PENALTY NOTICE

Section 155, Data protection Act 2018

Case ref: COM0804337

Marriott International Inc
10400 Fernwood Road
Bethesda
MD20817
USA

30 October 2020

1. INTRODUCTION & SUMMARY

1.1. This Penalty Notice is given to Marriott International Inc ("**Marriott**") pursuant to section 155 and Schedule 16 of the Data Protection Act 2018 (the "**DPA**"). It relates to infringements of the General Data Protection Regulation (the "**GDPR**"), which came to the attention of the Information Commissioner ("**the Commissioner**") as a result of an attack on Marriott's IT systems[1] that took place over a period that included 25 May 2018 to 17 September 2018 (the "**Attack**").

1.2. In summary, in 2014 the IT systems of Starwood Hotels and Resorts Worldwide Inc ("**Starwood**") were compromised by an unknown attacker or attackers (referred to, for ease of reference, as "**the Attacker**"), utilising an unknown attack vector. In 2016, Marriott acquired Starwood. Marriott did not detect the Attack at any time between acquiring Starwood and September 2018, including in the period after the entry into force of the GDPR in May 2018. During this latter period, the Attacker continued to traverse through the Starwood systems and had gained access to the cardholder data environment within the Starwood network. This access allowed the Attacker to export the personal data of Starwood customers to "dmp" files on the Starwood systems, potentially with a view to taking a copy of that data. It was only when the Attacker triggered an alert in relation to a table containing cardholder data that the Attack was discovered and could be mitigated. The personal data of a large number of individuals was involved in the Attack, including cardholder data, although the Commissioner has not seen any evidence of financial harm to individuals. Following the alert, Marriott promptly informed affected data subjects and took immediate steps to mitigate the effects of the Attack and to protect the interests of data subjects by implementing remedial measures.

1.3. Marriott is an international hotel chain, with operational headquarters in the USA. The provisions of the DPA and the GDPR apply to the processing of personal data by Marriot by virtue of

[1] References in this decision to Marriott's systems / network / security etc. concern the IT systems etc. that Marriott acquired from Starwood in September 2016 and retained and continued to use post-acquisition.

section 207(2) DPA and Article 3(1) GDPR. Marriott has confirmed that Marriott Hotels Limited is Marriott's main establishment within the EU, as defined in Article 4(16) GDPR.

1.4. The data subjects affected by this breach were customers of Starwood, which was at the relevant time owned by Marriott, in the United Kingdom, elsewhere in the EU, and in the rest of the world.

1.5. Marriott was the controller in respect of the personal data of its customers within the meaning of section 6 DPA and Article 4(7) GDPR, as it determined the purposes and means of the processing of the personal data. By *inter alia* collecting, recording, organising, structuring and storing the personal data of its customers, Marriott was processing that data within the meaning of section 3(4) DPA and Article 4(2) GDPR.

1.6. Marriott has not admitted liability for breach of the GDPR. However, for the reasons set out in this Penalty Notice, the Commissioner has found that Marriott failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and Article 32 GDPR.

1.7. The Commissioner has found that, in all the circumstances, and having regard, in particular, to Marriott's representations and the matters listed in Article 83(1) and (2) GDPR, the infringements constitute a serious failure to comply with the GDPR and, accordingly, that the imposition of a penalty is appropriate. The amount of the penalty that the Commissioner has decided to impose, having taken into account a range of mitigating factors set out further below and the impact of the Covid-19 pandemic, is £18.4 million.

1.8. Pursuant to Article 56 GDPR, the Commissioner is acting as lead supervisory authority in respect of the cross-border processing at issue in this case.

2. LEGAL FRAMEWORK

GDPR

2.1. On 25 May 2018, the GDPR entered into force, replacing the previous EU law data protection regime that applied under Directive 95/46/EC ("**Data Protection Directive**")[2]. The GDPR seeks to harmonise the protection of fundamental rights in respect of personal data across EU Member States and, unlike the Data Protection Directive, is directly applicable in every Member State.[3]

2.2. The GDPR was developed and enacted in the context of challenges to the protection of personal data posed by, in particular:

a. the substantial increase in cross-border flows of personal data resulting from the functioning of the internal market;[4] and

b. the rapid technological developments which have occurred during a period of globalisation.[5] As Recital (6) explains: "*… The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities….*"

2.3. Such developments made it necessary for "*a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market…*".[6]

2.4. Against that background, the GDPR imposed more stringent duties on controllers and significantly increased the penalties that could be imposed for a breach of the obligations imposed on controllers (amongst others).[7]

---

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[3] Recital 3.
[4] Recital 5.
[5] Recital 6.
[6] Recital 7.
[7] See, in particular, Recitals 11, 148, 150, and Article 5, Chapter IV and Article 83.

The relevant obligations

2.5. Chapter 1 GDPR sets out the general provisions. Article 5 of Chapter II GDPR sets out the principles relating to the processing of personal data. Article 5(1) lists the six basic principles that controllers must comply with in processing personal data, including:

> *1. Personal data shall be:*
>
> *…(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*

2.6. Article 5(2) GDPR makes it clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".

2.7. Chapter IV, Section 1 addresses the general obligations of controllers and processors. Article 24 sets out the responsibility of controllers for taking appropriate steps to ensure and be able to demonstrate that processing is compatible with the GDPR. Articles 28-29 make separate provision for the processing of data by processors, under the instructions of the controller.

2.8. Chapter IV, Section 2 addresses security of personal data. Article 32 GDPR provides:

> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> *(c) …*
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and*

organisational measures for ensuring the security of processing.

2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.9. Article 32 GDPR applies to both controllers and processors.

Penalties

2.10. Article 83(1) GDPR requires supervisory authorities to ensure that any penalty imposed in each individual case is "*effective, proportionate and dissuasive*".

2.11. The principle that penalties ought to be effective, proportionate and dissuasive is a longstanding principle of EU law. The Commissioner is under an EU law obligation to ensure that infringements of the GDPR are penalised in a manner that is effective, proportionate and dissuasive.

2.12. Further, Recital 148 emphasises, *inter alia*, that "*in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation.*" It also records that due regard should be given to the:

… nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor…

2.13. Recital 150 provides as follows:

In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose

administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

2.14. In line with the above, when deciding whether to impose a fine and the appropriate amount of any such fine, Article 83(2) GDPR requires the Commissioner to have regard to the following matters:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, including whether, and if so to what extent, the controller or processor notified the supervisory authority of the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, directly or indirectly from the infringement. [8]

2.15. Article 83(5) GDPR provides that infringements of the basic principles for processing imposed pursuant to Article 5 GDPR will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.16. Article 83(4) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 GDPR on the controller and processer will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €10 million or, in the case of an

[8] See also the Article 29 Data Protection Working Party *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*, adopted on 3 October 2017, endorsed by the European Data Protection Board at its first plenary session. These provide a high-level overview of the assessment criteria set out in Article 83(2) GDPR in Section III ("**the Article 29 WP Guidelines**".

undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.17. Article 83(3) GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the GDPR. It provides that *"… the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement"*.

