CLIENT NOTE

THE FIRST MASSIVE FINES UNDER THE EU GDPR

25 July 2019

For any queries relating to this article,

please contact:

Tan Tee Jim, *S.C.*

Partner, Intellectual Property

DID: 6557 4615

tanteejim@leenlee.com.sg

Zechariah J.H. Chan

Partner, Intellectual Property

DID: 6557 4710

zechchan@leenlee.com.sg

Tan Sih Im

Associate, Intellectual Property

DID: 6557 4612

tansihim@leenlee.com.sg

Authors:

Tan Tee Jim, *S.C.*

Zechariah J.H. Chan

Tan Sih Im

Introduction

1. When the European Union ("**EU**") General Data Protection Regulations ("**GDPR**") first came into force in May 2018, it was difficult to ascertain how aggressively it would be enforced. Whilst the maximum imposable fine of €20 million or 4% of total worldwide turnover is statutorily prescribed, there was scant case law on benchmark sentencing tariffs.

2. However, recent decisions by the UK Information Commissioner's Office ("**ICO**") to fine British Airways and Marriott International a cumulative £282.6 million have shed light on just how far EU's regulatory authorities will flex their regulatory muscles under the new regime.

British Airways fine

3. On 8 July 2019, the UK Information Commissioner's Office ("**ICO**") issued a notice of intention to fine British Airways a record £183.39 million for GDPR breaches. This constitutes roughly 1.5% of British Airways' annual revenue.

4. The proposed fine relates to a cyber incident in June 2018. User traffic to the British Airways website was diverted to a fraudulent site, where sensitive personal data of about 500,000 customers were harvested by attackers. The personal data included names, email and residential addresses, and log-in, travel, and credit card details of the customers.

5. Following investigations, the ICO found that British Airways had poor security arrangements which ultimately compromised its customers' personal data.

Marriott International fine

6. Just one day after the ICO's notice of intention to fine British Airways, the ICO issued a similar notice of intention to fine US hotel conglomerate, Marriott International, £99.2 million for GDPR infringements.

7. This proposed fine relates to a cyber incident in 2014 in which

personal data in 339 million guest records were exposed. Approximately 30 million of these records related to residents of the EU.

8. According to the ICO's investigations, the security vulnerabilities which ultimately culminated in the personal data exposure had begun when the systems of the Starwood hotels group were compromised in 2014. Marriott International subsequently acquired the Starwood hotel group 2 years later. However, the exposure of customer information was not discovered until 2018. Investigations revealed that Marriott International had failed to undertake sufficient due diligence when it bought Starwood, and should have done more to secure its systems.

9. In an official statement from the ICO, its Information Commissioner, Ms Elizabeth Denham, said:

> "*The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include* ***carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected***." (emphasis added)

10. It is pertinent to note that these security vulnerabilities began and existed in the Starwood hotels group *before* Marriott International had acquired the group. Yet, Marriott International was held accountable for these security lapses for failing to conduct sufficient due diligence into Starwood's privacy protocols.

Hard-line approach towards data protection

11. The ICO will consider representations by both British Airways and Marriott International before reaching its final decision. Therefore, the final quantum of the penalties imposed on both conglomerates remains to be seen.

12. However, one fact remains clear: the draconian fines proposed by the ICO against both groups herald a new aggressive approach towards data protection in the EU.

13. For context, Facebook was only fined £500,000 in 2018 for giving third party app developers access to individuals' personal data without clear consent from 2007 and 2014 in the Cambridge Analytica data scandal. This £500,000 fine imposed was the then-maximum allowed under the old data protection rules which have been superseded by the GDPR.

Conclusion

14. As highlighted in our article, the GDPR has extraterritorial reach and would apply to:

> "*the processing of personal data of **data subjects who are in the Union by a controller or processor not established in the Union**, where the processing activities are related to:*
>
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to **such data subjects in the Union**; or*
>
> *(b) the monitoring of their behaviour as far as their **behaviour takes place within the Union**.*" (emphasis added)

15. Therefore, Singapore organisations with a business presence in the EU should be aware of the extraterritorial reach of the GDPR and should seek advice on GDPR compliance.

16. For more information about the differences between the Singapore Personal Data Protection Act 2012 and the GDPR, please refer to our article.

The following partners lead our departments:

Kwa Kim Li
Managing Partner
kwakimli@leenlee.com.sg

Quek Mong Hua
Litigation & Dispute Resolution
quekmonghua@leenlee.com.sg

Owyong Thian Soo
Real Estate
owyongthiansoo@leenlee.com.sg

Tan Tee Jim, S.C.
Intellectual Property
tanteejim@leenlee.com.sg

Adrian Chan
Corporate
adrianchan@leenlee.com.sg

Louise Tan
Banking
louisetan@leenlee.com.sg