MAYER | BROWN

July 2019

英当局、GDPR 違反で 2 社に合計 2 億 7,500 万ポンドの制裁金を科す方針

ICO to Impose Fines Totaling of £275 Million Against Two International businesses for GDPR violations

Information Commissioner's Office（データ保護当局）（以下、「ICO」）は、顧客の個人情報のサイバー攻撃対策を怠ったとみられる大手国際企業 2 社に欧州連合一般データ保護規則（以下、「GDPR」）違反で合計 2 億 7,500 万ポンドを上回る制裁金を科す方針を発表した。

ICO は今月 8 日（月）、2018 年 8 月に発生した顧客情報流出によりブリティッシュ・エアウェイズ（以下、「BA」）に 1 億 8,339 万ポンドの制裁金を科す方針を発表した。本件サイバー攻撃は 2018 年 9 月 6 日に公表され、BA のウェブサイトにアクセスしたユーザーが悪質サイトに誘導され、約 50 万人の個人名、メールアドレス、クレジットカードの情報を含む顧客情報が流出したとみられる。ICO によると、BA は調査に協力し、セキュリティ対策を強化したとされている。制裁金は、BA の 2017 年度の売上高の 1.5 パーセントの金額に値すると見込まれ、欧州連合におけるデータ保護監督機関が GDPR に基づいて科す制裁金としては過去最高額である。

翌日 9 日（火）、ICO は Marriot International, Inc.（以下、「マリオット」）に、Starwood 予約データベースの個人情報流出に関して、9,920 万ポンドの制裁金を科す方針を発表した。本件データ流出は、欧州経済領域（EEA）の 30 か国以上に及ぶ約 3700 万人の個人情報を含む、3 億 3000 万人の個人情報が流出したもので、2014 年に発生した Starwood ホテルシステムのサイバー攻撃が原因と考えられる。本件について ICO に通知が届いたのは、マリオットが Starwood 社を買収した約 2 年後の 2018 年 11 月であった。ICO は、マリオットは Starwood の IT システムの見直し及び強化などの適切な措置をとるべきであったと判断した。マリオットは ICO の調査に協力し、セキュリティ対策を強化した。

GDPR には 2 段階の制裁金があり、特定事項の違反には、1,000 万ユーロまたは前年売上高の 2 パーセントのうちより大きい金額、個人の権利侵害などより深刻な違反には、2,000 万ユーロまたは前年売上高の 4 パーセントのうち大きい金額が科される。

BA 及びマリオットが科される制裁金の金額は、いずれも上記の金額を下回るが、ICO が両社の調査協力とセキュリティ対策の改善を勘案して金額を減額したものと考えられる。両社には 28 日間の異議申立期間が設けられ、ICO は両社及び欧州各国当局の意見などを考慮した上で最終決断を下す。

ICO の声明文によると、BA 及びマリオットのいずれの件においても流出した個人情報の性質ではなく、セキュリティ対策の欠陥に着目したものであるように考えられる。さらに ICO は、買収対象企業が GDPR に従う必要がある場合、IT セキュリティ及びデータ保護システムに関するデュー・ディリジェンスの必要性を強調した。今回の件は、ICO が個人情報流出の取締りを強化しつつあり、欧州内外の

企業に関わらず、GDPR に従った万全なデータ保護及びセキュリティー対策を整えるべきであることを表している。ICO が GDPR の違反による制裁金を科したのは今回が初めてであり、英国が EU 離脱後に適用するコンプライアンスの基準を打ち出したと考えられる。

メイヤー・ブラウン法律事務所について

当事務所は、GDPR 対応の社内規定整備や、サイバー攻撃を受けた場合の当局への通知をはじめとした GDPR 上の対処法や解決法まで、幅広くクライアントをサポートしております。

こちらの動画は、ロンドンにおける知的財産・IT グループのリーダーを務める **Mark Prinsley** 弁護士及び同グループのアソシエイトである西川竜太弁護士が、データ保護や GDPR の日本企業への影響について解説いたします。>>リンク

こちらは、当事務所東京オフィスのシニア・アソシエイト、**安達弁護士**による GDPR 施行初年度に企業が受けた影響をまとめた記事を掲載。>>リンク

当事務所の上記記事掲載リンク:

UK ICO Intends to Fine Marriott over £99m for Personal Data Breach under the GDPR

British Airways Fined over £183m for Personal Data Breach Under the GDPR

GDPR 対策やサイバーセキュリティ・データプライバシーについてご質問などございましたら、下記弁護士までお問い合わせください。

お問い合わせ

Oliver Yaros
Partner, London
+44 20 3130 3698
oyaros@mayerbrown.com

Mark Prinsley
Partner, London
+44 20 3130 3900
mprinsley@mayerbrown.com

Gabriela Kennedy
Partner, Hong Kong
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Raj De
Partner, Washington DC
+1 202 263 3366
rde@mayerbrown.com

Lei Shen
Partner, Chicago
+1 312 701 8852
lshen@mayerbrown.com

安達　知彦
Senior Associate, Tokyo
+81 3 4563 1411
tomo.adachi@mayerbrown.com

ICO to Impose Fines Totaling of £275 Million Against Two International Businesses for GDPR Violations

The UK Information Commissioner's Office ("ICO"), a European data protection supervisory authority, has flexed its muscles and has announced its intention to issue fines exceeding £275 million against two international businesses for failing to keep the personal data they hold secure from cyber-attacks under the European General Data Protection Regulation ("GDPR").

