£25,000 ICO fine is no drop in the ocean for Mermaids

Published 27 July 2021

On 8 July 2021, the ICO exercised its powers under Article 83 of the GDPR and published a £25,000 monetary penalty notice[1] ("**MPN**") to British gender variant and transgender youth charity, Mermaids, for the familiar failure to implement adequate technical security measures to keep its users' personal data secure, infringing Articles 5(1)(f) and 32 of the GDPR.

Whilst £25,000 appears to be a relatively modest fine in comparison to the penalties we have seen handed out by the ICO against the likes of British Airways and Marriott International, when put in context, Mermaids' fine in fact represents 2.8% of the charity's annual turnover. This is a far higher turnover percentage than those issued to corporate giants British Airways (1.5%) and Marriott (less than 1%) following their large-scale multi-national data breaches. It is noteworthy that the MPN expressly states that Mermaids' total income over the past three years was a relevant factor in determining the amount of the penalty.

The Mermaids fine serves as a salutary message to organisations of all sizes and sectors, including charities, that they too can face the full force of the ICO's enforcement powers if they take "*a negligent approach towards data protection*" because "*whilst we acknowledge the important work that charities undertake, they cannot be exempt from the law*" (Steve Eckersley, Director of Investigations).

What happened?

Mermaids is a charity which offers support to gender-diverse children, young people and their families. The ICO's investigation focused on an internal email group (GeneralInfo@Groups.IO) set up and used by Mermaids between August 2016 and July 2017. It was not until 14 June 2019 that Mermaids was notified by a service-user that these internal emails were publicly available online. The mother had been contacted by a Sunday Times journalist who, via a search engine, found confidential emails which included her telephone number and information relating to her child's mental and physical health. Mermaids received a notice from the Sunday Times in respect of their intention to publish an article about it.

The email group was listed in the Groups.IO search directory and indexed on large search engines such as Google. As a result, the emails were accessible to third parties and comprised personal data relating to a "*large group*" of 550 data subjects, 4 of whom were children.

Mermaids was criticised for not having any record or documentation which explained exactly how the group email service was created. They were unable to determine whether the emails were left accessible deliberately (to facilitate a general discussion) or whether it was an oversight not to select a more secure option. In any event, the default security settings that had been applied were determined to be "*insecure and inappropriate*".

Key takeaways

"*The likely increased vulnerability of a data subject in turn increases the risk of damage or distress*".

The Commissioner highlighted that the topic of gender incongruence is still regarded as a controversial and sensitive issue and can lead to increased vulnerability when considering the potential harm to affected data subjects as they "*may be at a higher risk of experiencing prejudice, harassment, physical abuse or hate crime*".

In regard to 15 of the affected data subjects, the emails included special category data, such as details of mental or physical health, sex life or sexual orientation. However, the ICO also considered conversations about transgender issues and individuals' personal experiences were sensitive in context and it was confirmed by those affected data subjects that the breach caused significant damage and distress, regardless of whether or not special category data was also disclosed.

"*An aggravating factor is the duration of the infringement…*"

Although the last email was sent on 21 July 2017, the internet-based email group remained searchable and viewable online until remedial action was taken almost two years later, in June 2019. The Commissioner noted that there was no clear documentation to demonstrate how the email group was created or decommissioned, but remained accessible to third parties and appeared to have been forgotten. Access could have easily been restricted to approved members of the email group had appropriate restricted access settings been set up.

"The nature of the contraventions is unaffected by the unanswered question as to the extent to which any other third party or parties accessed the data."

In other words, the number of unauthorised views does not matter. The ICO was unable to determine the extent of unauthorised views by any third party or parties, however, this had no mitigating impact on the ICO's assessment as to the gravity of the breach. Further, the significance of the contraventions was unaffected by the ease in which other third parties could have accessed the data, whether that be by accident or only if by using a precise and unusual syntactical search.

"Data protection policies were inadequate and there was a lack of adequate training, including a lack of face-to-face training, on data protection"

Despite the fact that mandatory data protection training was provided to all Mermaids' staff and volunteers, and updated on an annual basis, the ICO considered that given that the ongoing contraventions were not identified by anyone at Mermaids, it demonstrated that the training was inadequate and/or ineffective and that "there was a negligent approach towards data protection".

The Commissioner expressly acknowledged the profile that Mermaids had raised in recent years and concluded that: *"Regulatory action against Mermaids will serve as an important deterrent to other entities or persons who are not complying or who are risking not complying with their duties under the GDPR."*

[1]https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf

Authors

Camilla Elliot
London - Walbrook
+44 (0)20 7894 6363
celliot@dacbeachcroft.com

DAC BEACHCROFT