Preliminary Draft) to impose an administrative fine in relation to its infringement of Article 33(5), TIC made the following general submission:

- *“TIC’s documentation process was developed in good faith based on its understanding of the purpose and scope of the Article 33(5) requirements, specifically an understanding that the*

²⁶² Ibid, para 12.3

²⁶³ Ibid, para 12.5

²⁶⁴ Ibid, para 12.6

²⁶⁵ Ibid, para. 12.4

verification element related to verification of decisions by controllers not to notify. Given this understanding of the purpose of verification, it would have made no sense to record information about the timing of awareness or the notification process. This was a reasonable approach to take at the time, given this was a new requirement and everyone's understanding of the requirements was evolving. TIC submits that this case is an appropriate instance for the DPC to exercise its discretion and not impose a sanction as TIC made a good faith attempt at compliance.”²⁶⁶

Binding decision of the EDPB

- 13.5 As set out above at paragraph 1, this Decision is adopted on the basis of the EDPB Decision, (which was adopted on 9 November 2020, as described at paragraph 1.6), pursuant to Article 60(7) in conjunction with Article 65(6) GDPR. In doing so, the Commission has complied with the binding direction of the EDPB, as set out in the EDPB Decision at paragraph 207 thereof, in respect of the administrative fine imposed under this Decision. In this regard, the EDPB Decision, in finding that certain objections, raised by concerned supervisory authorities in respect of the administrative fine proposed in the Commission's Draft Decision, met the requirements of Article 4(24) GDPR²⁶⁷, directed 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.”²⁶⁸

- 13.6 In accordance with the above binding direction, I have taken account, at the relevant parts of Sections 14 and 15 below, of the specific comments of the EDPB, set out in paragraph 198 of the EDPB Decision, to the effect that “...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.”²⁶⁹

I have also taken account of the comments of the EDPB, set out in the EDPB Decision at paragraphs 182 to 197 thereof, and in which the EDPB has set out its reasons as to why greater weight should be accorded to these elements.

²⁶⁶ Ibid, para 17.1

²⁶⁷ The EDPB decided that the objections raised in respect of the administrative fine proposed in the Commission's Draft Decision by the Austrian Supervisory Authority (Österreichische Datenschutzbehörde), the German Supervisory Authority (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) and the Italian Supervisory Authority (Garante per la protezione dei dati personali) were relevant and reasoned under Article 4(24)

²⁶⁸ EDPB Decision, para 207

²⁶⁹ EDPB Decision, paragraph 198

14. CONSIDERATION OF THE CRITERIA IN ARTICLE 83(2) IN DECIDING WHETHER TO IMPOSE AN ADMINISTRATIVE FINE

This section sets out my consideration of the criteria at Articles 83(2)(a) to 83(2)(k) GDPR in deciding whether to impose an administrative fine.

Article 83(2)(a) - 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

- 14.1 I outline below my consideration of the nature, gravity and duration of the infringements. In so doing, I am required, by Article 83(2)(a) to take account of the nature, scope or purpose of the processing being carried out by TIC, and in addition, the number of data subjects affected and the level of damage suffered by them. I have, therefore, set out below the matters which I have considered under these headings.

Nature, scope or purpose of the processing

- 14.2 In terms of the ‘nature, scope or purpose of the processing’, I have had regard to the nature of the processing operations carried on by Twitter, which comprises a “microblogging” and social media platform on which users have the opportunity to document their thoughts in “tweets”.

A user of Twitter can decide if their tweets will be “protected” or “unprotected”. In the former case, only a specific set of persons (followers) can read the user’s protected tweets. In terms of the nature of the processing that gave rise to the Breach, which is the subject of the Inquiry, this arose from a ‘bug’, whereby if a user operating an Android device changed the email address associated with that Twitter account, their tweets became unprotected and consequently were accessible to the wider public without the user’s knowledge.

- 14.3 In terms of the scope of the processing, TIC has confirmed to the Commission that, as far as it can identify, between 5 September 2017 and 11 January 2019, 88,726 EU/ EEA users were affected by this bug. However, TIC has further confirmed that it dates the bug to 4 November 2014, but that it can only identify users affected from 5 September 2017. In this regard, TIC has confirmed its belief that “additional people were affected during the period from 4 November 2014 to 14 January 2019 when the bug was fully remediated.”²⁷⁰

- 14.4 In considering the nature, scope and purpose of the processing concerned, therefore, I have taken account of both the number of users affected by the underlying bug, and the nature of the processing operations that gave rise to the Breach. In this regard, and as I have set out at the

²⁷⁰ Updated Breach Notification Form

relevant sections below, I have, as part of my overall assessment of the nature, scope and purpose of the processing, had regard to the fact that the processing concerned in this case involved communications by data subjects who had deliberately chosen to restrict the audience of those communications. In this regard, I have taken specific account of the comments in the EDPB Decision, at paragraphs 186 and 187 thereof. In particular, I have taken account of the view expressed by the EDPB, at paragraph 187 of the EDPB Decision, to the effect that the Commission should have given significant weight to this fact in light of the reference in the Draft Decision (at paragraph 14.51 thereof) to the effect that *“the 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.”* These issues are outlined below, at paragraph 14.101 of this Decision, in the context of my consideration of the criterion under Article 83(2)(g) in relation to the categories of personal data affected by the infringement. However, as set out above, in taking account of the EDPB’s comments, I have given greater weighting to these factors as part of my overall assessment of the criteria under Article 83(2).

Number of data subjects affected and the level of damage suffered by them

14.5 In respect of the number of affected data subjects, as set out above, this has been confirmed by TIC as being 88,726 EU/EEA users (between the period from 5 September 2017 to 11 January 2019). However, as also set out above, TIC has confirmed that it is likely that additional users were affected during the period from 4 November 2014 to 14 January 2019, when it has confirmed that the bug was remediated. In the Preliminary Draft, I considered, on a provisional basis, that the fact that the personal data breach that led to the infringements in this case affected such a significant cohort of people rendered it a factor which should be taken into account in deciding to impose an administrative fine and, also, in terms of the level of that fine.

14.6 In its Submissions in relation to the Preliminary Draft, TIC submitted that taking account of the number of data subjects affected by the bug or incident leading to the Breach, *“...confuses the impact of the Underlying Bug with the impact of the alleged infringement (that is, the alleged delay in notifying the DPC).”*²⁷¹

TIC further submitted that *“The number of users potentially affected by the underlying bug was the number of people with protected tweets who had changed a setting during the relevant time period. However, none of these people...were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC...”*²⁷²

²⁷¹ Submissions in relation to the Preliminary Draft, para. 12.9

²⁷² Ibid, para. 12.10

In addition, TIC submitted (in respect of Article 33(5)) that

“Article 83(2)(a) directs the supervisory authority to consider the number of data subjects affected by the infringement. In this instance, the alleged infringement is a failure (in the DPC’s view) to maintain records which enabled the DPC to verify TIC’s compliance with Article 33.”²⁷³

14.7 In essence, TIC’s position is that no individuals were affected by the delayed notification of the Breach to the Commission. In addressing this contention, it is relevant to observe at this point that, in the particular circumstances of this case, the Commission did not order / direct any further substantive measures to be taken by TIC in relation to the Breach. This was in circumstances where, between the original Breach Notification being submitted to the Commission on 8 January 2019, in which TIC stated that it would not be informing users, and the Updated Breach Notification Form submitted on 16 January 2019, and interactions between TIC and the Commission concerning the Breach during the intervening period, TIC changed its original position and indicated, in the later Updated Breach Notification Form, that it would provide a user notice on 17 January 2019.²⁷⁴ In this regard, I do not consider that TIC can be sure that no users affected by the Breach were affected by the delayed notification. This is an assumption without any evidence to support it. The facts show that TIC notified data subjects on 17 January 2019 (some 9 days after it had first notified the Commission of the Breach when its position had been that it would not notify data subjects). It remains a possibility that the delayed notification to data subjects, following the delayed notification of the Breach to the Commission, may have caused damage to users affected by the Breach. In any event, the Commission’s assessment was inevitably delayed as a result of the delayed notification (which is acknowledged by TIC²⁷⁵). Further, and in any event, given that it was always open to the Commission to decide, on foot of its assessment of the Breach, that other steps needed to be taken by it or by TIC to safeguard, or mitigate any risks to, data subjects from the Breach, there was a significant volume of data subjects who potentially would have been affected (as a result of the potential for delay in such action being taken by the Commission due to the knock-on effect of the delayed notification).

14.8 I consider that similar issues arise in relation to the assessment under Article 83(2)(a) concerning the ‘level of *damage*’ suffered by affected data subjects. Insofar as the Breach itself is concerned, TIC has indicated that the level of potential impact for affected individuals is “*significant*”.²⁷⁶ 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. In this regard,

²⁷³ Ibid, para 17.5

²⁷⁴ See above at para. 2.9

²⁷⁵ Submissions in relation to the Preliminary Draft, para. 12.17 which stated “*To the extent there was an infringement under Article 33(1), it is correct that this might have delayed the assessment by the DPC. However, this did not have a practical impact on the affected data subjects, since the DPC did not take, or order TIC to take, any additional actions “...to protect and/or remedy the impact on” affected data subjects.*”

²⁷⁶ Breach Notification Form, section 5.6

I indicated in the Preliminary Draft 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. In its Submissions in relation to the Preliminary Draft, TIC acknowledged *“that the Underlying Bug created the possibility that information which might cause users embarrassment, damage or distress might be exposed; it is for this reason that it identified the potential impact as significant in its initial report of the Underlying Bug. However, the DPC is not entitled to assume from this that the data which was exposed did in fact include sensitive material and was in fact accessed by anyone...”*²⁷⁷

14.9 Additionally, in its Submissions in relation to the Preliminary Draft, TIC contended, with regard to the issue of “damage”, that none of the users affected by the underlying bug *“were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC, particularly since Twitter was already remedying the Underlying Bug when TIC notified the Underlying Bug to the DPC.”*²⁷⁸ While I accept that, on the facts, there was no evidence of direct impact caused to users as a result of the delayed notification, as I have referred to above in connection with the number of affected data subjects, the delayed notification created at least the potential for damage to data subjects, insofar as any remedial / safeguarding actions which the Commission might otherwise have directed TIC to take (or undertaken itself) would have consequently been delayed.

14.10 Accordingly, I consider 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 and any ensuing actions by the Commission), are still relevant factors to take into consideration in my analysis as to whether a fine should be imposed under Article 83.

14.11 In the Draft Decision, I noted that, whilst it cannot be definitively said that no users affected by the Breach were affected by the delayed notification, equally, there was no direct evidence of damage to them from the delayed notification. Accordingly, it was my view, as expressed in the Draft Decision, that less weight should be attributed to this factor in my overall assessment of Article 83, than I had previously indicated was my provisional position in the Preliminary Draft. I also confirmed that I had taken this into consideration as a mitigating factor in relation to Article 83(2)(k).

14.12 In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in

²⁷⁷ Submissions in relation to the Preliminary Draft, para. 12.12

²⁷⁸ Ibid, para. 12.10

my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.

