SULLIVAN & CROMWELL LLP

December 21, 2020

Irish Data Protection Commission Fines Twitter for Failures in Notifying Data Breach

DPC Finds Twitter's Irish Subsidiary Had Constructive Knowledge of a Personal Data Breach Through its Processor, and Thus Failed to Notify in a Timely Manner and to Adequately Document the Breach.

SUMMARY

With many technology firms choosing Dublin as their European base, the Irish Data Protection Commission (the "**DPC**") acts as one of the leading data regulators of big tech in Europe. In its first major decision concerning Twitter International Company ("**Twitter Ireland**") (an Irish incorporated subsidiary of Twitter Inc., incorporated in the United States), the DPC fined Twitter Ireland $500,000.00 for failing to notify the DPC in a timely manner of a breach concerning users' personal data and failing to keep appropriate records of the breach.

Whilst the fine falls well short of the maximum fine permitted under the European General Data Protection Regulation ("**GDPR**") (which provides for fines of up to 4% of annual worldwide revenue), the DPC has clarified important points of principle under GDPR. In particular, the decision provides guidance on the nature of the controller-processor relationship, clarifying that a controller cannot hide behind its processor's late notification of a breach if the controller should have known of the breach earlier had the protocols and processes that ought to be in place in the context of a controller-processor relationship been properly followed. The DPC also made clear that the time period by which the relevant supervisory authorities must be informed of a personal data breach will be strictly enforced, as will the requirements that the controller is under to keep appropriate records of the breach.

In addition to the Twitter inquiry that has now been concluded, the DPC is currently dealing with more than 21 cross-border investigations into the data processing activities of Apple, Facebook (and Facebook-owned platforms WhatsApp and Instagram), Google, LinkedIn, Quantcast, Tinder, and Verizon. Given the number of big tech firms that have chosen Ireland as the European base for their

operations, it seems inevitable that there will be future influential decisions issued by the DPC on the application of GDPR.

BACKGROUND

The DPC's inquiry and subsequent decision concerning Twitter Ireland arose in connection with a personal data breach, relating to a "bug" (i.e., an unintentional error imbedded in computer code) in Twitter group's Android app. As a consequence of the bug if a user operating an Android device changed the email address associated with that user's Twitter account, that user's tweets became unprotected and consequently accessible to the wider public without the user's knowledge. According to Twitter Ireland, the breach had arisen in the context of processing carried out on its behalf by Twitter Inc. For purposes of assessing the breach under GDPR, Twitter Ireland was considered the data controller and Twitter Inc. the data processor.

The bug was discovered on December 26, 2018 by an external contractor managing Twitter Inc.'s "bug bounty programme", which is a programme whereby anyone may submit a report of error discovered in Twitter's code. The issue was reported to Twitter Inc. on December 29, 2018. Twitter Inc. assessed the issue as potentially being a personal data breach on January 3, 2019 and triggered the company's incident response process on January 4, 2019. However, the Twitter Group's Global Data Protection Officer ("DPO") was not added to the incident response ticket and therefore was not notified on that date. The Twitter Group's DPO and Twitter Ireland were notified subsequently on January 7, 2019, following which Twitter Ireland reported the data breach to the DPC at 18.08 (GMT) on January 8, 2019. In reporting the breach, Twitter Ireland indicated that between September 5, 2017 and January 11, 2019, 88,726 EU and EEA users were affected by the bug. Twitter Ireland confirmed that the bug appeared to date from November 4, 2014, but that it could only identify users affected from September 5, 2017. It was possible therefore that more users were affected by the breach.

The DPC subsequently initiated an inquiry on January 22, 2019, examining Twitter Ireland's compliance with Article 33, GDPR which contains various requirements applicable to both controllers and processors with respect to the notification of personal data breaches to the relevant data supervisory authority. A preliminary draft of the DPC's decision was issued to Twitter Ireland on March 14, 2020 for the purposes of allowing Twitter Ireland to furnish its submissions. On April 27, 2020, a draft decision, taking Twitter Ireland's submissions into account, was prepared by the DPC. That draft decision was issued to other concerned supervisory authorities ("**CSAs**") on May 22, 2020, in accordance with Article 60, GDPR. Following this, and during the four-week timeframe provided for under Article 60(4), a number of CSAs raised objections to aspects of the draft decision. In particular, certain of the CSAs objected to the classification of Twitter Ireland as controller and Twitter Inc. as processor saying that both entities should properly be regarded as controllers, and arguing, relatedly, that the designation of both entities as controllers would have had implications, for example, for determining the moment of awareness of the breach.

