Facebook Fined $18.6M over String of 2018 Breaches of EU's GDPR

Description

USA: Facebook's parent company, Meta, has been fined €17 million (~$18.6 million) by the Irish Data Protection Commission (DPC) over a string of historical data breaches.

The security lapses in question, which appear to have affected up to 30 million Facebook users, date back several years — and had been disclosed by Facebook to the Irish regulator in 2018.

The DPC, which is Meta/Facebook's lead privacy regulator in the European Union, opened this security-related inquiry in late 2018 after it received no less than 12 data breach notifications from the tech giant in the six-month period between June 7, 2018 and December 4, 2018.

The European Union's General Data Protection Regulation (GDPR) — which came into application in May 2018 — puts a legal requirement on data controllers to swiftly disclose breaches of personal data to a supervisory authority if the leak of information is likely to pose a risk to individuals. (The most serious breaches should be notified within 72 hours.)

"The inquiry examined the extent to which Meta Platforms complied with the requirements of GDPR Articles 5(1)(f), 5(2), 24(1) and 32(1) in relation to the processing of personal data relevant to the twelve breach notifications," the DPC wrote in a press release announcing a final decision on its Facebook inquiry.

"As a result of its inquiry, the DPC found that Meta Platforms infringed Articles 5(2) and 24(1) GDPR. The DPC found that Meta Platforms failed to have in place appropriate technical and organisational measures which would enable it to readily demonstrate the security measures that it implemented *in practice* to protect EU users' data, in the context of the twelve personal data breaches."

In a statement responding to the DPC's penalty, a Meta spokesperson sought to play down the episode as merely a case of historically lax record-keeping — writing:

This fine is about record keeping practices from 2018 that we have since updated, not a failure to protect people's information. We take our obligations under the GDPR seriously, and will carefully consider this decision as our processes continue to evolve.

The penalty announced by the DPC is the first final decision from Ireland on a GDPR investigation against Facebook itself since the regulation begun being applied nearly four years ago — although the regulator did issue a separate (larger) sanction against Facebook-owned WhatsApp last year for violations of transparency rules.

The DPC confirmed that its draft decision on this Facebook inquiry had faced some objections from other EU data protection authorities — something that also occurred in an earlier probe of a Twitter security breach, as well as over the transparency decision on WhatsApp. (And in both those cases the GDPR's dispute resolution mechanism led to higher penalties being issued than Ireland had proposed.)

The DPC said two other authorities raised objections to its draft decision on this Facebook inquiry. But Ireland does not specify whether the fine was increased as a result of the objections, nor which authorities objected (or why).

It's notable that the penalty is relatively small — certainly it's a far cry from the theoretical maximum of 4% of Meta's global annual turnover (which would be well over a billion dollars).

However the DPC handed an even smaller fine (~$550,000) to Twitter at the end of 2020, also over administrative failings around a security breach notification.

While there are likely variations in what went wrong in each case, it's pretty clear that security breaches that are assessed by EU authorities as unintentional are likely to attract lower penalties than systemic or flagrant rule violations.

It also follows that a whole string of lapses has netted Facebook a larger penalty than Twitter, which had only been reporting a single breach (not a full dozen).

Major token hack

The details of all 12 security lapses Facebook 'fessed up to over the six-month period of 2018 are not listed by the DPC in its announcement of the sanction — but in September 2018 the tech giant publicly disclosed a major hack, which it suggested affected at least 50 million accounts after hackers exploited a security vulnerability on the site.

Facebook subsequently claimed that only 30 million users had actually had their tokens stolen in the hack.

The bug, which dated back to July 2017, had allowed hackers to obtain account access tokens which are used to keep users logged in when they enter their username and password — meaning that stolen tokens can allow hackers to break into accounts.

That major token hack wasn't the only security lapse for the tech giant in 2018, though.

In June, Facebook notified users of a bug which had created a vulnerability for several days the month

before, which it said had accidentally changed the suggested privacy setting for status updates to public from whatever users had set it to last — potentially causing up to 14 million users to over-share sensitive friends-only content with strangers.

Another bug we reported on, in November 2018, had allowed any website to pull information from a Facebook user's profile — including their "likes" and interests — without the person's knowledge.

And later that same year, in December, Facebook publicly disclosed a Photo API bug that it said had given app developers too much access to the photos of up to 5.6 million users.

This string of security lapses followed hard on the heels of the Cambridge Analytica story breaking into a global scandal — in March 2018 — when revelations of Facebook user data being sucked out of its platform to be repurposed for targeted advertising by the Trump campaign, which was seeking to opaquely influence the U.S. elections, wiped billions of dollars off its share price.

The Cambridge Analytica scandal also led lawmakers and regulators around the world to dial up their scrutiny of Facebook's handling of people's information — and has, ultimately, contributed to accelerating moves to overhaul and beef up regulation of digital platforms (such as the U.K.'s incoming Online Safety legislationor the EU's Digital Services Act).

But since the Cambridge Analytica scandal predated the GDPR coming into force, Facebook largely escaped direct regulatory sanction in Europe over that particular episode. Had the timing been a little different it might now be on the hook for a rather larger penalty.

The U.K.'s Information Commissioner's Office did fine Facebook £500,000 over Cambridge Analytica, the maximum possible under its pre-GDPR data protection regime. Although Facebook challenged the regulator's decision — before going on to agree to drop its appeal and pay the fine to settle with the ICO without admitting liability. It later emerged that the ICO had agreed to be gagged over the terms of that settlement.

The final results of full platform app audit Facebook claimed it would undertake in the wake of the Cambridge Analytica scandal, in a bid to reassure users it was purging bad actors and locking down user data, meanwhile, never saw the light of day.

Since then the GDPR has brought in tougher legal regime against data abuse — at least across the EU (the U.K. is no longer a member state) — however long delays between data scandals and enforcement continue to impede smooth working of the regulation.

Ireland's wider record on cross-border cases means a single decision against Facebook now is unlikely to do anything to ease trenchant criticism of its pace of GDPR enforcement against big tech — not least given that multiple other Facebook inquiries remain undecided. (And, as we reported yesterday, the DPC is now being sued for inaction over a separate GDPR complaint targeted at Google's adtech.)

It's thus likely no accident that — also today — the regulator elected to publish a report on its handling of cross-border GDPR cases.

Among the stats it chooses to spotlight are the following claims (covering the period May 25, 2018 to December 31, 2021):

- 1,150 valid cross-border complaints have been received by the DPC; 969 (84%) as lead supervisory authority (LSA) and 181 (16%) as a concerned supervisory authority (CSA).
- 588 (61%) cross-border complaints handled by the DPC as the LSA were originally lodged with another supervisory authority and transferred to the DPC.
- 65% of all cross-border complaints handled by the DPC as the LSA since May 2018 have been concluded, with 82% of those received in 2018 and 75% in 2019 now concluded.
- Of the 634 concluded cross-border complaints handled by the DPC as the LSA, 544 (86%) were resolved through amicable resolution in the interests of the complainant.
- 72 (22%) open cross-border complaints are linked to an inquiry and will be concluded on the finalisation of the inquiry. A large number of the remaining open complaints from 2018 and 2019 are linked to an inquiry.
- 86% of all cross-border complaints handled by the DPC as the LSA relate to just 10 data controllers.
- 38% of complaints transferred by the DPC to other EU/EEA LSAs (excluding the UK) have been concluded.

*

By Natasha Lomas

Featured image is from TechCrunch

Category

1. Economy-Business-Fin/Invest
2. Main
3. Politics-Geopolitics-Gov.-Events

Date Created
03/17/2022