GDPR GETS SERIOUS - TWO RECORD-BREAKING CYBER FINES IN TWO DAYS

The ICO has proposed unprecedented fines against British Airways and Marriott International – how should businesses respond?

The UK privacy regulator, the Information Commissioner's Office (ICO), has issued notices of intention to impose fines of over GBP 280m on two international businesses for GDPR breaches, in particular because of their perceived data security failures. The UK's Information Commissioner, Elizabeth Denham has stated:

"For a fine to be dissuasive against a company that has a turnover in this stratosphere, we have to provide the fine accordingly.

This is not a small business. This is not a charity. This is a large business that you'd expect would take care of personal data".

The ICO has set a radical precedent in data liability for businesses, which are now required to invest in order to avoid similar fines, which may reach up to 4% of annual global turnover. The message is that enterprises, particularly those of scale and complexity, are expected to invest heavily in data and cyber compliance in proportion to their turnover.

The message is clear. The implications for regulatory projects extend beyond just technology businesses and there are lessons to build into your global data compliance frameworks, including in transactions and cyber security planning. A window-dressing compliance programme that has not fundamentally changed the way you handle data holds significant risk.

Key issues

- **Big fines**: Combined value of over GBP 280m in total for British Airways and Marriott International, Inc by UK privacy regulator, the ICO, for breaches of the GDPR.
- **Appeals**: Both companies have stated their intention to make representations to the ICO in order to contest the findings and sanctions.
- **Need for investment**: The potential fines shine a light on the importance of legal and technical investment in cyber risk.
- **Litigation risk**: Defending allegations of negligence by regulators requires a renewed focus on audit, testing, record keeping and technical investment.

BRITISH AIRWAYS

The Penalty

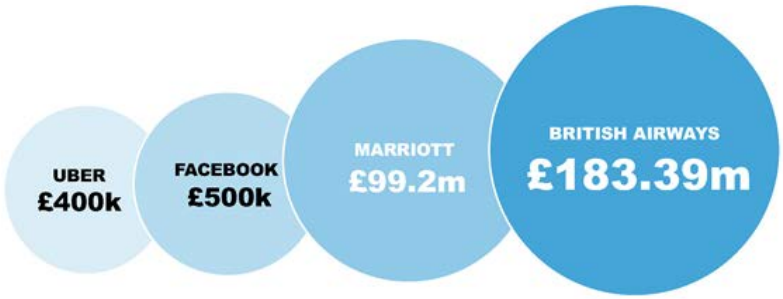
On 8 July 2019, the ICO issued a notice of intention to impose a record-breaking fine against British Airways Plc (BA) for infringements of the EU General Data Protection Regulation (GDPR).

The fine relates to a cyber incident, believed to have begun in June 2018, in which the personal data of approximately 500,000 BA customers was compromised.

The proposed GBP 183.4m fine equates to 1.5% of BA's global turnover for 2017. Under the GDPR, the maximum penalty for serious breaches is 4% of global turnover or EUR 20 million (whichever is the higher).

This is a significant increase on the maximum fine of GBP 500,000 under the previous UK regime, under which both Uber and Facebook have recently been fined for cyber-related incidents. BA will now be making representations to the ICO in respect of the proposed findings and sanction.

The ICO will review such representations from BA and other concerned data protection authorities before making a final decision.



The statement given on Monday by the Information Commissioner made it clear that the ICO will impose material sanctions on (and initiate investigations against) companies who fail to adequately protect personal data in their possession. How businesses handle incidents after discovery will not entirely mitigate liability – preparedness and being able to demonstrate this will hold importance:

"That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights".

What went wrong?

In June 2018, customers attempting to access the BA website were rerouted to a fraudulent web page, after which personal details including names, email addresses, credit card data, travel information and log in details were stolen by malicious actors. The incident was notified to the ICO in September 2018.

The company's responsiveness to the cyber incident has not been criticised by the ICO, which confirmed that BA has cooperated with its investigations and has since made improvements to its security arrangements in light of the breach. Instead, the ICO's view is that personal data had been put at risk through poor security arrangements at the company.

MARRIOTT INTERNATIONAL, INC

The Penalty

The ICO followed its announcement of the proposed BA fine with a second notice of intention to impose a fine of GBP 99.2m against Marriott International, Inc (Marriott) for infringements of the GDPR.

The Turkish privacy regulator, the KVKK, has also stated that it will be fining Marriott approximately EUR 234,000 and the business is subject to a number of class action lawsuits across the US.

As with BA, Marriott will now make representations to ICO, which the ICO will consider along with any contributions from other concerned data protection authorities before finalising its position.

