Inquiry Concerning Twitter International Company ('TIC')

(IN-19-1-1)

Date of Decision: 9 December 2020

This Inquiry, which was commenced by the Data Protection Commission ('the Commission) on 22 January 2019, examined whether Twitter International Company ('TIC') had complied with its obligations under the GDPR in respect of its notification, on 8 January 2019, of a personal data breach ('the Breach') to the Commission. The Breach, which occurred at TIC's processor, Twitter Inc., related to a bug whereby if a Twitter user with a protected account, using Twitter for Android, changed their email address, their account would become unprotected.

The purpose of the Inquiry was to examine certain issues surrounding TIC's notification of the Breach, as distinct from examining the substantive issues relating to the Breach itself. In this regard, the Inquiry examined whether TIC had complied with Article 33(1) of the GDPR, in terms of the timing of its notification of the Breach to the Commission, and whether it had complied with Article 33(5) of the GDPR, in respect of its documenting of the Breach.

The DPC submitted its draft decision in this inquiry to other Concerned Supervisory Authorities under Article 60 GDPR on 22 May 2020. This was the first draft decision to go through the Article 65 dispute resolution process and was the first Draft Decision in a "big tech" case on which all EU supervisory authorities were consulted as Concerned Supervisory Authorities. The European Data Protection Board adopted its decision under Article 65(1)(a) on 9 November 2020. The DPC issued its final decision to TIC on 9 December 2020.

Facts leading to Inquiry

TIC's notification of the Breach to the Commission, which led to the Inquiry, took place on 8 January 2019 by way of a completed Cross-Border Breach Notification Form. In the Form, TIC outlined that it had received a bug report through its 'Bug Bounty Program' to the effect 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." The Breach Notification Form further outlined, in respect of the reasons for not notifying the Commission 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 [sic] at which point Twitter's incident response process was put into action."

The Breach Notification Form identified the potential impact for affected individuals, as assessed by TIC, as being "significant". In a further follow up notification form submitted by TIC to the Commission on 16 January 2019, TIC confirmed the number of affected EU and EEA users was 88,726. It also confirmed that the bug which had led to the Breach "was introduced on 4 November 2014 and fully remediated by 14 January 2019" and that, as it was not possible to

identify all impacted persons (due to retention limitations on available logs), it believed that additional people were impacted during that period.

Inquiry under Section 110, Data Protection Act 2018

As it appeared from the Breach Notification Form submitted by TIC that a period of in excess of 72 hours had elapsed from when TIC (as controller) became aware of the Breach, and having regard to the number of affected data subjects, the Commission commenced the Inquiry, under Section 110(1) of the Data Protection Act 2018 ('the 2018 Act') for the purpose of examining whether TIC had complied with its obligations under Article 33, and more particularly, with its obligations under Article 33(1) and Article 33(5).

Compliance with Article 33(1)

In assessing TIC's compliance with Article 33(1), the Commission examined the timeline relating to TIC's notification of the Breach to the Commission. In this regard, TIC confirmed to the Commission during the Inquiry that notice of the bug was first received on 26 December 2018 by an external contractor engaged by Twitter to search for and assess bugs via the Bug Bounty Program, a program whereby anyone may submit a bug report. TIC further confirmed that, on 29 December 2018, the external contractor, having assessed the bug report, communicated the outcome of its assessment to Twitter Inc. TIC further confirmed that Twitter Inc. then commenced its internal Information Security review of the issue on 2 January 2019, and that, following this, on 3 January 2019, Twitter Inc. assessed the incident as being a potential personal data breach under the GDPR and determined that the incident response plan should be initiated. TIC also confirmed that, following this (on 4 January 2019), an Incident Management (IM) ticket was opened but that, due to a failure (by Twitter Inc. staff) to follow a particular step in the incident management process as it was prescribed, the Data Protection Officer (DPO) for TIC was not added to the IM ticket, which resulted in a delay in the DPO (and, therefore TIC as controller) being notified of the issue.

TIC confirmed to the Commission that it was first made aware of the Breach by its processor, Twitter Inc., on 7 January 2019. It submitted that, in circumstances where it had notified the Breach to the Commission on 8 January 2019, it had complied with the requirement to notify under Article 33(1).

Having considered the timeline in relation to TIC's notification of the Breach, the Commission formed the view that, notwithstanding TIC's actual awareness of the Breach on 7 January 2019, TIC ought to have been aware of the Breach at an earlier point in time and, in this particular case, at the latest by 3 January 2019. In forming this view, the Commission took account of the fact that 3 January 2019 was the date on which Twitter

Inc. first assessed the incident as being a potential personal data breach but that, for reasons of the ineffectiveness of the process in the particular circumstances that transpired and/or a failure by Twitter Inc. staff to follow its own incident management process, a delay occurred in the DPO being informed of the potential data breach, which, in turn, resulted in TIC (as controller) not being notified of the Breach until 7 January 2019.

In making this finding, the Commission also took account of an earlier delay that had arisen in the period from when the incident was first notified to Twitter Inc. by its external contractor on 29 December 2018 to when Twitter Inc. commenced its Information Security review of the issue on 2 January 2019. During the course of the Inquiry, TIC confirmed to the Commission that this delay had arisen "due to the winter holiday schedule" (in circumstances where three of the four days in question were holidays – a weekend and New Years Day) which had led to the issue not being identified and escalated as it should have been. However, the Commission did not accept this delay as being reasonable, in particular in circumstances where 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 and given that Twitter's services do not cease to operate during such times.