Nature of the infringement

14.13 In considering the nature of the infringements by TIC, these comprise (as set out above) a failure to comply with the notification requirements of Article 33(1) and a failure to comply with the requirement under Article 33(5) to ‘document’ a personal data breach. **In that regard, the infringements in question do not relate to the substantive matter of the Breach itself. This has been a central matter in my consideration of the factors relevant to the imposition of an administrative fine and the amount of same.**

14.14 As discussed above in Section 7, the objective of Article 33(1) is to ensure prompt notification of data breaches to supervisory authorities so that a supervisory authority can assess the circumstances of the data breach, including the risks to data subjects, and decide whether the interests of data subjects require to be safeguarded, to the extent possible, by mitigating the risks to them arising from a data breach, by action on the part of the supervisory authority – for example by requiring the controller to notify data subjects about the breach under Article 34(4).²⁷⁹

14.15 Non-compliance with Article 33(1) (whether in absolute terms, where there is no notification made at any point, or where there is non-compliance with the timeframe for notification) will interfere with that objective by preventing or delaying the supervisory authority from taking such enforcement action as may be appropriate in light of the risks posed by the particular data breach. This, in turn, may have an impact on the safeguards and mitigation measures which data subjects might otherwise benefit from. In other words, this may compound the potential damage suffered by data subjects – firstly, from the occurrence of the data breach itself and secondly, by stymying or delaying the taking of safeguarding actions on the part of the supervisory authority.

²⁷⁹ This underlying objective is apparent from Recital 85 which states that “A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons... Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority...” The role of the supervisory authority in overseeing the mitigation of risks to data subjects is also evident from Recital 86 which states that communication of data breaches which are likely to pose a high risk to data subjects should be made by a controller to data subjects “as soon as reasonably feasible and in close co-operation with the supervisory authority, respecting guidance provided by it...”

- 14.16 TIC submitted, in its Submissions in relation to the Preliminary Draft, that *“To the extent there was an infringement under Article 33(1), it is correct that this might have delayed the assessment by the DPC. However, this did not have a practical impact on the affected data subjects, since the DPC did not take, or order TIC to take, any additional actions “...to protect and/or remedy the impact on” affected data subjects.”*²⁸⁰
- 14.17 In the Draft Decision, I noted that I accepted TIC’s submissions on this point. As I have set out above, in the context of my consideration of the number of data subjects affected and the level of damage suffered by them, I also noted in the Draft Decision that, whilst it cannot be definitively said that no users affected by the Breach were affected by the delayed notification, equally, there was no direct evidence of damage to them from the delayed notification. Accordingly, I decided, in the Draft Decision, that less weight should be attributed to this factor in my overall assessment of Article 83, than I had previously indicated was my provisional position in the Preliminary Draft.
- 14.18 In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.
- 14.19 In assessing the gravity of the infringement below, however, I have taken into account the fact that TIC had commenced remediation of the Breach by the time of the notification to the Commission.
- 14.20 As I stated on a provisional basis in the Preliminary Draft, non-compliance with Article 33(5) also interferes with the exercise by a supervisory authority of its oversight and enforcement functions. Where there is an absence, or a deficiency, in documenting a personal data breach, it may prevent or hinder the supervisory authority in making a complete assessment of the circumstances of a personal data breach for the purposes of considering the extent of a controller’s compliance with its specific obligations under Article 33 and whether corrective measures should be taken in relation to how the controller has behaved with regard to those particular obligations. However, significantly, at a more fundamental level, non-compliance with Article 33(5) may prevent a supervisory authority from considering the circumstances of the personal data breach in a holistic manner - including in relation to the extent of the controller’s compliance with other obligations under the GDPR, such as those relating to security measures under Articles 5(1)(f) and 32 - and assessing whether further supervisory activity beyond those issues relating purely to Article 33

²⁸⁰ Submissions in relation to the Preliminary Draft, para. 12.17

needs to be taken (for example, the exercise of investigatory or auditing powers). Importantly, Article 33(5) is also intrinsically linked to the principle of accountability under the GDPR, and compliance with this provision may be an important indicator of the extent to which a controller has implemented an appropriate GDPR compliance programme.

14.21 In the Submissions in relation to the Preliminary Draft, TIC submitted that it does not agree with the position outlined above - that a potential consequence of non-compliance with Article 33(5) is that it may hinder a supervisory authority *“from considering the circumstances of the personal data breach in a holistic manner, including in relation to the extent of the controller’s compliance with other obligations under the GDPR, such as those relating to security measures under Articles 5(1)(f) and 32.”*²⁸¹ In this regard, TIC submitted that this *“...expands the scope of verification which the documentation is expected to support..”*

14.22 I do not accept TIC’s submission in this respect. It is certainly the case that a controller’s failure to comply with the requirement to document a breach could, potentially, prevent a supervisory authority from identifying (and separately investigating) additional failures in the controller’s compliance with other provisions of the GDPR, such as those under Article 5(1)(f) and Article 32. This is, logically, a potential consequence of a controller’s failure to document a breach. My statement above, therefore, does not ‘expand the scope of Article 33(5)’ as a means of verifying compliance with other Articles of the GDPR, as TIC submitted. My position, in this regard, is that the very nature of the Article 33(5) obligation enables the facilitation of supervisory oversight which is at the cornerstone of the GDPR system of monitoring and enforcement. The occurrence of one or more personal data breaches may be indicative of systemic or serious compliance issues within a controller, and the breach notification system in the GDPR often acts as the springboard, alerting supervisory authorities to potential compliance issues and problems and risks to the data subject. Accordingly, non-compliance with the requirement to document the matters set out in Article 33(5) potentially stymies the supervisory authority’s investigation not only of the incident in question, but also the wider circumstances which may have given rise, whether in whole or in part, to the occurrence of the breach.

14.23 TIC further contended, in its Submissions in relation to the Preliminary Draft, that *“..the DPC’s assessment of the nature of the infringement errs in that it talks about the general consequences that could arise from an infringement of this type, rather than assessing the nature of this specific infringement....further information was not required to enable the DPC to consider “the circumstances of the personal data breach in a holistic manner.” The nature of the breach was evident from the information recorded by Twitter in the JIRA ticket and Incident Report.”*²⁸²

14.24 With regard to TIC’s criticism that the Preliminary Draft did not assess the nature of this specific infringement, I now address this issue – in other words, the nature of TIC’s failure in the

²⁸¹ Ibid, para 17.6

²⁸² Ibid, para. 17.7

circumstances of this particular incident to comply with the documenting requirement in Article 33(5). On this note, I do not agree with TIC's further point above that the nature of the Breach was evident from the information recorded in the JIRA ticket and the incident report. I have described above in detail, both in sections 9 and 10, how I have assessed the purported documenting of the Breach and found the information provided by TIC (including the JIRA tickets and the Incident Report) to have been deficient for the purposes of Article 33(5) and the objective of the Commission verifying compliance with Articles 33(1) to 33(4). I do not intend to repeat the assessment here, but I consider that my analysis of the various documents provided by TIC, in this regard, demonstrates the nature – and indeed the impact, insofar as the consequences of the infringement on the effective performance of supervisory functions are concerned – of this specific infringement by TIC.

14.25 Further, as noted in section 10 above, contrary to TIC's assertions that further information was not required to enable the Commission to consider the circumstances of the Breach in a holistic manner, the deficiencies of the documentation provided by TIC as a 'record' of the Breach are demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple queries in order to gain clarity concerning the facts and sequencing surrounding the notification of the Breach, in particular, in relation to the issue of when TIC (through the DPO) was notified of the Breach by Twitter Inc. and the facts surrounding this issue.

14.26 I therefore consider that the nature of the obligations arising under Article 33(1) and Article 33(5) 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. As such, non-compliance with these obligations has serious consequences in that it risks undermining the effective exercise by supervisory authorities of their functions under the GDPR. With regard to the nature of the specific infringements in these circumstances, it is clear, having regard to the foregoing, that in the circumstances of this case, the delayed notification under Article 33(1) inevitably delayed the Commission's assessment of the Breach. With regard to Article 33(5), the deficiencies in the "documenting" of the Breach by TIC impacted on the Commission's overall efficient assessment of the Breach, necessitating the raising of multiple queries concerning the facts and sequencing surrounding the notification of the Breach.

Gravity of the Infringement

14.27 In terms of the 'gravity' of the infringements, I have considered this in the context of the nature, scope and purpose of the processing that led to the Breach, as set out above. I have also considered the issue of 'gravity' in the context of the number of data subjects affected by the Breach. I set out below my view in relation to the issue of 'gravity' in respect of the infringements by TIC of Article 33(1) and 33(5), respectively.

Gravity of the infringement of Article 33(1)

14.28 As I have set out above, the GDPR imposes a requirement on controllers to address personal data breaches in a timely manner, including the notification of same, in order to mitigate the impact on affected data subjects. In this regard, Recital 85 provides that

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons.”²⁸³

The Breach Notification Guidelines further state, in this regard, that

“Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.”²⁸⁴

14.29 In this case, TIC has asserted that it was in compliance with Article 33(1) because it notified the Breach to the Commission within 72 hours of TIC becoming aware of it. As I outlined in the Preliminary Draft, I considered that this interpretation ignores the fact that TIC, as controller, was responsible for overseeing the processing operations carried out by its processor, Twitter Inc., and for ensuring that its own processor made it aware of any data breach in a manner that would allow TIC to comply with the 72 hour notification requirement in Article 33(1). My provisional view was that, in such circumstances, a controller cannot avoid its responsibility under Article 33(1) by seeking to hide behind the failure of a processor, which it has appointed, to notify it of a personal data breach in relation to the personal data for which the controller is responsible. Such an interpretation - 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 obligation in Article 33 on a controller.

14.30 In addition, as explained above and in the Preliminary Draft, one of the primary purposes of notifying a personal data breach to a supervisory authority is to enable consideration, by the supervisory authority, as to whether action needs to be taken to protect individuals affected by the breach (which may include a direction that a controller notify such individuals). The ability of a supervisory authority to take this step, and the provisions in respect of communication of a personal data breach to data subjects as set out in Article 33(4), would also be frustrated (and potentially rendered ineffective) were it the case that a controller’s obligation to notify a breach, under Article 33(1), was contingent upon the compliance by its processor with its obligations.

²⁸³ Recital 85, GDPR

²⁸⁴ Breach Notification Guidelines, page 13

- 14.31 In its Submissions in relation to the Preliminary Draft, TIC submitted that “[it] *had not sought to hide behind any delays of its processor or evade responsibility, but rather to follow its existing, effective breach notification processes to apply an interpretation of ‘awareness’ that is in line with the Breach Notification Guidelines.*”²⁸⁵
- 14.32 I accept that TIC may not have deliberately sought to evade responsibility under Article 33(1) by seeking to excuse its own delayed notification of the Breach on the basis of its processor’s delay. However, and as I have set out above in section 7, I do not accept TIC’s proposed interpretation of Article 33(1), 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).
- 14.33 In terms of this particular case, any assessment of the gravity of the infringement must necessarily take account of how it interfered with the overall purpose of notifying a personal data breach to the supervisory authority. In this case, there was a delay (of two days) in notifying the Breach to the Commission which, in turn, delayed the assessment by the Commission of the Breach and its potential impact. (The length of this delay has also been considered below in the context of the duration of the infringement). As I have set out above, I accept, however, that, despite the potential for damage to data subjects arising from the potential for consequent delays in actions taken by the Commission to safeguard / mitigate risks to data subjects, as matters actually materialized, there was no direct damage to data subjects arising from the delayed notification.
- 14.34 In the Draft Decision, I outlined that I considered this factor to be relevant to my overall assessment of gravity concerning the infringement of Article 33(1). In accordance with the binding direction in the EDPB Decision, at paragraph 207 thereof, however, and having particular regard to the comments of the EDPB at paragraphs 186, 187 and 198 of the EDPB Decision, I have reassessed this issue and, in particular, the weight to be attributed to it in my overall assessment of Article 83. In this regard, notwithstanding that there was no direct evidence of damage to data subjects, as I have outlined above at paragraph 14.4, I have attributed a greater weighting to the nature and scope of the processing concerned and, in particular, the fact that the processing concerned involved communications by data subjects who deliberately chose to restrict the audience of those communications. The reassessment of this factor is reflected below as part of my overall consideration of Article 83(2) and is also reflected in the level of the administrative fine imposed in this Decision.
- 14.35 Furthermore, whilst TIC had commenced remediation of the Breach by the time of the notification to the Commission, I must, in assessing the gravity of the infringement in this case, be cognizant of the fact that the remedial measures by TIC were limited to forward looking action to close down the bug which was the root cause of the Breach. (These issues are also relevant to my consideration of the factors at Articles 83(2)(c) and (k), but I have dealt with them substantively in relation to the issue of gravity). Insofar as the impact on data subjects is concerned, as detailed herein, it appears

²⁸⁵ Submissions in relation to the Preliminary Draft, para. 12.18

that TIC did not carry out a backward looking analysis to identify the risks to data subjects arising from the Breach.

