NAME: STEPHEN KYALO -ADC-DP01-25005
PROGRAM: DATA PROTECTION SPECIALIST
TOPIC: GDPR CASE STUDY

REFERENCES

https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta , **The Guardian, 22nd May 2023**

1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board, **European Data Protection Board, 22nd May 2023**

Google fined record £44m by French data protection watchdog, **The Guardian, 21st Jan 2019**

Google Fined $57M by Data Protection Watchdog Over GDPR Violations | Digital Guardian **Fortra, 21st Jan 2019**

ICO statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, **European Data Protection Board, 9th July 2019**

GDPR Case Study: Marriott International, by Paul Biberstein, Brown University, Sreshtaa Rajesh, Brown University

1. **FACEBOOK GROUP**

In 2020, a ruling by the European Court of Justice was passed requiring **Meta Platforms Ireland Limited (Meta IE)**, a Meta subsidiary responsible for Meta's operations in the EU, to comply with the Standard Contractual Clauses(SCCs) established by the European Union. **SCCs** are legal tools approved by the EU that organisations can use to transfer personal data from the European Economic Area (EEA) to countries outside the EEA that do not offer an adequate level of data protection, as defined under the **GDPR.**

In 2021, a data leak exposed the personal information of up to 500 million Facebook users. This instigated an investigation by the **Irish Data Protection Commission** focusing on Facebook's compliance with GDPR's data protection principles. Upon investigation, **Meta IE was found to be in breach of GDPR by continuing to transfer user data from the EU to the US without the proper safeguards as stipulated in the SCCs**. In 2023, A record **fine of €1.2bn (£1bn)** was imposed on Meta IE by the Irish Data Protection Commission. Meta IE was mandated to put into place rigorous safeguards within a six-month timeframe following the ruling.

In response to the data breach, **Facebook implemented changes to its systems. Firstly, it disabled the ability for unauthorised individuals to scrape data from the platform**. Although the company did not reveal the specific methods used, it indicated that it was strengthening its defences to prevent similar attacks in the future.

The 2021 Facebook breach was an **intrusion on users' privacy and security**. With their names, phone numbers, locations, birth dates, and,

in some cases, email addresses in the public domain, **identity theft and privacy violations became a major concern**. This left many users wondering whether Meta was concerned about protecting their data. The leak eroded trust in Facebook and raised questions about the possibility of data exploitation.

2. GOOGLE GROUP

In 2018, a complaint was filed by an Austrian data privacy group, **None of Your Business(NOYB) and France's citizen advocacy group La Quadrature du Net** against Google. The case was filed with France's **CNIL (National Commission on Informatics and Liberty)**. **Google was accused of accussed of using users' data from across its various platforms**, including YouTube, Google Maps, among others, **in ad personalisation without the clear and proper consent from their users**. According to CNIL, the consent Google carries isn't specific enough, and this makes it difficult to understand the extent to which its data is used. Google was also found liable for splitting essential information into different pages. Users also found it difficult to request the data Google was collecting about them and how it was being distributed.

Google's actions breached the **Transparency and Consent principles of the GDPR**. Transparency was breached due to Google failing to provide sufficient information as to how they were collecting, processing, storing and utilising data from the users. CNIL found that Google failed to obtain valid consent for data processing. The consent mechanisms in

place were found not to be specific, resulting in uninformed users as to the extent of data processing.

Ultimately, Google was found liable and fined a **penalty of €50,000,000,** the highest at the time**.** Although Google filed for an appeal, France's highest administrative court, Conseil d'Etat, upheld the CNIL ruling. This case marked the first significant enforcement of GDPR on major tech companies.

The implications arising from this case emphasise the necessity for organisations to secure explicit, informed, and specific consent from users regarding the collection and use of their data. This means that organisations must clearly outline what data will be collected, how it will be used, and the purposes behind its use. Additionally, these organisations must provide use**rs with comprehensive and easily understandable information about their data collection practices**, including options for users to manage their data preferences. By doing so, organisations can build trust with their users and ensure compliance with data protection regulations.

3. MARRIOT INTERNATIONAL

In 2014, sophisticated **cyber attackers successfully breached the reservation systems of Starwood Hotels and Resorts**. This breach granted the attackers unrestricted access to a vast reservation database containing **sensitive information about hotel guests, including names, addresses, phone numbers, email addresses, and passport numbers**. Two years later, in 2016, **Starwood Hotels was acquired by Marriott International.**

It wasn't until 2018 that the breach was discovered, drawing attention to the extent of the data compromise. A thorough investigation revealed that nearly **339 million guest records had been exposed**, making it one of the largest data breaches in history involving a hotel chain. **Marriott International promptly reported the incident to relevant authorities**, including the U.S. Federal Bureau of Investigation (FBI) and the **UK's Information Commissioner's Office(ICO)**, given that approximately 7 million guests affected were from the United Kingdom and 30 million guests from the European Economic Area.

ICO's investigation revealed Marriott failed to undertake **due diligence when acquiring Starwood Hotels and Resorts and should have done more to secure the systems**. "*GDPR clearly states that organisations are responsible and accountable for the 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*", as stated by the ***Information Commissioner, Elizabeth Denham.***

IOC found Marriott to violate Article 32(1. Any information that can be used to identify a person must be secured with appropriate security measures.) with minor infringements to **Article 33**(Data Controllers/ Processors upon a breach are required to inform the appropriate authorities of the breach within 72 hours, Marriott waited for 2 months to inform the ICO.) and **Article 34** (Upon a data breach Data controllers are required to inform the data subjects of the breach without delay and in clear language, Marriott was compliant on this but IOC noticed some shortcomings in their

communication; failing to give their call center phone number in the emails sent.)

On reviewing these violations ICO **imposed a fine of £99,000,000** on Marriott International in 2019. The fine would later be **reduced to around £18,000,000 due to Marriott's cooperation** during the ICO investigation and the improvements to the security arrangements since the realisation of the breach.

The Marriott-Starwood data breach highlights the critical **need for strong cybersecurity measures and due diligence in corporate acquisitions.** The breach stemmed from vulnerabilities in Starwood's systems before Marriott's takeover, **emphasising the importance of thorough security assessments.**

The Information Commissioner's Office (ICO) found Marriott violated Article 32 of the GDPR by failing to implement appropriate security measures and did not timely notify affected individuals, breaching Articles 33 and 34. This breach exposed millions of sensitive personal data points, demonstrating **organisations' accountability for the data they handle.**

The ICO's substantial fine, later reduced due to Marriott's cooperation, **underscores the serious consequences of non-compliance with data protection regulations**. This incident shows that data security is a critical aspect of corporate responsibility. Organisations must ensure rigorous evaluations of data protection practices to maintain compliance, avoid penalties, and preserve customer trust.