2.18. Article 83(8) GDPR provides that the exercise by any supervisory authority of its powers to fine undertakings will be subject to procedural safeguards, including an effective judicial remedy and due process.

Cooperation and consistency

2.19. Where, as here, the processing in issue is cross-border, Article 56 GDPR makes provision for the designation of a lead supervisory authority. In this case, the Commissioner is acting as the lead supervisory authority. Chapter VII GDPR establishes the regime for ensuring cooperation between lead and other concerned supervisory authorities, permitting unified decision-making.[9]

2.20. Article 60 GDPR provides:

> *1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.*
>
> *2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.*
>
> *3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without*

[9] The relevant provisions enacting this regime must be read subject to, in particular, Articles 7, 70 and 127-128 and 131 of the Withdrawal Agreement between the EU and United Kingdom.

delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the

controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned."

2.21. Article 60(4) refers to the consistency mechanism, which is in Section 2 of Chapter VII GDPR. Article 63 provides that: *"In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section."* Article 65 GDPR provides, insofar as relevant, that:

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead

supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

DPA

The Commissioner

2.223. Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR. Section 115 DPA

provides, *inter alia*, that the Commissioner's powers under Articles 58(2)(i) (the power to impose administrative fines) and 83 GDPR are exercisable only by giving a penalty notice under section 155 DPA.

Penalties

2.24. Section 155(1) DPA provides that, if the Commissioner is satisfied that a person has failed or is failing as described in section 149(2) DPA, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

2.25. Section 149(2) DPA provides:

> *(1) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –*
>
> *(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
> *(b) …*
> *(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors)…*

2.26. Section 155 DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty.

2.27. Section 155(2) DPA provides that, subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the matters listed in Article 83(1) and (2) GDPR.

2.28. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

> *(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice.*

(2) The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).

(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.

2.29. Paragraph 5 sets out the required contents of a penalty notice, in accordance with which this Penalty Notice has been prepared.

Guidance

2.30. Section 160 DPA requires the Commissioner to produce and publish guidance about how she intends to exercise her functions. With respect to penalty notices, such guidance is required to include:

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties;

(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.

2.31. Pursuant to section 161 DPA, the Commissioner's first guidance documents issued under section 160(1) DPA had to be consulted upon and laid before Parliament by the Secretary of State in accordance with the procedure set out in that section. Thereafter, in issuing any altered or replacement guidance, the Commissioner required to consult the Secretary of State and such other persons as she considers appropriate. The Commissioner must also arrange for such guidance to be laid before Parliament.

The Commissioner's Regulatory Action Policy

2.82. On 4 May 2018, the Commissioner opened a consultation process on how the Commissioner planned to discharge her regulatory powers under the DPA. The consultation attracted responses from across civil society, commentators, and industry (including the finance and insurance, online technology and telecoms, and charity sectors). The consultation ended on 28 June 2018. Having taken all the views received during the consultation process into account, the Regulatory Action Policy (the "**RAP**") was submitted to the Secretary of State and laid before Parliament for approval.

2.83. Pursuant to section 160(1) DPA, the Commissioner published her RAP on 7 November 2018. Under the hearing *"Aims"*, the RAP explains that it seeks to:

- *"Set out the nature of the Commissioner's various powers in one place and to be clear and consistent about when and how we use them";*
- *"Ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected";*
- *"Guide the Commissioner and our staff in ensuring that any regulatory action is targeted, proportionate and effective…"*[10]

2.84. The objectives of regulatory action are set out at page 6 of the RAP, including:

- *"To respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focussing on [inter alia] those adversely affecting large groups of individuals".*
- "*To be effective, proportionate, dissuasive and consistent in our application of sanctions",* targeting action taken pursuant to the Commissioner's most significant powers on, *inter alia, "organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data"*.

[10] RAP, page 5.

2.35. The RAP explains that the Commissioner will adopt a selective approach to regulatory action.[11] When deciding whether and how to respond to breaches of information rights obligations she will consider criteria which include the following:

- *"the nature and seriousness of the breach or potential breach";*
- *"where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion";*
- *"the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy";*
- *"whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data";*
- *"the cost of measures to mitigate any risk, issue or harm";*
- *"the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute)".*[12]

2.36. The RAP explains that, as a general principle, *"more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action"*.[13]

2.37. Pages 24-25 of the RAP identify the circumstances in which the issuing of a Penalty Notice will be appropriate. They explain, *inter alia*, that in *"… considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction."* The RAP stresses that each case will be assessed objectively on its own merits. However, it explains that, in accordance with the Commissioner's risk-based approach, a penalty is more likely to be imposed in, *inter alia,* the following situations:

[11] RAP, pages 6-7 and 10.
[12] RAP, pages 10-11.
[13] RAP, page 12.

- *"a number of individuals have been affected";*
- *"there has been a degree of damage or harm (which may include distress and/or embarrassment)";* and
- *"there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it)".*

2.38. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described from page 27 onwards. In particular, the RAP sets out the following five-step process:

a. **Step 1.** An 'initial element' removing any financial gain from the breach.

b. **Step 2.** Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.

c. **Step 3.** Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.

d. **Step 4.** Adding in an amount for deterrent effect to others.

e. **Step 5.** Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

3. CIRCUMSTANCES OF THE FAILURE: FACTS

Marriott's acquisition of the Starwood network

3.1. Marriot acquired Starwood in September 2016. During the acquisition process, Starwood shareholders received 0.8 shares of Marriott, as well as $21 per Starwood common stock. After the acquisition, the Marriott and Starwood computer systems were kept

separate, and they remained separate throughout the relevant period. Marriott did, however, plan on integrating aspects of the Starwood network into the Marriott network over an 18-month period in order to create a single, unified network within Marriott's security footprint.

3.2. Upon acquisition, but prior to decommissioning the Starwood network, Marriott made enhancements to the security of Starwood's existing IT network.

3.3. During the acquisition process, Marriott states that it was only able to carry out limited due diligence on the Starwood data processing systems and databases.[14] For the avoidance of any doubt, the Commissioner is not making any finding of infringement in respect of the period between Marriott's acquisition of Starwood and the entry into force of the GDPR on 25 May 2018. Accordingly, the Commissioner has not determined whether or not it was possible for Marriott to conduct due diligence during a takeover. There may be circumstances in which in-depth due diligence of a competitor is not possible during a takeover.

3.4. This Penalty Notice concerns the extent to which, after the GDPR came into effect on 25 May 2018, Marriott adequately prepared the Starwood systems to protect personal data. In particular, it is necessary to assess whether the Attack disclosed a failure to ensure compliance with Articles 5.1(f) and 32 of the GDPR following its entry into force.

The planned integration of the Starwood and Marriott networks

3.5. The integration of Starwood into the Marriott hotels group began following the acquisition. While this involved the transferring of data from the Starwood systems to the Marriott network, the systems accessed by the Attacker remained segregated from the Marriott network.