- 14.36 In its Submissions in relation to the Preliminary Draft, TIC submitted, in respect of my assessment above regarding its failure to have conducted a backward looking analysis to identify the risks to data subjects arising from the Breach, that “[the] DPC did not raise any queries with TIC about the extent of TIC’s backward analysis during its inquiry.”

TIC further submitted that “...the nature of tweets is such that the essential impact of making a protected tweet public was obvious to the experienced security and legal team involved in managing the Underlying Bug, and did not require extensive analysis....Given this, the lack of a lengthy backward looking analysis should not be considered to be a factor aggravating the impact of an alleged delay in notification.”²⁸⁶

- 14.37 I do not accept TIC’s submission to the effect that no query was raised by the Investigator regarding ‘the extent of TIC’s backward looking analysis’ in circumstances where, during the course of the Inquiry, the Investigator made two separate requests that TIC provide it with documentary evidence of its risk assessment conducted in respect of the Breach. As detailed herein, TIC did not provide any such evidence of its risk assessment, either during the course of the Inquiry or as part of its Submissions in relation to the Preliminary Draft.

- 14.38 TIC also contended in its Submissions in relation to the Preliminary Draft²⁸⁷ that, given the nature of the bug, it was obvious to the Information Security team “.that no remedial action was available beyond ensuring the “private” status of the tweets was restored and notifying the impacted individuals”. Whilst this may be the case, Article 33(1) requires a controller to conduct an assessment of risk posed by a personal data breach, and in this case, it appears (based on the lack of documentary evidence retained by TIC) that no formalised assessment of the risk was carried out. In particular, and as set out above in section 10, in failing to carry out any form of risk assessment by reference to some form of analysis of the categories of personal data impacted, this suggests that TIC did not establish the true impact(s) of the Breach on its users. This is clearly contrary to the objectives of Article 33(1) and, indeed, the overall legislative intent that informs the GDPR.

In this regard, therefore, whilst I accept TIC’s submission in its Submissions in relation to the Preliminary Draft that it was evident, upon assessment of the bug, that no other remedial action (other than that taken) was required, I find TIC’s apparent failure to carry out any formal risk assessment to increase the gravity of the circumstances of the infringement.

²⁸⁶ Submissions in relation to Preliminary Draft, para. 12.21

²⁸⁷ Ibid, para. 12.21

14.39 Finally, in assessing the ‘gravity’ of the infringement under Article 33(1), I have noted the submission by TIC, in respect of the delays that arose during the timeline of the notification, that it

“...believes that this was an isolated breakdown of the Twitter Inc. response process, and the Global DPO would typically be involved at the earliest stages of the Twitter Inc., response process...”²⁸⁸

I have also noted similar contentions in this regard made by TIC in its Submissions in relation to the Preliminary Draft²⁸⁹.

14.40 Whilst I do 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, I have, however, taken account below (in my application of Article 83(2)(d)) of the isolated nature of the incident. (As I set out below, in considering TIC’s Submissions in relation to the Preliminary Draft, I have departed from the provisional view set out in the Preliminary Draft that the Breach was indicative of a broader, more systemic issue.)

Gravity of the infringement of Article 33(5)

14.41 In considering the gravity of the infringement of Article 33(5) in this case, I have had particular regard to the overall objective of Article 33, which is to ensure timely notification of a personal data breach to a supervisory authority. The primary purpose of this is to enable assessment by the supervisory authority of the breach, and its impact on affected data subjects.

Whilst a failure by a controller to ‘document’ a breach may not directly impact upon data subjects affected by the breach, proper documentation of breaches is required in order to enable a supervisory authority to verify the controller’s compliance with Article 33.

14.42 In its Submissions in relation to the Preliminary Draft, TIC submitted that *“The documentation kept by TIC did not hinder the assessment of the impact of the Underlying Bug.”²⁹⁰* In this regard, TIC took issue with the statement in the Preliminary Draft²⁹¹ to the effect that

“A failure by a controller to document a breach in accordance with the requirements of Article 33(5) ...will hinder any assessment of the breach carried out by the relevant supervisory authority.”

14.43 I have already considered above the impact of the deficiencies in the “documenting” of the Breach by TIC on the Commission’s overall efficient assessment of the Breach, necessitating the raising of multiple queries concerning the facts and sequencing surrounding the notification of the Breach. I

²⁸⁸ Submissions dated 1 February 2019

²⁸⁹ There are 11 references to this being an isolated failure/ isolated error/ isolated instance throughout the Submissions in relation to the Preliminary Draft

²⁹⁰ Submissions in relation to the Preliminary Draft, para 17.9

²⁹¹ Preliminary Draft, para.15.13

therefore do not accept that, in this case, the documentation kept by TIC did not hinder the assessment of the impact of the underlying bug. To the contrary, this hindered the Commission in seeking to clarify the facts in relation to TIC's notification of the Breach and, in particular, the reasons for the delay in Twitter Inc. notifying TIC of the Breach. As is outlined herein, this was evidenced by the fact that, during the course of the Inquiry, the Investigator was required to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

14.44 In its Submissions in relation to the Preliminary Draft, TIC made submissions (in relation to both Article 33(1) and Article 33(5)), in respect of the provisional assessment of the infringement in the Preliminary Draft, as 'moderately serious'.

14.45 In this regard, with regard to the infringement under Article 33(1), TIC stated as follows:

*"At most, the delay in notification, based on the DPC's interpretation of "awareness" was two days. To categorise this as "moderately serious" is manifestly excessive. The DPC is basing its assessment on the concerns it has raised in relation to obligations arising under other Articles of the GDPR which do not form part of the infringement being assessed."*²⁹²

As has already been set out above, I do not accept TIC's submission to the effect that my assessment of its compliance with Article 33(1) is based on "...concerns it has raised in relation to obligations arising under other Articles of the GDPR which do not form part of the infringement being assessed."

14.46 With regard to my provisional assessment in the Preliminary Draft of TIC's infringement of Article 33(5) as 'moderately serious', TIC submitted, in its Submissions in relation to the Preliminary Draft, as follows:

*"TIC's documentation was designed to record the key elements of a breach identified by the Breach Notification Guidelines: the details of the breach, the effects and consequences of the breach, and the remedial action taken by the controller. Its understanding was that Article 33(5) did not require it to document the facts around notification. Any deficiencies in this area arose from a misunderstanding in good faith of what the requirements were. TIC submits that this does not reach the threshold of being moderately serious, and it is not appropriate to impose a fine on this basis."*²⁹³

14.47 Whilst I accept TIC's submission to the effect that the deficiencies in its documentation of the Breach arose from a misunderstanding "in good faith" as to what the requirements were, I consider that, as already set out above, the requirements on a controller to document a breach are clear from the wording of Article 33(5).

²⁹² Submissions in relation to the Preliminary Draft, para 12.19

²⁹³ Ibid, para. 17.11

- 14.48 I have set out below, with regard to the factor under Article 83(2)(b), that I consider TIC's infringement of Article 33(5) to have a negligent character. In this regard, I note that the EDPB Decision (at paragraph 195 thereof) provides that the negligent nature of the infringement "*implies an additional element to take into consideration in the analysis of the gravity of the infringement*". As per the EDPB Decision, this arises in circumstances where "*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.*" Having regard to this statement by the EDPB and, in accordance with the binding direction as set out at paragraph 207 of the EDPB Decision, I have taken account of the negligent nature of the infringement in these circumstances as part of my overall assessment of the gravity of the infringement under Article 33(5).
- 14.49 Having regard to all of the matters dealt with above, and having taken account of TIC's submissions in relation to the Preliminary Draft, I confirmed in the Draft Decision that my assessment of the gravity of the infringements of Article 33(1) and Article 33(5) was that they were at the low to moderate end of the scale of gravity. In doing so, I noted in the Draft Decision that I had revised my initial assessment of the gravity of these infringements downwards from that which was set out in the Preliminary Draft, where I had outlined that I considered them to be moderately serious.
- 14.50 In assessing the gravity of the infringements for the purpose of this Decision, however, I am required to have regard to the EDPB Decision, and in particular, to the binding direction at paragraph 207 therein, that the Commission "*...reassess the elements it relies upon to calculate the amount of the fixed fine to be imposed on TIC.*" In this regard, I have also taken account of the comments of the EDPB, at paragraph 198 of the EDPB Decision, to the effect that the Commission "*should have given greater weight to the element relating to the nature, scope and negligent character of the infringement.*" I have also taken account of the comments of the EDPB, set out in the EDPB Decision at paragraphs 182 to 197 thereof, and in which the EDPB has set out its reasons as to why greater weight should be accorded to these elements.
- 14.51 Accordingly, and as I have set out above, I have reassessed these elements (which arise under Articles 83(2)(a) and 83(2)(b)) as required by the binding direction of the EDPB. I have also taken account of these elements, as reassessed in accordance with the EDPB Decision, as part of my overall assessment of the gravity of the infringements. In this regard, I consider it appropriate to determine the level of gravity, in respect of both the infringements under Article 33(1) and 33(5), as being moderately serious in nature.

Duration of the Infringement

- 14.52 In respect of the duration of the infringement, I have again considered this separately in respect of Article 33(1) and Article 33(5), and as set out below:

Duration of the infringement of Article 33(1)

14.53 In terms of assessing the duration of the infringement of Article 33(1), I have had regard to the fact that had the process in place between TIC (as controller) and Twitter, Inc. (as its processor) been followed as it should have been, TIC would have been aware of the Breach at an earlier point in time. Specifically, I consider that TIC ought to have been aware of the Breach at the latest by 3 January 2019, when the Twitter, Inc. legal team assessed the Breach and instructed that an incident be opened. I therefore consider that, notwithstanding TIC's 'actual awareness' of the Breach on 7 January 2019, TIC had constructive awareness of the Breach on 3 January 2019, which is the date on which Twitter Inc. identified the incident as being likely to comprise a reportable personal data breach.

14.54 I therefore consider that the infringement of Article 33(1) commenced on the expiration of 72 hours from 3 January 2019 (i.e. on 6 January 2019) and ended at the time of TIC's notification of the Breach to the Commission on 8 January 2019 (at 18:08).