What went wrong?

A variety of personal data, including approximately 339 million global guest records relating to residents in 31 countries in the European Economic Area, also containing credit card details, were stolen by malicious actors during a cyber incident impacting the company last November. Seven million of the compromised records related to UK residents, and the incident was notified to the ICO in the same month of the attack, in November.

The ICO has stated that the data vulnerability can be traced back to the comprised systems of Starwood hotels group (Starwood) which was acquired by Marriott in 2016. Crucially, the Starwood system was impacted in 2014, but this exposure was only identified in 2018.

The ICO has specifically flagged the insufficient due diligence undertaken when Marriott acquired Starwood, and has stressed that proper due diligence is a key accountability measure all organisations must comply with.

How have European regulators enforced the GDPR since May 2018?

There has not been a consistent approach taken to the size of penalties in enforcement of the GDPR across Europe. For similar cases relating to data security failings, regulators have applied significantly different levels of fines.

In January 2019, the French data protection authority, CNIL, imposed the then-highest fine for data protection violations to date on Google, which amounted to EUR 50 million.

The previous year, the Portuguese data protection authority, the CNPD, imposed a fine of EUR 400,000 on a Portuguese hospital.

In Germany, the local data protection authorities have imposed fines in approximately 100 cases to an aggregate amount of approximately EUR 450,000. The proposed fines in respect of BA and Marriott therefore go significantly beyond those which have been seen across Europe so far.

Nonetheless, there are no surprises from an ICO perspective. The ICO acknowledges that organisations should have predictability in understanding regulatory enforcement priorities, which is why the ICO has issued its Regulatory Action Policy. This document confirms the ICO's enforcement aims, priorities and approach. It provides that each case will be confirmed on its merits, but it is more likely that a penalty will be imposed where, for example:

- sensitive personal data has been involved;

- inaction is a feature of the incident; or
- there has been a failure to apply reasonable measures to mitigate the possibility of a breach.

This means that even preparedness is not enough, but a layer of audit, testing and practical implementation is required to future-proof the extent of sanctions. This will be more challenging in some areas, but the message is that doing nothing will not encourage a sympathetic response.

WHAT ARE THE GROUNDS OF APPEAL FOR BOTH BUSINESSES?

Section 162 of the Data Protection Act 2018 provides a right of appeal for those who are provided with an enforcement notice by the ICO. In order for a regulator to impose administrative fines for infringement of the GDPR under Article 83, the fine must be considered effective, proportionate and dissuasive, and due regard must be given to a number of factors listed under Article 83(2), including:

- the intentional or negligent character of the infringement;
- the nature, gravity and duration of the infringement;
- action taken by the business to mitigate the damage suffered by individuals;
- degree of responsibility of the business, taking into account security measures taken; and
- previous infringements of the business.

The appeal landscape in the UK is relatively untested, particularly for these size of fines. Any appeal will need to bring together a very convincing evidential trial to rebut allegations of negligence. Ask yourself – what could we show a regulator is they asked similar questions of us? You should also be aware of the guidance and regularity priorities disclosed by competent regulators. How does your preparedness and response map against the regulatory expectation in relevant countries?

3 LESSONS TO LEARN FROM THESE CASES

1. Audit and testing of cyber resilience is vital – this is a legal as well as technical workstream

Sophisticated testing plans, to match those of the depth and complexity in place for financial audit, should be designed to confirm compliance with GDPR standards. These require enhanced investment, and cross-team collaboration, but are the best way to demonstrate internally, and to regulators should they ask, that your GDPR compliance programme is not only live but also effective. Fines of scale will be challenging to issue if full control and risk

containment regarding the data you hold can be demonstrated through a deep and detailed paper trail.

2. Cyber due diligence must be a critical M&A diligence focus

Cyber risks can often be hidden. The old school approach of just asking a short set of questions regarding compliance during the diligence process is not good enough. Detailed legal interrogation of resilience must be matched with forensic testing of systems. Contractual frameworks in deal documentation to protect against risks attached to historic breaches must be far more robust. Deal protection should also contemplate the Target putting in place security measures to protect against future incidents. Risk for not observing these undertakings should be allocated and processes implemented to check compliance with these obligations.

3. If you are a business will significant turnover, you are expected to invest in GDPR compliance on an ongoing basis in accordance with your size – and this is not just a one-off investment

GDPR, and in particular cyber risk, is constantly changing and evolving. Investment in compliance on an ongoing basis, and not just treating this as a one off 'project', is the regulatory expectation – not just in the EU, but internationally. The link between level of turnover and level of investment is striking – if you are a large and sophisticated business, the ICO is indicating that your compliance programme should be similarly sophisticated.