3.6. As a result, the Attack did not involve access to the wider Marriott network and the Attacker would not have had access to personal data that was processed only on non-Starwood systems. The planned migration and the decommissioning of the Starwood

[14] See, for example, the representations served by Marriott in response to the Commissioner's Notice of Intent (**"Marriott's First Representations")**, para 1.33.

systems was expedited by Marriott after discovery of the Attack and the decommissioning of the relevant Starwood systems was completed on 11 December 2018.

The Attack

3.7. What follows is a summary of the key stages of the Attack.

Pre-acquisition infiltration of the Starwood IT systems

3.8. The Attacker installed a web shell on a device within the Starwood network on 29 July 2014. This device was used to support an Accolade software application. That application was used by Starwood to allow employees to request changes to any content of Starwood's website.

3.9. The installation of a web shell on the server gave the Attacker the ability to remotely access the system, therefore allowing for the accessing and editing of the contents of that system. This access was exploited in order to install Remote Access Trojans ("**RATs**") – malware which enables remote administrator control of the system. Administrator access allows a user to perform actions above that permitted by a normal user. As a result, the Attacker would have had unrestricted access to the relevant device, and any other devices on the network to which that administrator account would have had access.

3.10. On an undetermined date, the Attacker installed and executed "Mimikatz". This is a post-exploitation tool which allows login credentials temporarily stored in the system memory to be harvested. It scanned the server for all the usernames and passwords stored in this manner in the system and allowed the Attacker to continue to compromise user accounts, which were secured using a mixture of single and multi-factor authentication.[15] These accounts were then used to perform further reconnaissance and, ultimately, to run commands on the Starwood reservation database, as described below.

3.11. On 15 April 2015, a file named "Reservation_Room_sharer.dmp" was created on a Starwood device. This file could have been created

[15] Marriott's First Representations, para 1.40 and page 63.

by the Attacker with a view to exfiltrating all the data contained in the table at once.[16]

3.12. On 21 April 2015, a file named "Consumption_Roomtype.dmp" was created. This file could have been created by the Attacker with a view to exfiltrating all the data contained in this table at once.[17]

3.13. On 17 May 2016, a file named "reservation_Room_Sharer.dmp" was created. This file could have been created by the Attacker with a view to exfiltrating all the data contained in this table at once.[18]

3.14. Following Marriott's acquisition of Starwood, on 31 December 2016 or 1 January 2017,[19] additional malware which searched devices for payment card data, known as "memory-scraping malware", was installed on multiple Starwood Devices. Marriott believes, but cannot be certain, that this action was carried out by a different attacker to the one responsible for the actions described immediately above. The memory-scraping malware was executed on 10 January 2017 on eight property management systems, but the malware was not successful in collecting payment card data from any of the devices. The eight properties involved were not in the European Union.

Continued Attack, post-acquisition and following the GDPR coming into force

3.15. On 7 September 2018, the Attacker performed a "count" on the "Guest_Master_profile" table, which would have told the Attacker how many rows the table contained.

3.16. This count triggered an alert on the Guardium system placed on the database ("the **Guardium Alert**"). Such alerts were applied to tables which included card details.[20] The other tables mentioned above did not contain payment card information and were not protected by Guardium software. Thus, no alarm could be triggered by the actions of the Attacker.

---

[16] Marriott's First Representations, page 63.
[17] Marriott's First Representations, page 63.
[18] Marriott's First Representations, page 63.
[19] Marriott has also provided the alternative date of 1 January 2017 for this installation (see Marriott's Second Representations, page 37).
[20] "Guardium" is a data protection software produced by IBM.

3.17. The Attacker also exported the "Guest_Master_profile" table into a "dmp" file (as had previously occurred in relation to the other tables referred to above).

Discovery and reporting of the breach

3.18. On 8 September 2018, Accenture, the company managing the Starwood Guest Reservation Base, contacted Marriott's IT team regarding the Guardium alert of the previous day. This was the first Guardium alert relating to the Attack that Marriott had received since its acquisition of Starwood.

3.19. On 10 September 2018, the "PP_Master" table was exported to a "dmp" file on the Starwood system.

3.20. Following the Guardium alert, on 9/10 September 2018, Marriott instigated its Information Security and Privacy Incident Response Plan. On 12 September 2018, Marriott began to deploy real-time monitoring and forensic tools on 70,000 legacy Starwood devices. The purpose of this measure was to monitor the local system and identify potentially malicious activity in real-time, with findings reported back to Marriott's central monitoring server.

3.21. On 15/16 September 2018, Marriott identified further unauthorised activity from 7 July 2018, specifically the use of credentials of Accenture employees.

3.22. On 17 September 2018, the presence of a RAT was identified. Marriott took action to contain the RAT, by blocking the command-and-control IP addresses used by the RAT.

3.23. In early to mid-October 2018, the Attacker's use of Mimikatz on a number of occasions since 2014 was identified, as was the memory-scraping malware, referred to in paragraph 3.14. On 29 October 2018, Marriott contacted the United States Federal Bureau of Investigation.

3.24. On 13 November 2018, two compressed, encrypted and previously deleted files were identified. These files were named "guest_master_profile" and "pp_master". On 19 November 2018, the aforementioned files were decrypted, and it was found that they respectively contained an export of the Guest_Master_Profile table and the PP_Master table.

3.25. On 22 November 2018, Marriott notified the Commissioner of a personal data breach.

3.26. On 25 November 2018, Marriott discovered that a file named "Reservation_room_sharer.dmp" had been created on a Starwood device, and on 26 November 2018, Marriott identified a second file named "Reservation_room_sharer.dmp" which had been created on a Starwood device, and established that a file named "consumption_roomtype.dmp" had also been created.

3.27. On 30 November 2018, Marriott provided a follow-up report to the Commissioner regarding further personal data breaches. On the same day, Marriott issued a press release about the Attack and established a dedicated Starwood incident website. Marriott also began sending email notifications to affected data subjects on 30 November 2018. In the initial email notification to data subjects, Marriott informed them that a dedicated call centre had been set up in order to receive complaints. The email notification did not provide the telephone number for the call centre, however it did contain a link to the dedicated website, which included the telephone number of the call centre. Following telephone contact between the Commissioner's office and Marriott, the email was updated to include the telephone number for the call centre, and Marriott sent the revised version on 9 December 2018.[21]

4. PERSONAL DATA INVOLVED IN THE FAILURE

4.1. The Attacker appears to have obtained personal data in both encrypted and unencrypted forms. The unencrypted information included:

a. On the "Guest_Master_Profile_table" file: a numerical identifier to identify the guest, guest name, gender, date of birth, whether the guest has been identified as a VIP, whether the guest is a member of the Starwood loyalty programme and their account information ("SPG"), mailing address, passport country code, phone number, fax number, email address, and credit card expiration date.