14.55 I therefore consider the duration of the infringement in respect of Article 33(1) to be a period of two days. In this regard, while on the one hand, it could be considered in a general context that an infringement lasting two days ranks at the low end of the temporal spectrum, I must consider this timeframe relative to the overall breach notification system in the GDPR. In this context, I consider it relevant to look at the two-day delay in light of the overall timeframe generally permitted for breach notifications i.e. 72 hours or three days. As such, the two-day delay is more than half the time again of the period permitted for notification of breaches. Accordingly, I do not consider the two-day delay to be a trivial or inconsequential one.

Duration of the infringement of Article 33(5)

14.56 In the Preliminary Draft, I found on a provisional basis that TIC's failure to 'document' the Breach extended from 3 January 2019, being the date on which Twitter Inc. identified the incident as being likely to comprise a personal data breach, up to the present date - in other words, that it was an ongoing infringement.

14.57 In its Submissions in relation to the Preliminary Draft, TIC made a number of submissions concerning my assessment that the duration of the infringement under Article 33(5) is ongoing. In this regard, TIC referred to the *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679* ('Administrative Fines Guidelines'), which outlines that "*Duration of the infringement may be illustrative of, for example ... wilful conduct on the data controller's part, or ... failure to take appropriate preventative measures.*"²⁹⁴

²⁹⁴ Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, page 11

TIC further submitted that:

*“The DPC’s primary criticism of the documentation is that it did not enable the Investigator to determine when TIC became aware of the Underlying Bug...The Inspector clearly considered that only contemporaneous documentation would be acceptable to verify TIC’s compliance. Given this, it is not possible for TIC to end the alleged infringement of Article 33(5) in this case, so the alleged infringement is not indicative of wilful conduct on TIC’s part. It is also not indicative of a failure to take appropriate preventive measures.”*²⁹⁵

14.58 I do not consider that TIC’s failure to comply with Article 33(5) amounted to intentional or wilful conduct on its part. However, I do consider that it is evidence of negligent conduct on the part of TIC, insofar as it failed to ensure that it complied with the requirements of Article 33(5). I continue to be of the view that the infringement is continuing – and this arises as TIC continues to maintain that there is no deficiency in its documenting of the Breach and, therefore, has not taken steps to remediate these deficiencies. In this regard, I consider that it would have, at any point, been possible (including right up to and including the current point in time) for TIC to remedy the deficiencies in the documentation which it is required to maintain pursuant to Article 33(5) and therefore draw a close to the continuing nature of the infringement. Such remediation would not, however, erase the fact that an infringement of Article 33(5) had been ongoing during the intervening period between TIC first being alerted to the Breach and the remediation of the deficient documentation.

14.59 **For all of the above reasons, I therefore consider the duration of the infringement in respect of Article 33(5) to be an ongoing one.**

Article 83(2)(b) - The intentional or negligent character of the infringement

14.60 In respect of the criterion (at Article 83(2)(b)), the Administrative Fines Guidelines’ state that

*“In general, “intent” includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas “unintentional” means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.”*²⁹⁶

The Administrative Fines Guidelines go on to distinguish between circumstances that are indicative of ‘intentional breaches’ and those that are indicative of breaches occasioned by unintentional, or negligent, conduct. In this regard, the Guidelines cite *“failure to read and abide by existing policies”* and *“human error”* as being examples of conduct that may be indicative of negligence.²⁹⁷

²⁹⁵ Submissions in relation to the Preliminary Draft, para. 17.13 and 17.14

²⁹⁶ Administrative Fines Guidelines, page 11

²⁹⁷ Ibid, page 12

14.61 In the Preliminary Draft, I stated on a provisional basis that, while I had seen no evidence of an intentional infringement on TIC's part, I found, in respect of both Articles 33(1) and 33(5) that the infringements of these provisions arose due to negligence on the part of TIC. In its Submissions in relation to the Preliminary Draft, TIC objected to these provisional findings on both articles.

Negligence in respect of the Article 33(1) infringement

14.62 In the Preliminary Draft (at paragraph 16.3 thereof), I outlined my view that, having taken account of the delays that had arisen during the course of the timeline leading to notification of the Breach to the Commission, I was of the view this was "... indicative of a broader, more systemic issue."²⁹⁸

In its Submissions in relation to the Preliminary Draft, TIC outlined that

*"The DPC considers that the delay in notification was negligent on TIC's part primarily because "there were multiple delays throughout that process" and "in so far as [TIC's] agreed protocols with its processor did not operate as intended" this was indicative of negligence. This is factually inaccurate....there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process."*²⁹⁹

14.63 As set out above, I accept TIC's submission that Contractor 2's notification to Twitter Inc. of the bug on 29 December 2018, having received the bug report on 26 December 2018, was within the temporal service level stipulated in its contract with Twitter Inc. However, as set out above in detail, and for the reasons set out in section 7, I do not consider that the 4-day intervening period between the Information Security team at Twitter, Inc. receiving the JIRA ticket from Contractor 2 on 29 December 2018 and actually reviewing it on 2 January 2019 was reasonable. As such, I continue to consider that this constituted a delay in the overall chronology of the Breach.

14.64 As set out above, in essence, TIC has acknowledged that Twitter Inc.'s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled 'Escalation to Legal' was not completed as prescribed. Step 5 of the protocol was, essentially, a combined step requiring that certain named members of the Twitter Inc. legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added to the Incident and Investigation tickets. TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

²⁹⁸ Preliminary Draft, para. 16.3

²⁹⁹ Submissions in relation to the Preliminary Draft, para 12.23

14.65 TIC stated in its Submissions in relation to the Preliminary Draft that:

“The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate.”³⁰⁰

14.66 As I have set out above in section 7, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team as to who had been informed of the issue when the legal team were already involved, and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single, composite step entitled ‘*Escalation to Legal*’.

14.67 I am not satisfied that the DART Runbook, at the relevant time, was as clear as it could have been in spelling out that (a) separate notifications of the incident in question were required to be made to inform both the legal team and the DPO; and (b) notwithstanding the extant involvement of the legal team, steps should additionally have been taken to ensure that the TIC DPO, and thereby TIC (as controller), was also notified of the incident. This is borne out, in my view, by the explanation provided by TIC, as to why there was a deviation by the DART team from the protocol at this crucial point. It is also borne out by the very fact that TIC has, since the Breach, amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to “...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly”.³⁰¹ In my view, this amendment, and TIC’s comments in respect of same, are indicative of TIC’s own assessment of a lack of clarity in this part of the Runbook. However, for the avoidance of any doubt, this is solely by way of observation, and I am making no finding (nor should any inference of a finding be assumed), in relation to TIC’s compliance with Article 24 and/or Article 32.

14.68 I have, however, taken account of TIC’s submission, in its Submissions in relation to the Preliminary Draft, in respect of the broader technical and organisational measures which it had in place at the time of the Breach. Having considered these factors, and the submissions by TIC to the effect that the failure to follow the DART Runbook Step 5 was an isolated failure³⁰², I have departed from my

³⁰⁰ Submissions in relation to the Preliminary Draft, para 6.6

³⁰¹ Ibid, para 5.17

³⁰² Submissions in relation to the Preliminary Draft, for example, para 12.23 where TIC submitted that “...there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process.”

provisional view (as expressed in the Preliminary Draft) that the issues that arose were indicative of a broader systemic issue. I accept TIC's submission that its delayed notification of the Breach was an isolated occurrence and was not, therefore, indicative of any broader systemic issues. However, I remain of the view that the delay in TIC being made aware of the Breach, in this particular instance, arose as a result of negligence on the part of TIC (as controller), insofar as the protocol agreed with its processor in the form of the DART Runbook was not followed as it should have been at the relevant time.

14.69 **In the circumstances, I consider that there was a negligent character to TIC's infringement of Article 33(1).**

14.70 For completeness, I have identified no evidence of intentional conduct with regard to TIC's commission of the infringement under Article 33(1).

Negligence in respect of the Article 33(5) infringement

14.71 In respect of TIC's infringement of Article 33(5), I do not consider that there was 'intent' on the part of TIC to breach this provision in the sense that there was 'knowledge' and 'wilfulness'³⁰³ on the part of TIC to cause the infringement.

14.72 In the Preliminary Draft, I expressed my provisional view that the infringement of Article 33(5) arose as a result of negligent conduct by TIC. This was primarily because the documentation maintained by TIC in respect of the Breach did not record important key information concerning the facts and effects of the Breach and, in particular, concerning the notification of the Breach. I considered that this was demonstrated by the fact that, during the course of the Inquiry, the Investigator had to raise multiple rounds of queries to establish the facts relating to the timeline for the notification of the Breach.

14.73 In its Submissions in relation to the Preliminary Draft, TIC submitted that:

*"Its documentation process was developed in good faith based on the wording of Article 33(5) and the [Breach Notification Guidelines] at the time. It was based on an understanding that the verification element related to verification of decisions by controllers not to notify. This was a reasonable approach to take at the time, given that this was a new requirement and everyone's understanding of the requirements was evolving. Therefore, its behaviour did not meet the standard required for negligence."*³⁰⁴

³⁰³ Administrative Fines Guidelines, page 11 – "In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."

³⁰⁴ Submissions in relation to the Preliminary Draft, para. 17.16

While I am not questioning TIC's good faith in this regard, I nevertheless do not accept TIC's submission in circumstances where, as already outlined, the requirements for documenting a personal data breach are clearly stated in Article 33(5); and in circumstances where I find that TIC, in documenting the Breach, did not maintain a record, specifically, of a personal data breach and, furthermore, its documentation was not sufficient to enable its compliance with Article 33 to be verified.

14.74 **In the circumstances, I consider that there was a negligent character to TIC's infringement of Article 33(5).**

14.75 In this regard, I also take into account the comments in the EDPB Decision (at paragraph 195 thereof) to the effect 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"* and that *"[t]his element implies an additional element to take into consideration in the analysis of the gravity of the infringement."*³⁰⁵

14.76 As I have set out above, having regard to this statement by the EDPB and, in accordance with the binding direction set out at paragraph 207 of the EDPB Decision, I have taken account of the negligent nature of the infringement under Article 33(5) as part of my overall assessment of the gravity of the infringement.

Article 83(2)(c) - Any action taken by the controller or processor to mitigate the damage suffered by data subjects

14.77 In considering this criterion, I have had regard to the fact that, notwithstanding the delay in commencing its assessment of the bug once it had been notified of same by Contractor 2, Twitter Inc. engaged in activity to fix the bug and, therefore, attempted to mitigate the damage suffered by data subjects generally by ensuring that there would not be any further repetition of this issue. I note, in this regard, that TIC has outlined the measures taken by Twitter Inc., between 3 January 2019 and 14 January 2019, to fix the bug.³⁰⁶

14.78 I also note that TIC has stated that Twitter Inc., at the direction of the Global DPO, issued a public notice to notify affected users on 17 January 2019. (I note that, while, based on the initial Breach Notification Form, it was not TIC's intention to issue such a notice, following the submission of same to the Commission on 8 January 2019, TIC subsequently stated that it would do so in its Updated Breach Notification Form of 16 January 2019). With regard to the issue of the public notice, I have regard to the fact that TIC has confirmed that

³⁰⁵ EDPB Decision, paragraph 195

³⁰⁶ Submissions of, inter alia, 25 January 2019, 1 February 2019

“..while TIC believes that people who were impacted by this issue would have immediately realized that their account had been unprotected by virtue of the disappearance of the “lock” from their account profile...and thus would have been able to immediately reprotect their account should they have chosen, TIC decided to provide notice to impacted persons upon becoming aware of this issue.”³⁰⁷

- 14.79 In the Preliminary Draft I expressed the provisional view that, in circumstances where, as set out above, TIC did not furnish any evidence as to how it assessed the risk arising from the Breach, it was not possible to ascertain whether the publication of the notice by TIC was carried out in furtherance of its obligation under Article 34 (*‘Communication of a Personal Data Breach to the Data Subject’*). I further stated that, in the event that TIC had assessed the Breach as being *“likely to result in a high risk”* to data subjects, such that the obligation to notify data subjects under Article 34 is triggered, then the issuing by it of a public notice would not amount to a mitigating factor, given that it was carried out by TIC in furtherance of its obligation as a controller under Article 34, rather than as a voluntary additional remedial measure.
- 14.80 In its Submissions in relation to the Preliminary Draft, TIC submitted that I was incorrect to conclude, as set out above, that if TIC issued the public notice on foot of its statutory obligation to do so under Article 34, this would not amount to a mitigating factor.