Following receipt of the CSAs' objections, the DPC submitted the matter to the consistency mechanism referred to in Article 63, as is required by Article 60(4), GDPR. 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 relevant and reasoned objections. Following the completion of that dispute resolution process, on November 17, 2020, the EDPB notified its decision to the DPC finding that whilst the CSAs' objections, for the most part, were validly made, they did not meet the necessary threshold of providing clear demonstration as to the significance of the risks posed by the DPC's draft decision as regards the fundamental rights and freedoms of data subjects. The EDPB did, however, require the DPC to re-assess the elements it had relied upon in its draft decision to calculate the fine that was to be imposed (which in the draft decision was assessed at $150,000 to $300,000) "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." In particular, the EDPB found that the DPC should "have given greater weight to the element relating to the nature, scope and negligent character of the infringement" and that "the proposed fine range should be adjusted accordingly."

In accordance with Article 65(6), GDPR, the DPC issued its final decision on December 9, 2020.

OBLIGATIONS UNDER GDPR TO NOTIFY AND TO DOCUMENT BREACHES

The DPC's inquiry focused on Twitter Ireland's compliance with the provisions of Article 33, GDPR.

Article 33(1) requires (in relevant part) that data controllers notify personal data breaches to the relevant data supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." Recital 87 further requires that "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." Data processors have a role in breach notification under GDPR, being required under Article 33(2) to notify controllers without undue delay after becoming aware of a personal data breach.

Article 33(3) sets out detailed requirements for the content of the notification which must include (at least): (i) a description of 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; (ii) the name and contact details of the DPO or other contact point where more information can be obtained; (iii) a description of the likely consequences of the personal data breach; and (iv) a description of 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(5), GDPR requires data controllers to "document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken" so that "[t]hat documentation shall enable the supervisory authority to verify compliance with [Article 33]."

THE DPC'S DECISION

The Obligation to Notify

In its final decision issued on December 9, 2020, the DPC concluded that Twitter Ireland had not complied with its obligations under Article 33(1). In reaching this conclusion, the DPC noted that the requirement under Article 33(1), that a data controller notify a breach within 72 hours after having become aware of it, 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. 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. On this basis, the DPC found that it is the controller's responsibility 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).

The DPC's final decision highlights some specific issues that arise in connection with the controller-processor relationship (in this case, the relationship between Twitter Ireland (the controller) and its US parent company Twitter Inc. (the processor)) in the context of data breach notifications. It found that 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. The DPC emphasised that it is the controller's responsibility to oversee the processing operations carried out by its processor and, as part of this, to ensure (by means of effective protocols) 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). 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 an 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.

The DPC applied the controller's liability strictly noting that where a controller does not ensure that it has effective protocols in place for breach notification by its processor, and/or where such a process fails or is not followed correctly by the processor, thereby resulting in a delay or failure in the processor making the controller aware of the breach, then the controller is 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. The DPC found that such an interpretation 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 under the scheme of GDPR.

In this case, Twitter Ireland had confirmed that Twitter Inc. assessed the issue as potentially being a personal data breach on January 3, 2019. As a result of "the ineffectiveness of the process in the particular circumstances which transpired" in this case "and/or a failure by Twitter Inc. staff to follow its incident management protocols" (this point having been admitted by Twitter Ireland), Twitter Ireland was not notified of the incident by Twitter Inc. until January 7, following which it notified the DPC of the breach on January 8. Notwithstanding that Twitter Ireland was not actually aware of the breach until January 7 (and thus reported the breach within 24 hours of its actual knowledge, and within the timeframe envisaged by Article 33(1) GDPR), the DPC found that it ought to have been aware of the breach at an earlier point in time, at the latest by January 3, 2019 and that any arrangements with Twitter Inc. should have enabled this. The DPC concluded on Article 33(1) that any alternative application 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), would undermine the effectiveness of the Article 33 obligations on a controller and would be at odds with the overall purpose of GDPR.