[21] Marriott First Representations, page 65.

b. On the "reservation_room_sharer_table": a central reservation confirmation number, a unique numerical room identifier, guest name, SPG account information, whether the guest has been identified as a VIP, a separate VIP code, 5.25 million unencrypted guest passport numbers (935,000 of which were passports associated with EEA member state records), country of guest's passport, arrival time, departure date, address, phone and fax numbers, email address, whether the guest has checked in, flight number and airline code, and the total number of guests in the room.

c. On the "consumption_room_type_table": a reservation confirmation number, the Guest Master profile ID, a unique numerical room identifier, room type, number of child guests, number of adult guests, number of cribs used in the room, number of rollaway beds designed for adults and the number of rollaway beds designed for children, guest arrival date;

d. On the "PP_master_table": the passport number record specific decryption key. Marriott considers that this would not be sufficient to decrypt the passport numbers as a master encryption key is also required, and does not appear to have been obtained by the attackers.

4.2. The encrypted information was as follows:

a. 18.5 million encrypted passport numbers, 4,290,000 of which were associated with EEA member state records.[22]

b. 9.1 million encrypted payment cards, 873,000 of which are associated with EEA member state records.[23]

4.3. Marriott's estimate is that 339 million guest records were affected. Of these, 30.1 million were EEA records,[24] of which 7 million are associated with the United Kingdom. All data subjects who were affected pre-GDPR were also affected by the actions of the Attacker post-GDPR, as the entire contents of the affected tables were exported to "dmp" files on the Starwood system each time.

[22] Marriott's First Representations, page 65.
[23] Marriott's First Representations, page 65.
[24] Marriott's First Representations, page 65.

However, the specific personal data involved differed between individual data subjects.

5. PROCEDURE

5.1. This section summarises the procedural steps the Commission has taken. The Annex to this Penalty Notice provides a more detailed chronology.

5.2. Marriott notified the Commissioner of the Attack on 22 November 2018. In response, the Commissioner commenced an investigation into the incident. That investigation included various exchanges with Marriott and considering detailed submissions and evidence.

5.3. On 5 July 2019, the Commissioner issued Marriott with a Notice of Intent to impose a penalty, pursuant to section 155(1) DPA and Schedule 16 of the DPA (the **"NOI"**). The proposed penalty was £99,200,396.00.

5.4. Marriott made written representations in response to the NOI on 23 August 2019, which are referred to in this Notice as "**Marriott's First Representations**". Marriott did not request an opportunity to make oral submissions.

5.5. Between August and October 2019, Marriott and the Commissioner exchanged correspondence about a number of issues, including (a) the application of the Commissioner's Draft Internal Procedure, which is discussed further below; (b) the application and/or operation of the Article 60 GDPR consultation process; and (c) Marriott's request for further opportunities to make submissions or representations prior to and during the Article 60 process.

5.6. In a letter dated 6 December 2019, the Commissioner:

a. confirmed that she no longer intended to exercise her discretion to convene the Panel;

b. confirmed that the Draft Internal Procedure would not be taken into account in setting any penalty imposed on Marriott, having considered the detailed representations Marriott had made on this issue in its First Representations. The letter confirmed that the Commissioner would continue to apply the EU and domestic

legislative framework in conjunction with the Regulatory Action Policy;

c. outlined how the Article 60 consultation process would be conducted in this case; and

d. agreed to give Marriot the opportunity to make further representations on the Commissioner's draft decision if Marriott agreed to extend the six-month period for the issuing of a penalty notice prescribed in paragraph 2 of Schedule 16 of the DPA. The Commissioner proposed a new deadline of 31 March 2020.

5.7. The Commissioner's position on these issues was informed, in particular, by careful consideration of Marriott's First Representations. Given the length and detail of those representations and the overall complexity of the case, that consideration took time and considerable resources. That process also resulted in changes and clarifications to the form and content of the draft decision.

5.8. The Commissioner was also especially mindful of the fact that she acted as lead supervisory authority pursuant to Article 60 GDPR in this case, and that it was therefore important that her investigation and decision be as comprehensive as possible, since the draft decision must be submitted for the consideration of other supervisory authorities pursuant to Article 60(3).

5.9. Although not required by law, the Commissioner considered that a further opportunity for Marriott to make representations was appropriate, provided that an agreement could be reached on extending the statutory timetable having regard, in particular, to: (i) the complexity of the case, (ii) Marriott's representations, and (iii) the fact that this is one of the first major decisions made under the new EU data protection regime.

5.10. Following further correspondence, Marriott confirmed on 17 December 2019 its agreement to a statutory extension of time to 31 March 2020. On 20 December 2019, the Commissioner provided Marriott with a draft decision, and invited it to make further written representations and to provide any other relevant evidence it wished the Commissioner to take into account.

5.41. On 31 January 2020, Marriott provided further detailed written representations on the Commissioner's draft decision ("**Marriott's Second Representations**").

5.42. On 12 February 2020, the Commissioner wrote to Marriott requesting further information and documents which arose from her consideration of the Second Representations.

5.43. In the light of the length and complexity of the Second Representations, on 13 February 2020 the parties agreed a further statutory extension of time until 1 June 2020.

5.44. Between 28 February 2020 and 28 April 2020, Marriott provided the Commissioner with the information she had requested on 12 February 2020.

5.45. On 3 April 2020 the Commissioner invited Marriott to make further representations specifically in respect of the financial impact on its business caused by the Covid-19 pandemic. Marriott provided a response to this request on 17 April 2020.

5.46. Due to the impact of the Covid-19 pandemic, on 17 April 2020 the parties agreed a further statutory extension of time for the issuing of a penalty notice to 30 September 2020.

6. CIRCUMSTANCES OF THE FAILURE: BREACHES

Marriott's failures

6.1. The Commissioner's conclusion is that between 25 May 2018, when the GDPR entered into force, and 17 September 2018, Marriott failed to comply with its obligations under Article 5(1)(f) and Article 32 GDPR. Marriott failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

6.2. This section describes the specific failures to comply with the GDPR that the Commissioner has found and responds to Marriott's First and Second Representations on the Commissioner's NOI and draft decision.

The relevant standard

6.3. As set out above, Article 5 GDPR requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The data controller, in this case Marriott, is responsible for, and must be able to demonstrate compliance with, that requirement.

6.4. Article 32 GDPR concerns the security of processing personal data and, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, requires a controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include encryption of personal data and a process for regularly testing, assessing and evaluating the effectiveness of such technical and organisational measures.[25]

6.5. Not every instance of unauthorised processing or breach of security will necessarily amount to a breach of Article 5 or Article 32. The obligation under Article 5 GDPR is to ensure *appropriate* security; the obligation under Article 32 is to implement *appropriate* technical and organisational measures to ensure an *appropriate* level of security, taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to the rights of data subjects.

6.6. When considering whether there has been a breach of the GDPR and whether to impose a penalty, the Commissioner must therefore avoid reasoning purely with the benefit of hindsight. The focus should be on the adequacy and appropriateness of the measures implemented by the data controller, the risks that were known or could reasonably have been identified or foreseen, and appropriate measures falling within Article 5 and/or Article 32 GDPR that were not, but could and should have been, in place.