TIC refers, in this regard, to the Administrative Fines Guidelines, which refer to *“timely action taken by the data controller / processor to stop the infringement from continuing...”* as being an example of a mitigating action.

The Administrative Fines Guidelines also state, on this point, that

“[Article 83(2)(c)] acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/negligent approach but where they have done all they can to correct their actions when they become aware of an infringement. Regulatory experience...has previously shown that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions.”³⁰⁸

- 14.81 The above clearly indicates that, for an action carried out by a controller to be considered as a mitigating factor, it must be a voluntary remedial action, whereby the controller takes ‘responsibility to correct or limit the impact of their actions’. An action, taken by a controller where it is mandated to do so on foot of a statutory obligation cannot be viewed as a mitigating factor.

³⁰⁷ Submissions dated 1 February 2019, Annex, para 11

³⁰⁸ Administrative Fines Guidelines, page 12, 13

14.82 In its Submissions in relation to the Preliminary Draft, whilst TIC submitted that its issuance of the public notice should be deemed to be a mitigating factor, it does not furnish any evidence or explanation as to whether this action was taken on foot of its obligations under Article 34 or otherwise. Therefore, in the continued absence of evidence as to how TIC assessed the risk to affected users, it is not possible to determine whether the publication of the notice comprises a mitigating factor.

14.83 **Based on the foregoing, I consider that the steps taken by Twitter Inc., to rectify the bug are the sole mitigating factor in assessing the amount of the administrative fine to be imposed.**

Article 83(2)(d) - The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

14.84 As I have set out above, the GDPR imposes a requirement on controllers to address personal data breaches in a timely manner, including the notification of same, in order to mitigate the impact on affected data subjects. In this regard, Recital 85 provides that

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons.”³⁰⁹

The Breach Notification Guidelines further state, in this regard, that

“Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.”³¹⁰

14.85 As set out above in section 6, the obligations on a controller in terms of notifying a personal data breach under Article 33(1), 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 governed by Article 28; and the obligation to implement appropriate (and effective) technical and organisational measures, in accordance with Articles 24 and 25 and, in particular, Article 32 GDPR.

14.86 As set out above, in essence, TIC has acknowledged that Twitter Inc.’s delay in notifying the DPO (and, thereby TIC) occurred because Step 5 of its protocol (the DART Runbook), entitled ‘*Escalation to Legal*’ was not completed as prescribed. Step 5 of the protocol was, essentially, a combined step requiring that certain named members of the Twitter Inc., legal team be made aware of the issue (by adding them to the Incident and Investigation tickets) **and** that the TIC DPO be also added

³⁰⁹ Recital 85, GDPR

³¹⁰ Breach Notification Guidelines, page 13

to the Incident and Investigation tickets. TIC has stated (both during the Inquiry and in its Submissions in relation to the Preliminary Draft) that this step was not completed in circumstances where, because the Twitter Inc. legal team was already involved at this point in the process, the DART team *assumed* that this step, including the requirement to notify the DPO (and, therefore TIC as controller), had been satisfied.

14.87 In the Preliminary Draft, I noted that TIC had admitted that delays had occurred in both the initial assessment of the incident giving rise to the Breach and in its notification to the Commission. These delays arose, as confirmed by TIC, as a result of a deviation from, or failure to follow, agreed processes by its processor, Twitter Inc., and by a third party (Contractor 2), and in the case of one delay, as a result of *“the winter holiday schedule.”*³¹¹ I therefore concluded, on a provisional basis, that it appeared to be the case that the measures were not effective, in this instance, as they did not operate as they were intended to.

14.88 In its Submissions in relation to the Preliminary Draft, TIC submitted that

*“The processes which TIC had in place with Twitter Inc. were appropriate to ensure regulators were notified promptly of data breaches in accordance with Recital 87 and Article 33(1) GDPR. An isolated failure to follow a process on one occasion, when the same process has been followed successfully on several previous occasions, does not demonstrate that the process itself is not appropriate.”*³¹²

14.89 As I have set out in section 7, I cannot draw any conclusions as to the specific circumstances in which the DART team made the assumption it did, whereby it formed the view that Step 5 of the protocol had been completed in circumstances where the Twitter Inc. legal team were already involved. However, having re-examined the DART Runbook in light of the explanation provided by TIC (and as again set out in its Submissions in relation to the Preliminary Draft), I accept that confusion could have arisen on the part of the DART team as to who had been informed of the issue when the legal team were already involved, and in circumstances where the direction to notify members of Twitter Inc.’s legal team and the TIC DPO was contained in one single, composite step entitled *‘Escalation to Legal’*.

In this regard, and as I set out above, I am not satisfied that, as submitted by TIC in its Submissions in relation to the Preliminary Draft, the DART Runbook, as it was at the relevant time, was as clear as it could have been in spelling out that separate notifications of the incident in question were required to be made to inform both the legal team **and** the DPO, and that, notwithstanding the

³¹¹ Submissions dated 25 January 2019, Annex, footnote 3: *“This 4-day delay appears to have been a deviation from the agreed upon process between Twitter and Contractor 2. We are investigating the cause for this and it will be part of our post mortem process”*.

³¹² Submissions in relation to the Preliminary Draft, para 6.6

extant involvement of the legal team, steps should additionally have been taken to ensure that the TIC DPO, and thereby TIC (as controller), was also notified of the incident.

- 14.90 This is borne out, in my view, by the explanation provided by TIC, as to why there was a deviation by the DART team from the protocol at this crucial point. It is also borne out by the very fact that TIC has, since the Breach, amended the DART Runbook in respect of this step (to notify the DPO and, therefore TIC as controller) in order to “...make it clearer when the Information Security team were required to tag the Office of Data Protection to ensure that TIC is notified promptly”.³¹³ In my view, this amendment, and TIC’s comments in respect of same, are indicative of TIC’s own assessment of a lack of clarity in this part of the Runbook. However, for the avoidance of any doubt, this is solely by way of observation, and I am making no finding (nor should any inference of a finding be assumed) in relation to TIC’s compliance with Article 24 and/or Article 32.
- 14.91 I have, however, taken account of TIC’s submission, in its Submissions in relation to the Preliminary Draft, in respect of the broader technical and organisational measures which it had in place at the time of the Breach. I note that these have been detailed as including biennial third party assessments of Twitter’s security program, together with formal risk assessment of information security practices, and the existence of a security committee meeting quarterly to review the effectiveness of the security program³¹⁴.
- 14.92 As referred to above, having considered these factors, and the submissions by TIC to the effect that the failure to follow the DART Runbook Step 5 was an isolated failure³¹⁵, I have departed from my provisional view (as expressed in the Preliminary Draft) that the issues that arose were indicative of a broader systemic issue. I have also taken account of the enhancement measures implemented by TIC in respect of its processes following the Breach. In this regard, TIC has confirmed that it has now amended the DART Runbook to make it clearer as to when the Information Security team is required to tag the Office of Data Protection to ensure that TIC is notified promptly. I also note, in this regard, that TIC has stated that Twitter Inc. has since provided additional training to its Information Security team that receives such reports from Contractor 2 to ensure that they are “*...better able to identify issues that are not security related but may be privacy / data protection issues*”. I further note that TIC has confirmed that this training also highlighted the importance of mentioning the DPO team (therefore TIC (as controller)) in the JIRA ticket so that the DPO team receives email notices in respect of the issue.³¹⁶
- 14.93 In its Submissions in relation to the Preliminary Draft, TIC expressed concerns regarding the weighting to be given to this criteria and emphasized that any weighting under this should not

³¹³ Submissions in relation to the Preliminary Draft, para 5.17

³¹⁴ Ibid, para 12.33

³¹⁵ Submissions in relation to the Preliminary Draft, for example, para 12.23 where TIC submitted that “*...there were not multiple delays in the process; there was a single, isolated failure to follow part of the agreed internal process.*”

³¹⁶ Submissions in relation to the Preliminary Draft, para 5.17

include a view of the effectiveness of TIC's measures overall as these have not been properly examined.³¹⁷ As I have noted above, my consideration of this criterion is simply that, and should not be confused with an assessment of compliance with Article 24, 25 and/or 32, which is outside the scope of this Inquiry and which I make no findings of any kind in relation to. For the purpose of assessing this criterion, I must assess the degree of responsibility taken by TIC in relation to technical and organizational measures implemented by TIC under Articles 25 and 32. In this regard, I have noted above, the existing and enhanced technical and organizational measures applied by TIC, including the amendments to the DART Runbook and the staff training measures. I also note, more generally, the existence of the internal structures and safeguards concerning responsibility for information security issues and the existence of a recurring external third party expert audit in this regard.

- 14.94 I should also note that, in its Submissions in relation to the Preliminary Draft, TIC emphasised its *"track record with regard to breach notifications generally"*³¹⁸ and points to *"the fact that in seven previous incidents TIC had submitted notifications of the incident without undue delay and within 72 hours of its processor Twitter, Inc. becoming aware of the incident."*³¹⁹ However, I consider that these issues amount to an assertion without being evidenced, and to verify same would involve an examination which is outside the scope of this Inquiry.
- 14.95 Having regard to the above, in circumstances where I am persuaded that there was not a broader systemic issue, and that, based on the high level evaluation of technical and organisation measures which I have conducted for the purpose of this criterion, TIC has demonstrated a generally responsible and accountable approach towards data security, I consider that the isolated failure of the protocol between it and its processor does not merit a significant or even a moderately negative weighting to be attributed under this criterion. However, despite the isolated nature of the incident underlying the Breach, I cannot discount this criterion completely, given that the DART Runbook, as it was at the relevant time, did not appear to have been as clear as it could have been (in light of the confusion that arose in respect of the failure to notify the DPO) in spelling out that separate notifications of the incident in question were required to be made to inform both the legal team and the DPO. As noted above, I consider that the subsequent amendment of the Runbook, and TIC's comments in respect of same, are indicative of TIC's own assessment of a lack of clarity in this part of the Runbook.

Accordingly, I consider that there has been a moderate to high level of responsibility demonstrated by TIC in the context of this criterion.

³¹⁷ Ibid, para 12.32

³¹⁸ Ibid, para 5.2 amongst other references

³¹⁹ Ibid, para 7.6

Article 83(2)(e) - Any relevant previous infringements by the controller or processor

14.96 The criterion at Article 83(2)(e) is not applicable in this case.

Article 83(2)(f) - The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

14.97 In the Preliminary Draft, I noted, under this factor, that TIC had cooperated fully with the Commission's investigation but that, as a statutory obligation, such cooperation did not constitute a mitigating factor in and of itself. I further noted that consideration of the extent of TIC's cooperation with the Commission in order to remedy the infringement and mitigate possible adverse effects of the infringement does not arise here, as the underlying bug, which was the root cause of the Breach, was in the process of being remedied by the time notification to the Commission took place.