STEPS TO TAKE NOW

1. **Cyber incident response plans:**
   - **map your business against global regulatory and reporting requirements** to create a plan that enables a strategic, controlled and effective incident / regulator response – this should build in reporting requirements beyond data and cyber alone;
   - **train your internal teams effectively** (including Legal, IT Security, HR, Communications, Compliance and Procurement) in the process and procedures of your cyber incident response so that you can efficiently deploy the cyber incident response plan;
   - **consider your internal communications plan** in the event of a cyber incident, to ensure that records are kept so that you will be able to defend the business's response, in the event of a regulatory investigation or civil claims. The communications plan should include consideration of how to ensure legal privilege (or its equivalent) is preserved; and
   - **regularly auditing your business and cyber incident response plan** through attack simulations and vulnerability analysis to ensure that your defences are effective.

2. **Business due diligence** - when acquiring a business, in addition to any legal due diligence, technical due diligence by qualified experts should be undertaken to identify critical cyber and data processes and weaknesses at an early stage.

   Appropriate warranties, undertakings and indemnity protection should be built in to transaction documents. The Information Commissioner specifically identified proper due diligence when making corporate acquisitions as a key accountability measure in the case of Marriott.

3. **Security and monitoring** - it is important to implement appropriate data security infrastructure and processes, including encryption, pseudonymisation as well as regular and effective perimeter testing with timely notifications, to allow you to meet regulatory reporting requirements if there is a breach.

4. **Data mapping and retention** - analyse and record what personal data is held in your business, where it is located, and for how long, in order to risk assess the potential impact of a cyber incident. Minimising the personal data that is held to that which is necessary mitigates the risk in the event of a cyber security incident.

5. **Your response team and culture** - ensure that you have an adequately qualified response team in place, including a chief information security officer (CISO). It is important that stakeholders of the business, including employees, culturally "buy into", and implement, best practice - policies alone are not enough.

6. **Liability analysis** - where your business outsources IT and cyber security services (or relies on third party providers), review the contractual provisions in respect of their liability in the event of a cyber incident.

   Ensure such provisions are broad enough, any liability caps high enough, and that limitations of liability are not too wide to enable your business to recover losses in the event of service delivery failings which contribute to a cyber incident. Do not simply accept that a limitation is "market" practice – this will differ by sector and risks identified in due diligence.

7. **Insurance** - consider taking specific cyber incident insurance to protect against the significant liability exposure of a GDPR breach. Where you have cyber insurance, review the policy terms to ensure you understand the breadth of coverage for your business. Where relevant in the M&A context, understand whether cyber risk is insurable in relevant jurisdictions and whether coverage exists, including in management discussions.

8. **Understand the global context** – these regulatory actions have been anticipated in regulatory commentary, action policies, and other enforcement actions. Ignoring the lessons from these actions simply because they do not reside in your sector is not the right approach. Read between the lines and understand the aspects which can help protect your business from future sanction or investigation.

WHAT NEXT?

The ICO has issued a warning shot. The question now is whether other regulators in Europe go even further – could 2019 bring the first billion Euro fine? To rebut allegations of negligence, the message is clear – implement detailed audit and testing, act on areas of weakness, and invest in privacy and cyber security compliance commensurate to your size.

CONTACTS

London

Jonathan Kewley
Partner

T +44 20 7006 3629
E jonathan.kewley
@cliffordchance.com

Jamie Andrew
Lawyer

T +44 20 7006 1367
E jamie.andrew
@cliffordchance.com

Sam Ward
Partner

T +44 20 7006 8546
E samantha.ward
@cliffordchance.com

Richard Jones
Director of Data Privacy

T +44 20 7006 8238
E richard.jones
@cliffordchance.com

Kate Scott
Partner

T +44 20 7006 4442
E kate.scott
@cliffordchance.com

Frankfurt

Susanne Werry
Senior Associate

T +49 69 7199 1291
E susanne.werry
@cliffordchance.com

Brussels

Pierre-André Dubois
Of Counsel

T +32 2 533 5066
E pierre.dubois
@cliffordchance.com

Tokyo

Luna Hiraoka
Senior Associate

T +81 3 6632 6327
E luna.hiraoka
@cliffordchance.com

Singapore

Paul Landless
Partner

T +65 6410 2235
E paul.landless
@cliffordchance.com

Washington

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

New York

Dan Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Paris

Dessi Savova
Partner

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com