The Obligation to Document

In considering whether Twitter Ireland had complied with Article 33(5) in documenting the breach, the DPC undertook a thorough analysis of the detailed information that should be documented pursuant to the various sub-paragraphs of Article 33 as well as a thorough assessment of the various pieces of information furnished by Twitter Ireland in the course of its notifying the breach. The DPC found ultimately that Twitter Ireland had failed to comply with its obligations under Article 35(5) in that the information furnished by it did not contain sufficient detail so as to enable the question of its compliance with the requirements of Article 33 to be verified. Twitter Ireland had produced an "Incident Report" which it submitted was the primary record in which it documented the facts, effects, and remedial action taken in respect of the breach. But the DPC found that the Incident Record was not a sufficient record for documenting of the breach on the basis that it failed to contain all material facts relating to the notification of the breach. In particular, the DPC highlighted that the report did not contain any reference to, or explanation of, the issues that led to the delay in Twitter Ireland being notified of the breach. In addition, the Incident Report did not address how Twitter Ireland assessed the risk, arising from the breach, to affected users.

The DPC also found that some other documentation that had been furnished by Twitter Ireland contained "disparate" items of limited information relating to the facts of the breach and its impact on users, but that these items (either individually or collectively) did not contain sufficient information for the purposes of verifying Twitter Ireland's compliance with Article 33. The DPC criticized the documentation provided by Twitter Ireland as being of a too "generalized" nature, that could not be said to comprise a record or document of the personal data breach within the terms of Article 35(5). Finally, the DPC observed that the deficiencies in the documentation furnished by Twitter Ireland as a "record" of the breach were 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.

IMPLICATIONS

The DPC's decision demonstrates the vital importance of ensuring that both the necessary processes are in place between controllers and processers to ensure swift notification by the processor to a controller on its becoming aware of a breach and that those processes are implemented in practice. Where a controller relies on a group company to process personal data on its behalf, individuals within that group company involved in such processing (including the notification of any breaches arising out of such processing) should be trained on the various requirements of GDPR, and the potential consequences of failing to comply with such requirements. Where a controller engages an external processor, the controller should be satisfied that the protocols and processes required to ensure compliance with GDPR are put in place and properly implemented. The DPC's decision makes clear that a controller cannot hide behind a failure by its processor to implement agreed processes and protocols. The controller is responsible to ensure that any procedures that are put in place are properly followed.

The DPC's decision also highlights the strict manner in which the steps that a controller must take to notify breaches of personal data under GDPR will be applied. A delay of just a few days in this case was sufficient to justify a fine under GDPR. In addition, the documentation that was provided by Twitter Ireland in connection with the breach was rigorously analyzed by the DPC and was ultimately found to be insufficient to enable the DPC to verify compliance with the provisions of GDPR concerning breach notification.

The fine imposed on Twitter Ireland, was a fraction of the maximum fine that could have been levied (which the DPC estimated to be some $60 million), and the multi-million dollar fines imposed by other European data supervisory authorities under GDPR. Indeed, the EDPB as part of its binding decision rendered pursuant to Article 65, GDPR required the DPC to reconsider the fine that had been proposed in its draft decision to ensure that it fulfilled the purpose of administrative fines rendered under GDPR as a corrective measure. In its final decision, when re-considering the level of fine to impose, the DPC highlighted that it considered the breaches to be due to an isolated failure (as opposed to their being indicative of broader, more systemic issues). The DPC also found that the breaches were negligent as opposed to intentional in nature and that the steps taken by Twitter Inc. to rectify the bug were a mitigating factor in the level of the fine. Ultimately, whilst the fine issued by the DPC in this instance appears to be relatively low, companies subject to GDPR should not assume that the DPC will be similarly restrained in the future.

* * *

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.