[25] See also Recitals 76, 77 and 83 GDPR.

6.7. Having carefully examined the available evidence, including the evidence and submissions from Marriott and Marriott's Representations, the Commissioner is satisfied that there were multiple failures by Marriott to put in place appropriate technical or organisational measures to protect the personal data being processed on Marriott's systems, as required by the GDPR

6.8. The NOI and draft decision identified a number of failures by Marriott to put in place appropriate security measures. Following careful consideration of the detailed representations received from Marriott, four principal failures by Marriott are now the subject of this Penalty Notice, which are outlined below.

Preliminary issue: revised scope of the findings made

6.9. In the NOI and the draft decision, concerns were raised in relation to the gaps which the Attack identified in the application of multi-factor authentication ("**MFA**") within the relevant Starwood network. The Attacker was able to access the Starwood Cardholder Data Environment ("**CDE**") because MFA was not applied to all accounts and systems with access to the CDE.

6.10. Marriott has explained that:

a. it believed that MFA was in place across the CDE because it had received assurances from Starwood's management to this effect;[26] and

b. this belief was corroborated by two Reports on Compliance ("**ROCs**"), issued by independent PCI DSS[27] assessors on 29 April 2016 (pre-acquisition) and 23 May 2017 (post-acquisition), which stated that MFA was in place for anyone requiring access into the segmented CDE and was enabled on the jump-server via [redacted].[28] Marriott placed particular reliance in its representations on 23 May 2017 report.

6.11. Having considered, in particular, Marriott's Second Representations in response to the draft decision,[29] the Commissioner is satisfied that Marriott did not breach its obligations under the GDPR by

[26] Marriott's First Representations, para 1.40(a).
[27] Payment Card Industry Data Security Standard ("**PCI DSS**").
[28] Marriott's First Representations, para 1.40(b).
[29] Marriott's Second Representations, paras 3.2 – 3.7 and 3.20-3.24.

relying upon the ROCs (in particular, the ROC issued in May 2017) issued by the PCI DSS assessors to conclude that access to the CDE was protected by MFA (albeit erroneously). The incomplete implementation of MFA is not therefore the subject of this Penalty Notice (and consequently was not taken into account in assessing the appropriate penalty).

The four principal failures

6.412. Taking into account the representations made by Marriott,[30] the following four principal failures are the subject of this Penalty Notice.

(1) Insufficient Monitoring of Privileged Accounts

6.413. As explained above, the Attacker was able to obtain access to the CDE by exploiting an unknown gap in the scope of application of MFA. This failure to secure the 'outer ring' of the CDE is not the subject of this Penalty Notice. Instead, it is of concern that once the Attacker gained access to the CDE, appropriate and adequate measures were not in place to allow for the identification of the breach and to prevent further unauthorised activity (including further unauthorised processing of personal data). This concern arises first in respect of Marriott's failure to put in place appropriate ongoing monitoring of user activity, particularly activity by privileged accounts.

6.414. Marriott had itself determined that there was insufficient monitoring of privileged user accounts [redacted]

Whilst Marriott did deploy a Security Operations Centre ("**SOC**") [redacted], this was insufficient for the reasons given at para 6.423 below.

6.415. The National Cyber Security ("**NCSC**") guidance, published on 17 November 2018, entitled "*10 Steps to Cyber Security: Guidance on how organisations can protect themselves in cyberspace, including the 10 steps to cybersecurity*", lists "*monitoring*" as one of the relevant steps. It explains the importance of monitoring to detecting

[30] See, for example, Marriott's Second Representations, paras 2.2(b)-(c), 3.1(b), 3.8-3.13, and 3.25-3.29.

[redacted]

or responding to attacks which have already taken place or commenced:

> *Detect attacks: Either originating from outside the organisation or attacks as a result of deliberate or accidental user activity. Attacks may be directly targeted against technical infrastructure or against the services being run. Attacks can also seek to take advantage of legitimate business services, for example by using stolen credentials to defraud payment services.*
>
> *React to attacks: An effective response to an attack depends upon first being aware than an attack has happened or is taking place. A swift response is essential to stop the attack, and to respond and minimise the impact or damage caused.*
>
> *Account for activity: You should have a complete understanding of how systems, services and information are being used by users. Failure to monitor systems and their use could lead to attacks going unnoticed and/or non-compliance with legal or regulatory requirements.*[32]

6.16. The NCSC guidance also explains that monitoring activities should include, *inter alia,* the monitoring of network traffic and user activity. This NCSC guidance builds upon earlier guidance published by the NCSC which is to similar effect. See, for example, the NCSC guidance entitled "*Introduction to identity and access management*" published in January 2018[33] which refers to: (a) "*basic principles to follow when designing user access management"*; and (b) "*basic architectural good practice when designing and administering access management systems*". Such basic principles and practices include "*operations and monitoring – the supporting processes and technology to identify and enable investigation of breaches of policy or controls*". The guidance explains that:

> *Given the high value to an attacker of compromising your identity and access management systems they should be given priority for security maintenance. This means, amongst other things, prompt application of security patches across your estate (or otherwise mitigating security issues), practicing good user and privileged user management, and*

[32] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/monitoring

[33] https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

applying appropriate protective monitoring. Additionally, we recommend:

- *designing your access control systems to allow for easy monitoring of account usage and accesses*
- *being able to tie all user actions in the system to the user that performed them…"*

6.17. Both examples of NCSC guidance detail the basic need for multiple security techniques, processes and technologies in order to secure systems. Accordingly, Marriott ought to have been aware of the need to have multiple layers of security in place in order to adequately protect personal data. Although Marriott had assured itself that it had MFA in place[34] (which, as explained above, the Commissioner accepts that Marriott did), and had certain additional security measures in place, this was not sufficient. Marriott ought to have had in place better monitoring of user activity to aid in the detection of an attack, as an additional layer of security.

6.18. A forensic report into the incident, dated 11 April 2019, was commissioned by Marriott and prepared by Verizon (the "**Verizon Report**"). It notes that Marriott had not configured logging in respect of "*access to systems and/or applications within the CDE*."[35] Marriott did have the results of the ROCs and its own annual penetration tests. However, these did not evaluate the appropriateness of the way in which Marriott monitored (including through logging) the Starwood system or the configurations used for any such monitoring (including logging). Logging configurations are not within the scope of these tests. This is not a criticism of the ROCs or the penetration tests themselves. Rather it reflects the fact that Marriott ought to have taken steps to implement measures which would identify vulnerabilities which the ROCs and penetration tests would not identify. Such steps would include the implementation of effective monitoring (including logging) and alerts as part of Marriott's wider security measures. This is the gap identified by the Verizon Report.

6.19. In this case, appropriate monitoring would have included the appropriate logging of user activity, especially in relation to privileged users. The logging of user activity once within the CDE, in

[34] Contrary to, for example, para 3.6 of Marriott's Second Representations.
[35] Verizon Report, page 18.

addition to the logging done by the Guardium software, would have aided in the detection of unusual account activity (such as where, in this case, the Attacker regularly utilised legitimate accounts to perform unauthorised user activity within the CDE). Marriott's failure to log user activity in this way was inconsistent with its obligations under the GDPR.