14.98 In its Submissions in relation to the Preliminary Draft, TIC submitted that *"TIC went beyond its statutory duty to co-operate in the transparency of its responses, and the level of information it provided...[and] This should be treated as a mitigating factor."*³²⁰

TIC further submitted, in this respect, that during the course of the Inquiry, it had offered to provide an affidavit to confirm certain information and that *"[this] offer went beyond its statutory duty to cooperate."*³²¹

14.99 Whilst I acknowledge that TIC did cooperate fully, I do not accept TIC's submission in this respect in circumstances, where as outlined above, TIC was statutorily obliged to cooperate, pursuant to, amongst other provisions, Article 31 GDPR. Furthermore, I consider that TIC's offer to provide information by way of affidavit arose in circumstances where the documentation which it had maintained in relation to the Breach was deficient and, by its own admission³²², it was unclear from its notification when it had become aware of the underlying bug and that it could not provide any timestamped evidence of this in circumstances where the TIC DPO had been notified orally. As TIC expressly stated in its Submissions in relation to the Preliminary Draft, it offered to provide an affidavit as proof of the point in time at which TIC had become aware of the Breach. I note that this occurred against a backdrop where the investigator had stated in his Draft Report that he was not satisfied that there was compliance by TIC with Article 33(1). Accordingly, it is clear that the purpose of the affidavit was provided with TIC's own interests in mind, given the potential for the investigator to reach a final provisional view that TIC had not complied with Article 33(1).

³²⁰ Submissions in relation to the Preliminary Draft, para 12.35

³²¹ Ibid, para 17.20

³²² Ibid, para 15.3

14.100 Therefore, I remain of the view that TIC's cooperation during the Inquiry is not a mitigating factor.

Article 83(2)(g) - The categories of personal data affected by the infringement

14.101 In the Preliminary Draft, I indicated my provisional view that, whilst the nature and categories of the personal data affected had not been confirmed by TIC, it was reasonable to operate on the basis that some of the personal data involved in the Breach constituted special categories of personal data. In this regard, I considered 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. I also considered that the 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. In this respect, I have considered 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.

14.102 In its Submissions in relation to the Preliminary Draft, TIC submitted that, in considering the nature and scope of the personal data involved in the Breach, "[this] confuses categories of personal data affected by the Underlying Bug with categories of personal data affected by the alleged infringement."³²³ TIC further contended that "*The number of users potentially affected by the underlying bug was the number of people with protected tweets who had changed a setting during the relevant time period. However, none of these people...were affected by the breach alleged by the DPC, namely, the alleged delay in notification of the Underlying Bug to the DPC...*"³²⁴

14.103 TIC also argued that

*"...the DPC is not entitled to assume from this that the data which was exposed did in fact include sensitive material and was in fact accessed by anyone, and in any case, this is not directly relevant to the alleged infringement breach alleged by the DPC (namely, the alleged delay in notification of the Underlying Bug to the DPC)."*³²⁵

14.104 In essence, TIC's position is that no individuals were affected by the delayed notification of the Breach to the Commission and that it cannot be assumed that sensitive material was affected by the Breach or the delayed notification. In this regard, I do not consider that TIC can definitively state, as it does, that no users who were affected by the Breach were affected by the delayed notification. This is an assumption without any evidence to support it. I have already considered the issue of the level of damage suffered by data subjects above under the criterion at Article

³²³ Submissions in relation to the Preliminary Draft, para. 12.36

³²⁴ Ibid, para. 12.10

³²⁵ Submissions in relation to the Preliminary Draft, para 12.12

83(2)(a) and I consider that those considerations are also relevant here. Having regard to the *potential for damage* caused by the delayed notification, which I set out above in the context of Article 83(2)(a), and having regard to the fact that the notice to data subjects was provided some nine days following the delayed notification to the Commission, I consider that it cannot be stated, as TIC purports essentially to do so, that there were no categories of personal data affected. As I have set out above, at Article 83(2)(a), while there was no direct evidence of damage, there was, however, potential for *data subjects* to be affected by the delayed notification of the Breach to the Commission. This inherently means that there was equally potential for limitless or any categories of personal data to be affected by the delay in notification to the Commission. In this respect, I note that TIC itself has stated, in the context of considering the issue of tweets being made public, that:

“With a large number of potentially exposed accounts, one would simply assume that the exposed data could include any category of personal data.”³²⁶

This was the very point that I had made on a provisional basis in the Preliminary Draft - i.e. that it was reasonable to operate on the basis that some of the personal data involved in the Breach constituted special categories of personal data. Finally, relevant to this issue, I also note that TIC stated in its Submissions in relation to the Preliminary Draft that *“TIC acknowledges that the Underlying Bug created the possibility that information which might cause users embarrassment, damage or distress might be exposed.”³²⁷*

- 14.105 Accordingly, having regard to the *potential* for damage to data subjects caused by the delayed notification to the Commission (which I have set out above in the context of Article 83(2)(a)), the corollary of this is that any category of personal data could have been affected by the delayed notification. Whilst, as stated above, there was no direct evidence of damage, at the same time, it cannot be definitively said that there was no damage to data subjects or no affected categories of personal data.

Article 83(2)(h) - The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

- 14.106 In the Preliminary Draft, I expressed the provisional view that the central issue in this Inquiry, and which informs the infringement in respect of Article 33(1), concerns the notification of the Breach to the Commission. Therefore, my view was that this issue is directly related to this criterion. Whilst TIC notified the Commission of the Breach on 8 January 2019, confusion arose as a result of language used by TIC in the Breach Notification Form.

³²⁶ Ibid, para. 16.3

³²⁷ Ibid, para. 12.12

14.107 As I explained, and as has also been described above in this Decision, considerable uncertainty regarding the facts surrounding the notification of the Breach to the Commission arose from the language used in the Breach Notification Form, wherein the terms ‘we’ and ‘our’ were used to refer interchangeably to Twitter Inc. and TIC. During the correspondence exchanged during the course of the Inquiry, therefore, the Investigator sought and obtained clarification from TIC in relation to its language usage. TIC itself has acknowledged that the phrasing used in the Breach Notification Form (and Updated Breach Notification Form) gave rise to uncertainty and has made submissions during the course of the Inquiry to explain its use of language in the notification and the background to same.

14.108 In its Submissions in relation to the Preliminary Draft, TIC submitted that *“The factors taken into account by the DPC under this factor are inappropriate. This factor is aimed at whether or not the controller sought to conceal an infringement from the DPC.”*³²⁸

However, the Administrative Fines Guidelines state that

*“The controller has an obligation...to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating / mitigating factor. **Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty...***³²⁹”

14.109 This indicates that, in addition to considering the question of whether notification took place, a supervisory authority may have regard to the format of such notification. In this case, I accept that TIC did not submit a notification to the Commission that was factually incomplete in relation to the Breach itself. However, the language used in the Notification, and in particular, the use of the words ‘we’ and ‘our’ to refer interchangeably to TIC (as controller) and Twitter Inc. (as processor) did generate confusion at the outset.

14.110 In the Preliminary Draft, I also set out my provisional view that it was a relevant factor under this criterion that the documentation maintained by TIC in respect of the Breach, and which it has held out as being a record of the Breach, did not include certain key information so as to enable TIC’s compliance with the notification requirements in Article 33 to be verified (in accordance with Article 33(5)).

14.111 In its Submissions in relation to the Preliminary Draft, TIC submitted that it did not consider the deficiencies in TIC’s documentation of the Breach to be a relevant factor to be considered under this heading. In this regard, TIC submitted that

³²⁸ Submissions in relation to the Preliminary Draft, para. 12.38

³²⁹ Administrative Fines Guidelines, page 15

“Whether or not TIC’s records of the Underlying Bug contained sufficient information regarding the timing of its notification for the purposes of Article 33(5) does not go to the manner in which the DPC became aware of the infringement....Whilst it acknowledges it has a statutory obligation to cooperate, the fact that it at no time sought to conceal its processes or the error that had occurred in following them should at least mean that the manner in which the infringement became known to the DPC should not be treated as an aggravating factor leading to the imposition of fine.”³³⁰

- 14.112 Whilst I accept that TIC was forthcoming in furnishing all documentation which it had in respect of the Breach, I still consider that the fact that the documentation which it maintained as its ‘record’ of the Breach did not allow the Commission to verify its compliance with Article 33 and, in particular, did not allow verification of TIC’s compliance with its notification obligation under Article 33(1) is a relevant factor.

Furthermore, for the reasons set out above, notwithstanding the explanations (in respect of its use of language in the Breach Notification Form) that have been provided by TIC in its submissions, I consider that the imprecise nature of the information originally provided in the notification which was made to the Commission is a relevant factor when setting the amount of the fine to be imposed.

Article 83(2)(i) - Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

- 14.113 The criterion at Article 83(2)(i) is not applicable in this case.

Article 83(2)(j) - Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

- 14.114 The criterion at Article 83(2)(j) is not applicable in this case.

Article 83(2)(k) - Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

- 14.115 In respect of this criterion, I have not identified any other factors, additional to those which I have already considered in the context of any of the other criteria above, which I consider appropriate and relevant to consider under this provision in the context of the potential aggravation or

³³⁰ Submissions in relation to the Preliminary Draft, para. 17.23

mitigation of the circumstances of this case. I note also, in this regard, that TIC did not make any additional submissions under this factor in its Submissions in relation to the Preliminary Draft.

Conclusion with regard to consideration of factors under Article 83(2)

14.116 As stated above, having had due regard to the factors set out, as I am required to do, under Article 83(2), I have decided that the infringements which have been identified warrant the imposition of an administrative fine in the circumstances of this case.

I must, therefore, next proceed to decide on the amount of the administrative fine, in light of both my consideration of the factors set out above under Articles 83(2) (a) to (k), and also in light of the obligation under Article 83(1), which applies to me as the decision maker in the Commission, to ensure that the administrative fine imposed in this case is effective, proportionate and dissuasive.

In deciding on the amount of the fine which is to be imposed in respect of the two infringements identified, it is appropriate that I consider both infringements simultaneously in the calculation of the fine in light of Article 83(3) GDPR, which states:

“If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.”

Consequently, in circumstances where the fine for one of the infringements was greater than the other, the total fine would be equal to the largest fine in any event.

15. CALCULATION OF ADMINISTRATIVE FINE

- 15.1 I have considered the above factors in determining the amount of the administrative fine to be imposed, as I am required to do under Article 83(2). In this regard, the sections that follow below will identify the matters to be considered when setting the amount of the fine.
- 15.2 The weight to be given to the factors in Articles 83(2)(a) to (k) and their impact on the amount of the fine are matters for the supervisory authority’s discretion. The expression “due regard” (in Article 83(2)) provides the supervisory authority with a broad discretion in this respect.
- 15.3 I explained in the Preliminary Draft that, in the absence of specific EU-level guidelines on the calculation of fines in this context, I am not bound to apply any particular methodology.³³¹ In

³³¹See by analogy *Electrabel v Commission*, T-332/09, ECLI:EU:T:2012:672, para 228, *Marine Harvest ASA v Commission*, T-704/14, ECLI:EU:T:2017:753, para 450

practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine.³³² I, therefore, ultimately intend to identify the amount of the administrative fine to be imposed on TIC on a general basis (as in the judgments cited in the footnotes above) and by reference to the factors to which I am required to have due regard in accordance with Article 83(2) and which I have already applied to the circumstances of this case in detail above. In doing so, I must also ensure that, in accordance with the obligation on supervisory authorities under Article 83(1), the administrative fine imposed in this case is effective, proportionate and dissuasive.