As outlined in the Decision, the alternative application of Article 33(1), and that which was suggested by TIC during the Inquiry, 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.

Compliance with Article 33(5)

In assessing TIC's compliance with Article 33(5), the Commission carried out a review of the documentation provided by TIC during the course of the Inquiry, and in which it claimed that it had documented the Breach.

In doing so, the Commission found that TIC had not complied with Article 33(5). This was in circumstances where the documentation maintained by TIC – either individually or collectively – 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 course of TIC's management of the incident.

In addition, the Commission found that the documentation maintained by TIC in relation to the Breach did not contain sufficient information so as to enable the question of TIC's

compliance with the requirements of Article 33 to be verified, as is required by Article 33(5). In particular, the Commission found that the documentation, which TIC had identified as being the primary record in which it had documented the facts, effects and remedial action taken in respect of the Breach, was deficient in circumstances where it did not contain all material facts relating to the notification of the Breach to the Commission. In particular, the documentation did not contain any reference to the issues that had led to the delay in TIC being notified of the Breach by its processor, nor did it address how TIC had assessed the risk to affected users arising from the Breach. The Commission also found that the deficiencies in the documentation furnished by TIC as a record of the Breach were further demonstrated by the fact that, during the Inquiry, the Commission had to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

Process under Article 60 and Article 65 GDPR

On 22 May 2020, the Commission issued a draft of its Decision ('the Draft Decision') to the other concerned supervisory authorities ('CSAs') for their opinion in accordance with the process under Article 60 GDPR. The Draft Decision set out the Commission's proposed finding of infringements under Articles 33(1) and 33(5) and its proposal to impose an administrative fine. Under Article 60(4), CSAs have a period of four weeks within which to express a relevant and reasoned objection to a draft decision.

A number of CSAs expressed objections in relation to aspects of the Draft Decision, including objections on the basis that the Commission should, as part of its Inquiry, have considered other provisions of the GDPR; objections relating to non-substantive matters, such as the designation of the role of the respondent under investigation (TIC) and the competence of the Commission, as Lead Supervisory Authority, to deal with the matter; and objections in relation to the administrative fine which the Commission proposed.

Having considered the objections raised, and having endeavoured to reach consensus with the CSAs, the Commission was unable to follow the objections in an amended Draft Decision. On this basis, the Commission referred the matter to the European Data Protection Board ('EDPB') for determination pursuant to the Article 65 dispute resolution mechanism. The EDPB commenced the Article 65 procedure on 8 September 2020. Having adopted its binding decision under Article 65(1)(a) ('the EDPB Decision') on 9 November 2020, the EDPB notified same to the Commission on 17 November 2020. Thereafter, pursuant to Article 65(6), the Commission was required to adopt its final decision on the basis of the EDPB Decision "without undue delay and at the latest by one month after the Board has notified its decision."

Article 65(1)(a) provides that the EDPB's binding decision under Article 65 "…shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of [the GDPR]". In this regard, in terms of the EDPB's assessment of the objections raised by the CSAs in this case, the EDPB Decision found that certain of the objections raised were not 'relevant and reasoned' within the meaning of Article 4(24) on the basis that they did not provide a clear demonstration as to the significance of the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union (as is required by Article 4(24)).

With regard to a number of other objections raised, and which had been made on the basis that the Commission should have considered further infringements under other provisions of the GDPR (specifically, Articles 5(1)(f), 5(2), 24 and 32), whilst the EDPB found that these objections were relevant and reasoned under Article 4(24), it determined that it could not, on the basis of the factual elements in the Draft Decision or in the objections themselves, establish the existence of such further (or alternative) infringements.

Finally, and with regard to the objections raised by CSAs in respect of the administrative fine imposed, the EDPB found that certain of these objections were relevant and reasoned under Article 4(24). As such, the EDPB issued a binding direction to the Commission to re-assess the elements that it had relied upon to calculate the amount of the fine (under Article 83(2) GDPR) and to amend its Draft Decision by increasing the level of the fine. (For further detail on the EDPB Decision, please refer to the EDPB website where the EDPB Decision is published).

Decision under Section 111 of 2018 Act

The Commission adopted its final Decision ('the Decision') on the basis of the EDPB Decision, pursuant to Article 60(7) in conjunction with Article 65(6), on 9 December 2020. In finding that TIC had infringed both Article 33(1) and Article 33(5), the Commission imposed an administrative fine of $500,000 (estimated for this purpose at €450,000) which reflected an increase in the level of the proposed administrative fine set out in the Draft Decision, in accordance with the direction of the EDPB. In determining this fine, the Commission ensured, as it is required to do under Article 83(1) GDPR, that the fine imposed was effective, proportionate and dissuasive. In this regard, in deciding to impose a fine and in determining the amount of same, the Commission considered the full range of factors under Article 83(2) GDPR in the context of the circumstances of this particular case. In doing so, the Commission 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. The Commission also had regard to the negligent character of the infringements. In setting the fine, the Commission also took

account of certain other factors, including the steps that had been taken by Twitter Inc. to rectify the bug.

In reaching its decision in this case, the Commission also highlighted that controller compliance with the obligations under Article 33(1) and Article 33(5) is of central importance to the overall functioning of the supervision and enforcement regime performed by data protection authorities.