6.20. Marriott states that "*no amount of logging would necessarily have identified an attacker unless the attacker operated from an identified suspicious IP address, which is not the case in this matter.*"[36] It is right to say that no security measure "*would necessarily*" work, there being no guarantee that any security measure is wholly effective. It is also true that it is harder to detect an attacker who is not operating from a suspicious IP address. However, this is precisely why the monitoring of legitimate user accounts (including through logging) within the network for unusual activity is vital. This is recognised by the NCSC, which states in relation to monitoring: "*these solutions should provide both signature-based capabilities to detect known attacks, and heuristic capabilities to detect unusual system behaviour*".[37]

(2) Insufficient Monitoring of Databases

6.21. In addition to the insufficient monitoring of user accounts and the user activity linked to those accounts, Marriott failed to adequately monitor the databases within the CDE. In this respect, the Commissioner is concerned by the following three failures: (a) deficiencies in Marriott's setup of security alerts on databases within the CDE; (b) the failure to aggregate logs; and (c) the failure to log actions taken on the CDE system, such as the creation of files and the exporting of entire database tables.

6.22. Marriott deployed IBM Guardium to monitor activity on the database within the CDE. As configured by Marriott, IBM Guardium had two functions. First, it logged activity (such as efforts to create, read, update, or delete data within a database). Secondly, it issued alerts in certain circumstances. The problems with the approach adopted are as follows.

[36] Marriott's Second Representations, para 3.39.

[37] NCSC "10 Steps to Cyber Security" Guidance, dated 17 November 2018: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring

6.23. With respect to logging, there were two main problems:

a. First, whilst Marriott had a security incident event management system ("**SIEM**") and a SOC to collect the logs being generated by the system, Marriott did not ensure sufficient logging of key activities such as user activity or actions taken on a database. The insufficient logging rendered the SIEM and SOC ineffective. Marriott also insufficiently logged in other areas of its network, such as firewall and access logs.

b. Second, Marriott did not engage in server logging of the creation of files (or alternatively it did not use the IBM Guardium software in a similar way), which allowed the Attacker to export entire databases to 'dmp' files undetected. Such logging is likely to have been feasible for Marriott as such mass export of data does not regularly occur within the normal course of business so as to generate an unhelpful number of false-positives. This form of logging on the system, and the evaluation of the created logs, could have enabled Marriott to detect unexpected activity within the CDE.

6.24. In response to the concerns raised, Marriott has referred to its use of Proventa and McAfee's IntruShield (two systems which generate and aggregate logs).[38] These are not, however, sufficient to address the risks faced by the Starwood network. McAfee's Intrushield aids in the detection of zero-day, DoS attacks, spyware, malware, botnets and VoIP threats, while Proventia operated as an intrusion detection system. Like Proventa, IntruShield does not address the shortcomings identified above, namely the failure to monitor database activity and user actions on network devices.

6.25. Marriott stated in its First Representations, and the Commissioner agrees, that such logging would not have *prevented* the Attack in of itself, but "*merely informs a response once the system operator is aware of the malicious activity*".[39] However, regular and close monitoring and evaluation of logs can assist in the early detection of attacks, their mitigation, and the prevention of future attacks. That Marriott did not detect the Attack until alerted by Guardium is

[38] Marriott's Second Representations, para 3.40.
[39] Marriott's First Representations, para 1.61.

indicative of Marriott failing regularly to test, assess, and evaluate the effectiveness of its security measures.

6.226. With respect to the Guardium alerts, the problem was that the circumstances in which IBM Guardium would issue alerts were limited in a way which undermined its ability to detect unauthorised activity within the databases.

6.227. In particular, alerts were only placed on tables that contained payment card information, and only specific queries (where table names were directly referenced, such as in a count) triggered warnings in the system. Although the database as a whole did have some protection from Guardium,[40] the known actions of the Attacker prior to 7 September 2018 did not meet the conditions for the triggering of an alert.[41] Marriott has explained that specific alerting rules and tables were chosen in order to reduce false-positives. However, this explanation is insufficient to justify an approach where only tables including payment card data were placed within the scope of Guardium rules. Marriott's focus on payment card information illustrates a failure to implement appropriate technical and organisational measures to ensure an appropriate level of overall security for all other personal data.

6.228. A risk-based approach was required in this case (as acknowledged in para 1.45 of Marriott's First Representations). Payment card data is likely to be the highest risk category, and the tables containing payment card data could therefore warrant higher security than other tables depending on the sensitivity of the other data held. However, while a risk-based approach may require payment card data to have *additional* security alerts, this does not justify a complete lack of alerts on tables containing other personal data. Moreover, the other data held may vary in its sensitivity, requiring different security measures to be applied to the tables/relevant processing.

6.229. Marriott stated that it reasonably assumed, based upon the PCI DSS testing results, that the Guardium alerts in respect of the CDE were appropriately configured.[42] However, the PCI DSS tests concerned

[40] Namely in terms of detecting unauthorised access based on IPs or failed login attempts, which the Attacker in this incident bypassed through compromised user credentials.
[41] As confirmed by Marriott in its correspondence dated 20 December 2018, page 6.
[42] Marriott's First Representations, paras 1.43-44.

the perimeter defences against an attack rather than monitoring systems concerned with the detection of an attacker who had already penetrated the CDE. The tests did not assess the appropriateness of the discriminatory application of the alerts across the CDE segment, nor what this meant for the security of categories of personal data stored in tables which did not contain payment card information. They do not, therefore, provide the reasonable assurance which Marriott claims.

6.230. Finally, Marriott suggested that because it believed MFA was implemented across the CDE, this rendered its reliance on that authentication tool and the Guardium alerts as configured reasonable and therefore in compliance with Articles 5(1)(f) and 32 GDPR. This is not accepted, monitoring (including logging) of the types discussed in paras 6.13 to 6.29 above are standard security measures. Control of access through MFA does not displace the need for adequate monitoring (including logging) of activities that assist in detecting a breach once it is in train (see paras 6.15-6.17 above).

(3) Control of critical systems

6.231. As discussed at paragraphs 6.213-6.230 above, Marriott failed to ensure that the actions taken on its systems were appropriately monitored. In addition to the use of monitoring and security alerts, it would have been appropriate for Marriott to implement a form of server hardening as a preventative measure, which could have prevented the Attacker from gaining access to administrator accounts and performing reconnaissance before traversing across a network.

6.232. In particular, the implementation of whitelisting is one way in which Marriott could have performed server hardening. Whitelisting is a form of programming which only allows certain users or IP addresses to access certain systems or software, as required for their specific role. It is important in reducing attack surfaces and reducing the risk of attackers being able to traverse through a network after gaining entry to a single user account.