- 15.4 In advance of considering the amount of the fine in this particular case, I have considered the appropriate cap for the fine as a matter of law. In this regard, Articles 83(3) – 83(6) categorise the provisions of the GDPR and specify the cap, or maximum amount, of fines in respect of same.

In respect of the infringements in question, which arise under Article 33, the fining cap is set by Article 83(4), which provides that, in respect of infringements of Articles 8, 11, 25-39, 42 and 43 GDPR, the maximum value for a fine is 2% of the annual turnover of the undertaking.

The relevant undertaking

- 15.5 In order to calculate the fine, therefore, it is necessary to identify the relevant undertaking, adopting the approach to this question used in applying Articles 101 and 102 of the Treaty on the Functioning of the European Union (the “TFEU”) and which is defined therein as being

[the] “*economic [unit] which consist[s] of a unitary organisation of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis and can contribute to the commission of an infringement*”.³³³

- 15.6 As the CJEU held in *Akzo v Commission*:

“60. In the specific case where a parent company has a 100% shareholding in a subsidiary which has infringed the Community competition rules, first, the parent company can exercise a decisive influence over the conduct of the subsidiary...and, second, there is a rebuttable presumption that the parent company does in fact exercise a decisive influence over the conduct of its subsidiary...”

61. In those circumstances, it is sufficient for the Commission to prove that the subsidiary is wholly owned by the parent company in order to presume that the parent exercises a decisive influence over the commercial policy of the subsidiary. The Commission will be able to regard the parent company as jointly and severally liable for the payment of the fine imposed on its subsidiary, unless

³³² See by analogy, *Marine Harvest ASA v Commission*, T-704/14, ECLI:EU:T:2017:753, para 456.

³³³ *Viho Europe BV v Commission*, C-73/95 P, ECLI:EU:C:1996:405, para 50

the parent company, which has the burden of rebutting that presumption, adduces sufficient evidence to show that its subsidiary acts independently on the market...”³³⁴

- 15.7 Based on my understanding that TIC is wholly owned by Twitter Inc, I wrote to TIC on 13 February 2020 to explain that I was minded to apply the said presumption derived from EU competition law, namely that

“[i]n respect of TIC’s economic activities, the undertaking as defined by Articles 101 and 102 of the Treaty on the Functioning of the European Union (“the TFEU”), and referred to in Recital 150 of the General Data Protection Regulation (“the GDPR”), is Twitter Inc.”

TIC responded by letter dated 19 February 2020. TIC did not dispute that it was a subsidiary of Twitter Inc, but set out its contrary view that TIC alone was the relevant undertaking. In this regard, TIC stated as follows:

“TIC notes that, for the purposes of Articles 101 and 102 TFEU, a single economic entity may include a subsidiary’s parent company where it exercises “decisive influence” over the subsidiary, to the extent that the subsidiary does not enjoy real independence in making commercial decisions. When applied here in the context of the GDPR though, it is clear that TIC, as the sole independent controller of personal data of EEA data subjects, enjoys independence in respect of decisions about the purposes and means of processing. Conversely, Twitter Inc., which is not a controller of the relevant personal data, does not exercise decisive influence over the data processing.”

- 15.8 TIC seeks to rebut the said presumption by asserting that, in relation to the specific area of data processing, TIC has sole control and Twitter Inc does not exercise decisive influence. TIC relies on the “context of the GDPR”, arguing that it would be “paradoxical” if TIC could have “independent control” over data processing (as the “controller”) but be at the same time subject to the “decisive influence” of its parent company.
- 15.9 In order to rebut the presumption of decisive influence, however, it is not sufficient to show that the subsidiary enjoyed operational autonomy or that the parent had only minimal engagement with the subsidiary’s affairs in the area in which the wrongdoing took place.
- 15.10 The General Court has held that *“[o]perational independence does not, in itself, prove that a subsidiary decides upon its conduct on the market independently of its parent company. The division of tasks between subsidiaries and their parent companies and, in particular, the fact that the local management of a wholly owned subsidiary is entrusted with operational management is*

³³⁴ *Akzo Nobel and Others v Commission*, C-97/08, ECLI:EU:C:2009:536, paras 60 - 61

*normal practice in large undertakings composed of a multitude of subsidiaries ultimately owned by the same holding company”.*³³⁵

- 15.11 The General Court has held that this approach is justified “*by the fact that, in the case of a subsidiary which is wholly, or almost wholly, owned by a sole parent company, there is in principle a single commercial interest and the members of the subsidiary’s bodies are designated and appointed by the sole shareholder, which may give them at least informal instructions and impose performance criteria on them. In such a case, therefore, there is necessarily a relationship of confidence between the management of the subsidiary and the management of the parent company and the management of the subsidiary necessarily acts by representing and promoting the only commercial interest that exists, namely the interest of the parent company. Thus, the unity of the market conduct of the parent company and of its subsidiary is ensured in spite of any autonomy conferred on the management of the subsidiary as regards its operational management, which comes within the definition of the parent company’s commercial policy in the strict sense. As a general rule, moreover, it is the sole shareholder that defines, on its own and according to its own interests, the procedure whereby the subsidiary takes decisions and that determines the extent of the subsidiary’s operational autonomy... Therefore, as a general rule, the management of the subsidiary thus ensures that the subsidiary’s commercial conduct complies with that of the rest of the group in the exercise of their autonomous powers*”.
- ³³⁶
- 15.12 In the *Ori Martin* case, the parent claimed that it was established for tax optimisation purposes only, was minimally staffed and had minimal engagement with the subsidiary. The CJEU held that in order to establish a single economic entity (and maintain the presumption) the test was not whether the parent gave the subsidiary instructions in the area covered by the misconduct or in relation to misconduct itself.³³⁷ The question was whether, in view of the economic, organisational and legal links which united the subsidiary to the parent company, the subsidiary enjoyed real autonomy (emphasis added). In the *Akzo* case, the General Court suggested that this could be demonstrated by evidence of the subsidiary not complying with instructions from its parent.³³⁸
- 15.13 In *International Removal Services*, it was established in fact that (a) the parent’s board met for the first time only after the end of the infringement; (b) the parent’s only activity was exercising the voting rights at the subsidiary’s AGM, whereas, under Belgian company law, it is only a company’s board and not the AGM which manages the company; (c) in any event, no AGM was held by the subsidiary during the period in question; and (d) the parent had no influence over the composition

³³⁵ *Huhtamäki Oyj v Commission* T-530/15 ECLI:EU:T:2019:498, para 228; *RWE Dea v Commission*, T-543/08, EU:T:2014:627, para 49

³³⁶ *Huhtamäki Oyj v Commission* T-530/15 ECLI:EU:T:2019:498, para 229; *RWE Dea v Commission*, T-543/08, EU:T:2014:627, para 50.

³³⁷ C-490/15 P ECLI: EU: C: 2016: 678, para. 60.

³³⁸ Para 62 as quoted in *Akzo Nobel and Others v Commission*, C-97/08, ECLI:EU:C:2009:536, para 27.

of the subsidiary's board. Nevertheless, the CJEU held that the presumption of decisive influence had not been rebutted.³³⁹

- 15.14 In my view, and in the light of the EU authorities on the meaning of “undertaking” under Articles 101 and 102 TFEU, 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 in view of the links between them.

I also note, in this regard, 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.

- 15.15 In its Submissions in relation to the Preliminary Draft, TIC has not otherwise sought to rebut the presumption of decisive influence or to rebut the legal analysis set out above in relation to the concept of “undertaking”.

I therefore remain of the view that, while the provisions of the GDPR are addressed to data controllers, the cap for the value of any fine imposed must be the turnover of the ‘undertaking’ as defined under Articles 101 and 102 TFEU.

On the basis of the foregoing, the cap for any fines imposed by the Commission will be calculated with reference to Twitter Inc.’s turnover.

Amount of the administrative fine

- 15.16 I note, by analogy with EU competition law, that the fining authority should not anticipate the submissions of parties by providing the final proposed fine in its statement of objections.³⁴⁰ In applying this principle, I noted in the Preliminary Draft that it is impossible to specify a precise figure without having regard to the views of the party subject to the inquiry. Moreover, as I stated in the Preliminary Draft, it is clear, as a matter of Irish law, that TIC was entitled to be informed of the allegation against it and to be given the opportunity to respond to it.³⁴¹
- 15.17 On this basis, in the Preliminary Draft, I identified the proposed range of the administrative fine which I provisionally decided to impose rather than identifying a specific amount of the fine. This was in order to facilitate the making of submissions from TIC on both the amount of the fine and the application of factors to which I have had regard in accordance with Article 83. As referred to

³³⁹ *Commission v SA Portielje*, C-440/11, ECLI:EU:C:2013:514 paras 81-87.

³⁴⁰ Cases 125/2007 P, 133/2007 P, 135/2007 P and 137/2007 P *Erste Group Bank v Commission* (ECLI:EU:C:2009:576), para 182.

³⁴¹ *Gunn v Bord an Choláiste Náisiúnta Ealaíne is Deartha* [1990] 2 IR 168, 179.

in this Decision, TIC made submissions in relation to the matters relating to the provisional findings of infringement and in relation to the factors pertaining to the question of whether an administrative fine should be imposed (and, to a very limited extent, the amount of same, if any).

- 15.18 In deciding on the proposed range of the fine (as set out in the Preliminary Draft and Draft Decision), and in determining the amount of the fine, I have, as set out above, had due regard to all of the factors set out in Articles 83(2)(a) to (k) as applicable, having taken account of TIC's submissions on these matters as set out in its Submissions in relation to the Preliminary Draft. I also note TIC's limited submission in relation to the amount / range of the fine concerning the upper limit of the range of the fine which was proposed, on a provisional basis, in the Preliminary Draft (\$500,000) as follows:

*"Even if the DPC is correct in its finding that TIC infringed Article 33(1), which TIC strenuously disputes, it is wrong to conclude that a fine, and particularly a fine potentially as high as \$500,000, is appropriate in this case."*³⁴²

- 15.19 In addition, in determining the amount of the fine, I have complied with the binding direction of the EDPB, as set out in the EDPB Decision at paragraph 207 thereof, to the effect that the Commission 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."*³⁴³

In this regard, I have already set out above, at section 14, how I have reassessed the elements identified in the EDPB Decision, at paragraphs 182 to 198 thereof, and which relate to the factors under Articles 83(2)(a) and 83(2)(b). In accordance with the EDPB's direction that the level of the fine be increased, I set out below the amount of the fine which I have decided to impose, taking into account the requirements of effectiveness, dissuasiveness and proportionality under Article 83(1) and taking into account the criteria under Article 83(2).

- 15.20 In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, I consider that it is proper and appropriate to take into account the relative financial position of Twitter Inc., which for the reasons set out above, is the relevant undertaking. I note, in this regard, that the annual turnover of the

³⁴² Submissions in relation to the Preliminary Draft, para. 12.4

³⁴³ EDPB Decision, para. 207

relevant undertaking, Twitter Inc., was \$3.46 billion³⁴⁴ in 2019, these being the most recently available annual turnover figures for Twitter Inc.