On 8 July 2019, the ICO announced its intention to fine British Airways ("BA") £183.39 million under the GDPR for a personal data breach it suffered in August 2018. The breach, described as a "sophisticated, malicious criminal attack", was first disclosed by BA on 6 September 2018. Details of approximately 500,000 BA customers were compromised during the breach, which involved the diversion of user traffic from the BA website to a fraudulent website. The personal information compromised included names, email addresses and payment card details used during the booking process. The ICO indicated that BA cooperated with the ICO investigation and has made security improvements following the incident.

The penalty is reported to amount to about 1.5% of the global annual turnover of BA in 2017 and is the highest fine issued so far by a European Union data protection supervisory authority for a personal data breach under the GDPR.

On 9 July 2019, the ICO announced its intention to fine Marriott International, Inc. ("Marriott") £99.2 million under the GDPR for a personal data breach that occurred in relation to the Starwood guest reservation database system. The breach is believed to have started when Starwood hotels systems were affected by a cyber-attack in 2014. The breach was uncovered and notified to the ICO in November 2018, two years after Starwood's acquisition by Marriott. Personal data contained in over 330 million guest records were exposed by the incident. About 30 million records related to individuals from over 30 countries in the European Economic Area (EEA). Approximately 7 million records related to individuals located in the UK. The ICO determined that Marriott should have taken additional steps to review and secure the IT infrastructure used by Starwood. The ICO noted that Marriott had co-operated with the investigation conducted by the ICO and had improved its security practices since the incident.

The GDPR established two tiers of penalties that can be issued by European data protection supervisory authorities; the standard maximum and the higher maximum. The standard maximum allows for a fine equal to the greater of 10 million Euros or 2% of total annual worldwide turnover in the preceding financial year of the relevant undertaking for a violation of certain provisions, whereas the higher maximum allows for the greater of 20 million Euros or 4% of the total annual worldwide turnover in the preceding financial year of the relevant undertaking for a violation of more serious provisions, including data protection principles or data subjects' rights.

The penalties issued to BA and Marriott fall below both of these thresholds, which may reflect BA and Marriott's cooperation with the ICO investigation and that those organizations have made improvements to its security practices since the incidents were discovered. Both organizations have 28 days to make further representations to the ICO about the calculation of the fine before the ICO makes its final decision. The ICO has said that it will carefully consider any representations made by them and the other European data protection authorities before it takes its final determination.

In both cases, the focus of the ICO's statements of intent seems to be on the security failures that led to the breach occurring, rather than necessarily being on the types and sensitivity of personal data affected. The ICO also focused on the requirement to conduct an appropriate due diligence process into the IT security and data protection practices of a future target of any M&A activity where that target is subject to the GDPR. No matter how breaches happen, it is clear that the ICO is taking security breaches very seriously and these events should serve as a strong reminder to companies to

get their house in order in order to comply with the security and other obligations under the GDPR, which applies to businesses both in Europe and outside of Europe. Being the first two fines it has issued under GDPR for a personal data breach, the ICO in particular could be approaching these episodes as an opportunity to "set out its stall" with respect to future enforcement action, with its eye on setting the standard of compliance in the UK in a post-Brexit environment.

At Mayer Brown, we have advised clients operating across a range of sectors on how to comply with the GDPR requirements. We have also advised a number of clients that have suffered cyber-attacks on how to respond to those types of security incidents in accordance with their GDPR and other legal obligations. In particular, we have experience of the types of issues that have been encountered responding to that type of incident, how to conduct the GDPR review and notification process, the questions that the ICO, other authorities, clients and others typically ask and the other types of issues that create difficulties for our clients.

Mark Prinsley, head of the Intellectual Property & IT group in London and Ryota Nishikawa, London based associate in the Intellectual Property & IT Group, discuss the relevance of data protection and GDPR for Japanese business. *>> Click here*

Bylined article by senior associate **Tomo Adachi** (Tokyo) summarizing the key impacts and trends that we have seen in the first year of the GDPR regime. *>> Click here*

For further details on these fines please see:
UK ICO Intends to Fine Marriott over £99m for Personal Data Breach under the GDPR

British Airways Fined over £183m for Personal Data Breach Under the GDPR

For further information about our GDPR Readiness Service and our Cybersecurity & Data Privacy Practice, please contact any of the lawyers identified below or your usual Mayer Brown contact.

Contacts

Oliver Yaros
Partner, London
+44 20 3130 3698
oyaros@mayerbrown.com

Mark Prinsley
Partner, London
+44 20 3130 3900
mprinsley@mayerbrown.com

Gabriela Kennedy
Partner, Hong Kong
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Raj De
Partner, Washington DC
+1 202 263 3366
rde@mayerbrown.com

Lei Shen
Partner, Chicago
+1 312 701 8852
lshen@mayerbrown.com

Tomo Adachi
Senior Associate, Tokyo
+81 3 4563 1411
tomo.adachi@mayerbrown.com