6.233. Whitelisting should be deployed where appropriate on critical systems, and those systems which have access to large amounts of personal data. The NCSC Guidance states that: "*you should develop a strategy to remove or disable unnecessary functionality from*

systems."[43] Whitelisting is also described in NCSC Cyber Essentials guidance as a defence against malware.[44] This supports advice given in earlier guidance by NIST. In October 2015 NIST published a guide to whitelisting which shows how whitelisting can be utilised to prevent unauthorised software from being installed on a device.[45] In this incident, whitelisting could have aided in halting the reconnaissance and privilege escalation stage of the Attack.

6.834. There are many forms of whitelisting. Binary software whitelisting is a form of access control where only authorised software and scripts can be installed on a given system or user areas. For example, only allowing pre-approved software such as Microsoft Word and Outlook to be installed on work laptops. This can be distinguished from other forms of whitelisting, such as the process by which only authorised IP addresses can gain access to network resources.[46] Whilst it is not possible to list the devices in relation to which whitelisting could have been appropriate, at a minimum whitelisting would be expected on: (a) devices which could be remotely accessed; (b) devices which store large amounts or, or sensitive categories of, personal data; (c) any other systems which Marriott regards as 'critical' to their network operations; (d) any POS terminals at a property level; and any other devices which process payment card transactions.[47] The implementation of binary software whitelisting would – if correctly implemented - have prevented the installation and execution of a RAT. While it is true that the RAT was installed and executed on the system both pre-acquisition and pre-GDPR, and was therefore not attributable to Marriott, the continued absence of whitelisting post-GDPR left the systems for which Marriott was responsible vulnerable to further RAT installations and executions.

6.835. Marriott stated in its First Representations that binary software whitelisting was rarely implemented by companies at the time of the

---

See https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps

[44] NCSC Cyber Essentials Guidance: Requirements for IT infrastructure (dated April 2020): https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure.pdf (pages 10-11, under the heading "Malware Protection"). This language was also included in the now archived version of this guidance, which dated from January 2015: https://webarchive.nationalarchives.gov.uk/20150605225501/https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-secure-configuration--11

[45] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf (dated October 2015). See, in particular, section 2.1 on page 2.

[46] See para 1.52 of Marriott's First Representations.

[47] "Protecting Point of Sale Devices from Targeted Attacks" (Microsoft), dated 1 April 2014. https://download.microsoft.com/documents/en-us/Protecting_Point_of_Sale_Devices-April_2014.pdf. See, in particular, page 5.

incident, because it places a heavy burden on IT systems.[48] However, binary software whitelisting was a well-recognised and established security practice for some time before the GDPR came into force, and certainly by that date. The NCSC Guidance lists whitelisting ("*prevent unknown software from being able to run or install itself…*") as a "*Cyber Essential*". That guidance was published in October 2015, and therefore pre-dates the GDPR.[49] In addition, there is guidance published by the National Institute of Standards and Technology ("**NIST**"), which recognises whitelisting as a better option than anti-malware.[50] The NIST Guidance was published in 2015, and therefore significantly pre-dates the implementation of the GDPR.

6.36. Marriott also stated in its First Representations that binary software whitelisting could be circumvented by attackers 'side loading' RATs by using legitimate executable code.[51] Whitelisting, like all security measures, cannot be entirely resistant to attack. However, where side-loading did take place in the Attack, that appears to have been because Marriott's systems vaguely or improperly specified a dynamic-link library (DLL) which allowed such side-loading to take place.[52] Whilst Marriott is right to suggest that these are risks which cannot be fully eliminated from any third-party software,[53] this only highlights the fact that Marriott ought to have carried out regular audits, updates of software and restricted file and directory permissions. The existence of outdated/obsolete software is also an issue noted in both the 2017 and 2018 PCI DSS Reports, and these could have been mitigated by properly reacting to issues discovered in the penetration tests.

6.37. In any event, no single security measure can fully protect a system against attack or compromise. It would have been appropriate for Marriott to have implemented a 'defence in depth' strategy, of which whitelisting could play an important role, in order to protect their systems against attack and monitor activity on their network in

[48] Marriott's First Representations, para 1.53.
[49] See: https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack
[50] See: https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack and the reference to *"whitelisting and execution control – prevent unknown software from being able to run or install itself."*
[51] Marriott's First Representations, para 1.53.
[52] See: https://attack.mitre.org/techniques/T1073/ for an explanation of the vulnerabilities that allow side loading to take place.
[53] Marriott's Second Representations, para 3.31.

order to promptly mitigate any unauthorised or malicious actions that managed to bypass their security controls.

6.38. The measures discussed above are readily available and mature solutions (i.e. solutions that have been known about in the industry for a long period of time), which are appropriate and could have been implemented by Marriott, to the extent necessary, without entailing excessive cost or technical difficulties. However, it is only suggested that whitelisting (or equivalent server hardening measures which would limit the functionality of systems to only that which is required of them) could be appropriately deployed on (a) critical systems which attackers may target whilst looking to access other, sensitive areas of the network, or (b) systems which could access other (separate) systems containing personal data. Therefore, it would be appropriate to implement a server hardening measure across devices with access to the CDE, the CDE environment itself and any other network devices that could access either large quantities or sensitive categories of personal data.

(4) Encryption

6.39. Payment card data and, in some cases, passport numbers, were encrypted by Marriott using AES-128, an industry standard encryption algorithm. Oracle databases (the Starwood reservation database included tables stored in an Oracle database) provided the functionality to encrypt table entries in this way, and it was Marriot's responsibility to ensure this was configured correctly.

6.40. However, in keeping with Marriott's focus on PCI DSS compliance, encryption was not applied to other categories of personal data. The Commissioner is particularly concerned that not all passport numbers were encrypted.

6.41. In its First and Second Representations, Marriott stated that it had adopted a mature and risk-based approach to cyber security by targeting its security efforts on the tables containing cardholder information.[54] In support of its position, Marriott relied upon a selective quotation from the NCSC Guidance in its written

[54] Marriott's Representations, para 1.27 and 1.63, see also para 3.45 of Marriott's Second Representations.

submissions. However, the Commissioner notes that the full quote provides as follows:

> *In some scenarios, the use of encryption to protect bulk data should be the norm. For example, where data is transmitted over the internet, stored on a laptop, or stored on removable media. However, encryption relies on good key management, and in some scenarios it is challenging to engineer a solution which makes meaningful use of encryption to protect personal data. This is sometimes the case in systems which are always online, where data needs to be available to query.* ***In these scenarios, your systems architects and designers will need to think carefully about how encryption can be used in a meaningful way***.[55]

6.42. However, Marriott has not provided any risk assessments which demonstrate the evaluative judgement it arrived at and the rationale for its approach to the encryption of personal data. On the contrary, Marriott has taken an inconsistent approach by encrypting some but not all passport numbers. In addition, while it may be true that cardholder information is of higher risk than other categories of personal data, this does not vitiate the risk to other categories of personal data. Thus, while the NCSC guidance quoted above, does not say that Marriott is required to implement encryption across all personal data, it does require Marriott to explain why it chose to selectively encrypt data.[56] Even if Marriott reasonably believed that the CDE was protected by MFA, it was aware – or ought to have been aware – that no system is fully secure.[57]

6.43. Marriott, in its First Representations, also claimed that it would have been impractical for it to have encrypted any more personal data than it did.[58] However a number of methods exist to facilitate the identification of the user to which a piece of data refers, so that decryption of personal data can take place quickly and when necessary. One method is through the use of a unique identifier (such as an UUID), which can aid in querying and decrypting individual pieces of data associated with individual customers where required in almost real-time. There are also Hardware Security

[55] See: https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data (emphasis added).
[56] Marriott's Second Representations, para 3.46(c).
[57] Marriott's Second Representations, para 3.46(b).
[58] Marriott's First Representations, para 1.27(b).