- 15.21 In considering the application of the principles of effectiveness, proportionality and dissuasiveness of the administrative fine, I consider that a fine cannot be effective if it does not have significance relative to the revenue of the data controller. In addition, I consider that, in order to be “effective”, a fine must reflect the circumstances of the case at hand. In this case, and as I have outlined above, I consider the infringements under Article 33(1) and 33(5) to be moderately serious in terms of their gravity.
- 15.22 In order for a fine to be “dissuasive”, it must have deterrent effect, thereby dissuading both the controller/processor concerned, as well as other controllers/processors that carry out similar processing operations, from engaging in the conduct concerned. The CJEU has held, in this regard, that “[t]he severity of the sanctions must be commensurate to the seriousness of the breaches for which they are imposed, in particular by ensuring a genuinely dissuasive effect..”³⁴⁵ In this regard, I consider that a fine cannot be dissuasive if it will not be of real financial significance to the addressee.
- 15.23 In terms of the principle of proportionality, this cannot be adhered to if the infringement is considered in the abstract, regardless of the impact on the controller. In order for any fine to be proportionate, therefore, I am required to adjust the quantum of the fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. For this reason, I must consider whether the fine does not exceed what is necessary in order to enforce compliance with the GDPR.
- 15.24 As regards the maximum amount (the “cap”) for the fine which may be imposed in this case, the relevant cap for any fine in respect of the two identified infringements is \$69.2 million – that is, 2% (as set out in Article 83(4) in respect of any infringements of, *inter alia*, Article 33 GDPR) of \$3.46 billion.
- 15.25 Having regard to all of the foregoing, and, in particular, having had due regard to all of the factors which I am required to consider under Articles 83(2)(a) to (k), as applicable, and in the interests of effectiveness, proportionality and deterrence, and in light of the re-assessment of the elements I have implemented and documented above in accordance with the EDPB Decision, I have decided to impose an administrative fine of **\$500,000**, which equates (in my estimation for this purpose) to **€450,000**. In deciding to impose a fine in this amount, I have had regard to the previous range of

³⁴⁴ This is as stated as being the ‘revenue’ figure for 2019 in the ‘Consolidated Statement for Operations Data’ on page 32 of the Twitter Inc. Fiscal Year 2019 Annual Report.

³⁴⁵ Case C-81/12 Asociația Accept v Consiliul Național pentru Combaterea Discriminării, para 63

the fine, set out in the Draft Decision (of \$150,000 - \$300,000), and to the binding direction in the EDPB Decision, at paragraph 207 thereof, that the level of the fine should be increased “*..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.*” Having regard to the requirement under Article 83(1), and based on my consideration of **all** of the factors under Article 83(2) and my analysis in respect of same, I am satisfied that a fine in this amount will be effective, proportionate and dissuasive, taking into account all of the circumstances of this case. In addition, in circumstances where the fine which I have now decided to impose represents an increase of approximately 67% on the upper level of the range of the fine previously proposed in the Draft Decision, I consider that the fine imposed accords with the binding direction of the EDPB.

- 15.26 In determining the above fine, I have, as set out above, had due regard to **all** of the factors under Articles 83(2)(a) to (k) and to the issues which I have considered in detail under each of those factors. However, I have had particular regard to the nature, gravity and duration of the infringements concerned, taking account of the nature, scope and purpose of the processing and the number of data subjects affected. In this regard, and as I have set out above, I consider that compliance with the obligations under Articles 33(1) and 33(5) is central to the overall functioning of the supervision and enforcement regime performed by supervisory authorities. I have also had particular regard, in this case, to the negligent character of the infringements.

In setting the fine, I have also taken account of the steps that were taken by Twitter Inc. (between 3 January 2019 and 14 January 2019) to rectify the bug. In addition, I have taken account of my assessment, under Article 83(2)(d) (as revised from my assessment of this factor in the Preliminary Draft), in respect of the degree of responsibility of the controller.

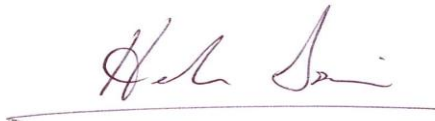
- 15.27 Finally, as decision-maker for the Commission, I consider it important to strongly discourage the activity involved in these infringements. In this regard, I suggest that TIC take particular note of Article 83(2)(e) GDPR (where past infringements can be taken into account in relation to any future exercise of corrective powers that may arise) going forward.
- 15.28 **The Commission adopts the within Decision pursuant to Article 60(7) in conjunction with Article 65(6) GDPR. In doing so, and having regard to the requirement at Recital 129 that a legally binding measure should be clear and unambiguous, the Commission has confirmed the precise fine to be imposed in this matter at paragraph 15.25 above.**

This Decision is addressed to:

Twitter International Company,
One Cumberland Place,
Fenian Street,
Dublin 2,
Ireland.

Dated the 9th day of December 2020

Made by Decision-Maker for the Commission:

A handwritten signature in dark ink, appearing to read 'Helen Dixon', is written over a horizontal line.

Helen Dixon
Commissioner for Data Protection

**Annex I - Schedule of documentation considered by the decision maker for the purpose of
preparation of the Decision**

Pre-Commencement of Inquiry

1. Email dated 8 January 2019 (18:08 hours) from DPO for TIC to the DPC breaches mailbox, attaching completed Cross-Border Breach Notification Form
2. Letter dated 11 January 2019 from Commission to DPO for TIC
3. Email dated 16 January 2019 (02:23 hours) from DPO for TIC to the DPC breaches mailbox, attaching the following:
 - a. Updated Cross-Border Breach Notification Form; and
 - b. Copy “In Application Notice(s)”
4. Email dated 16 January 2019 (16:42 hours) from DPO for TIC to Commission, attaching list of countries with ‘impacted persons’

Post-Commencement of Inquiry

5. Letter dated 22 January 2019 from investigator for the Commission to DPO for TIC (Notice of Commencement of Inquiry), attaching Appendix A (Request for Information)
6. Letter dated 25 January 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
 - a. Annex (containing responses to queries)
 - b. Exhibit A – copy “Bug Bounty Report from Contractor 1, received 26 December 2018”
 - c. Exhibit B – copy “Protected Tweets Information Help Center page”
 - d. Exhibit C – copy “Data Breach Investigation Through Vulnerability Disclosure Runbook”
 - e. Exhibit D – copy “Security Incident Management Workflow”
 - f. Exhibit E – copy “JIRA Ticket declaring severity of incident”
 - g. Exhibit F – copy “Incident Report”

- h. Exhibit G – copy “fix for code review”
 - i. Exhibit H – copy “JIRA Ticket for partial server side fix”
 - j. Exhibit I – copy “JIRA Ticket for validation that issue is resolved in client side fix”
 - k. Exhibit J – copy “JIRA Ticket for localization team preparation of user notice”
 - l. Exhibit K – copy “document containing EU and EEA country-by-country breakout of impacted users”
 - m. Exhibit L – copy “JIRA Ticket to identify user accounts that will be re-protected alongside issuance of user notice”
 - n. Exhibit M – copy “JIRA Ticket for start of work to re-protect accounts”
 - o. Exhibit N – copy “JIRA Ticket affirming that Android client fix is complete”
 - p. Exhibit O – copy “JIRA Ticket affirming server side work and fix”
7. Letter dated 29 January 2019 from investigator for the Commission to DPO for TIC, attaching Appendix A (Request for Information)
8. Letter dated 1 February 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
- a. Annex (containing responses to queries)
 - b. Exhibit A – redacted “JIRA Ticket”
 - c. Exhibit B – “Investigation Ticket”
 - d. Exhibit C – “IM Ticket”
 - e. Exhibit D – “Investigation Ticket Watchers”
 - f. Exhibit E – “IM Ticket Watchers”
 - g. Exhibit F – “7 January 2019 Calendar Invite”
 - h. Exhibit G – “9 January 2019 Calendar Invite”

- i. Exhibit H – “11 January 2019 Calendar Invite”
 - j. Exhibit I – “14 January 2019 Calendar Invite”
 - k. Exhibit J – “14 January 2019 Calendar Invite”
 - l. Exhibit K – “15 January 2019 Calendar invite”
 - m. Exhibit L – “16 January 2019 Calendar invite”
 - n. Exhibit M – “17 January 2019 Calendar invite”
- 9. Letter dated 6 February 2019 from Commission to DPO for TIC, with the following attachments:
 - a. Appendix A (Request for Information)
 - b. Copy “Data Breach Investigation Through Vulnerability Disclosure Runbook”, as furnished to the Commission in the form of Exhibit C to the letter dated 25 January 2019 from DPO for TIC to investigator for the Commission
- 10. Letter dated 8 February 2019 from DPO for TIC to Commission, with the following attachments:
 - a. Annex (containing responses to queries)
 - b. Exhibit A – “7 January 2019 Calendar Invite”
 - c. Exhibit B – “Current Data Breach Investigation through Vulnerabilities”
- 11. Letter dated 28 May 2019 from investigator for the Commission to DPO for TIC, attaching draft Inquiry Report
- 12. Email dated 30 May 2019 (17:25 hours) from DPO for TIC to investigator for the Commission
- 13. Email dated 4 June 2019 (10:25 hours) from investigator for the Commission to DPO for TIC
- 14. Email dated 4 June 2019 (15:49 hours) from DPO for TIC to investigator for the Commission
- 15. Letter dated 17 June 2019 from DPO for TIC to investigator for the Commission, with the following attachments:
 - a. Annex A – General Submissions in response to draft Inquiry Report

- b. Exhibit A to Annex A – “Slack message dated 7 January 2019”
 - c. Annex B – Submissions on specific aspects of the draft Inquiry Report
16. Email dated 21 June 2019 (15:54 hours) from investigator for the Commission to DPO for TIC
 17. Email dated 21 June 2019 (16:13 hours) from DPO for TIC to investigator for the Commission
 18. Letter dated 16 July 2019 from investigator for the Commission to DPO for TIC, attaching Appendix A (Request for Information)
 19. Letter dated 19 July 2019 from DPO for TIC to investigator for the Commission, attaching Annex A (responses to queries)
 20. Final Inquiry Report (undated) together with document entitled “Documentation associated with Inquiry IN-19-1-1”

Decision-Making Stage

21. Letter sent 21 October 2019 from H. Dixon, Commissioner to DPO for TIC
22. Email dated 23 October 2019 from DPO for TIC to H. Dixon, Commissioner
23. Email dated 5 November 2019 from DPO for TIC to H. Dixon, Commissioner
24. Letter dated 11 November 2019 from H. Dixon, Commissioner to DPO for TIC
25. Letter dated 28 November 2019 from H. Dixon, Commissioner to DPO for TIC
26. Letter dated 2 December 2019 from DPO for TIC to H. Dixon, Commissioner
27. Letter dated 13 February 2020 from H. Dixon, Commissioner to DPO for TIC
28. Letter dated 19 February 2020 from DPO for TIC to H. Dixon, Commissioner

29. Letter dated 14 March 2020 from H. Dixon, Commissioner to DPO for TIC attaching Preliminary Draft Decision and covering letter

30. Letter dated 27 April 2020 from external legal counsel for TIC to H. Dixon, Commissioner, attaching Submissions in Relation to the Preliminary Draft Decision

a. Attachments to TIC Submissions in relation to the Preliminary Draft Decision comprising:

- i. TIC Data Handling Policy
- ii. TIC Employee Security Handbook
- iii. Independent Audit Reports for periods: 2011-2013; 2013-2015; 2015-2017; 2017-2019

31. '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' ('the EDPB Decision')