Modules which Marriott could have utilised, encrypting data in near real time at its source and decrypting it at its destination.

6.44. In addition, the level of security that the encryption could have achieved was compromised within the Starwood guest reservation database by a script, developed by Starwood, which allowed for AES-128 encrypted entries in a database table to be decrypted. [redacted]

6.45. [redacted]

6.46. [redacted]

6.47. [redacted]

[59] Marriott's First Representations, paragraph 1.64. As to paragraph 1.64(c), while the Commissioner agrees that it is unlikely that the attacker did run the script millions of times, if the attacker so wished, this could have been achieved in very little time as it could be run as an automated process.
[60] Marriott's Second Representations, para 3.46(a).

[redacted]

Marriott's wider arguments

6.48. In addition to the arguments referred to above, Marriott's Representations raised a number of more general legal and/or factual arguments. This section addresses the following submissions made by Marriott:

a. **First,** that the Commissioner had assessed the issue of breach without reference to "*any clear standards*",[61] reasoned with the benefit of hindsight and regarded the fact that the Attack was successful as an indicator that the security measures were inappropriate.[62] Marriott claims that the Commissioner has applied an "*impossibly high standard of care*".[63]

b. **Second**, that the Commissioner failed to apply a holistic approach.[64]

c. **Third**, that the Commissioner impermissibly relied upon Marriott's pre-GDPR conduct, and incorrectly concluded on a provisional basis that Marriott had failed to carry out sufficient and appropriate due diligence.[65]

d. **Fourth**, that the Commissioner erred in referring to Article 25 GDPR in the NOI.[66]

e. **Fifth**, that the Commissioner erred in reaching the provisional view in the NOI that Marriott had breached the notification requirement under Article 33 of the GDPR.[67]

---

[61] Marriott's First Representations, paras 1.3-1.7.
[62] Marriott's First Representations, paras 1.8-1.12. See, to similar effect, Marriott's Second Representations, Executive Summary, para 3, and para 3.1(b), and paras 3.15-3.18.
[63] Marriott's First Representations, Executive Summary, para 1; para 1.2, see also Marriott's Second Representations, paras 3.14-3.18.
[64] Marriott's First Representations, Executive Summary, paras 1and 5, and paras 1.13-1.15; and Marriott's Second Representations, para 2.2(c).
[65] Marriott's First Representations, Executive Summary, paras 3-4, paras 1.18-1.20 and 1.29-1.37.
[66] Marriott's First Representations, para 1.21.
[67] Marriott's First Representations, Executive Summary, para 7, and paras 2.1-2.10 and 2.16.

f. **Sixth**, that the Commissioner was wrong provisionally to find in the NOI that Marriott's notification to data subjects breached Article 34 of the GDPR.[68]

6.49. In its First and Second Representations, Marriott also advanced a number of points in relation to: (a) the Commissioner's approach to determining whether to impose a penalty; and (b) her methodology in calculating the proposed penalty as set out in the Notice of Intent and the draft decision. These arguments are addressed in Section 7 below.

(1) The correct approach/standard

6.50. Marriott claims that: (a) the Commissioner's factual findings were inaccurate; and/or (b) the Commissioner cannot maintain the conclusion that appropriate measures were available that Marriott failed to take to remove and/or mitigate the risk of an attack of the kind which occurred in this case because she had applied the incorrect standard or approach.[69]

6.51. In the analysis set out above, the Commissioner has clarified certain factual findings made in the Notice of Intent in the light of the submissions made by Marriott in both its First and Second Representations, including by, in particular, clarifying her position in respect of the incomplete application of MFA.

6.52. Further, paragraphs 6.3-6.8 above, provide an accurate summary of the position on the relevant standard and set out the Commissioner's response to Marriott's argument that she applied an incorrect, unduly high, inappropriate or unclear standard in the NOI and/or draft penalty notice. The analysis set out in Section 6 above clearly explains the basis for the finding that Marriott failed to put in place appropriate security arrangements as required by the GDPR by reference to the specific facts of this case. Contrary to the claims made in Marriott's First Representations, the Commissioner has not applied a one-size-fits-all approach to what measures are appropriate to secure different types of personal data.[70]

[68] Marriott's First Representations, paras 2.11-2.15 and 2.16.
[69] Marriott's First Representations, paras 1.3—1.5 and 1.39-1.70; and Marriott's Second Representations, Executive Summary, para 3.
[70] Contrary to, in particular, paras 1.16-1.17 of Marriott's First Representations.

6.53. As the Commissioner has set out above, and as she set out in the NOI, there were a number of appropriate measure(s) available to Marriott that an organisation of its scale would be expected to take to secure its data operations. Contrary to the claims made by Marriott, this Penalty Notice (nor the NOI/draft decision) do not proceed on the basis that simply because the Starwood system was the victim of the Attack, it follows that Marriott breached the GDPR.[71] The reasoning supporting this Penalty Notice, and the NOI and draft decision, does not adopt such a simplistic approach.

6.54. For essentially the same reasons, contrary to Marriott's submissions,[72] the Commissioner's findings do not involve applying the benefit of hindsight in an improper manner, or at all (as already explained above). The Commissioner is satisfied that there were four distinct weaknesses in Marriott's system each of which Marriott ought to have identified and remedied, using one of the range of options available to Marriott (as discussed above). The Commissioner does not rely on the 'success' of the Attack as evidence that a breach of the GDPR definitely occurred. Instead, the Attacker's ability to exploit deficiencies in Marriott's security measures, for which remedies were available, discloses wider failures to put appropriate measures in place. In particular, the failure to encrypt all passport numbers was inadequate. There was also a failure to place Guardium alerts on tables other than those which contained payment information, thereby allowing the attack to go on undetected for a longer period.

6.55. At para 1.12 of its First Representations, Marriott also claims that there is no basis for the suggestion that, under the GDPR, it ought to have identified the type of Attack which is the subject of this Notice, or carried out any further improvements on the Starwood systems, because the system was the "*victim of a sophisticated attacker, which adopted a multi-vectored approach to its attack and was able to circumvent numerous protections that were in place*". However, the sophistication or specific vector of the attack is not the relevant focus. A controller has to implement appropriate measures to ensure the security of its systems. The measures mentioned above could have been implemented using standard industry tools, and could have prevented, detected and/or mitigated the impact of

[71] Marriott's First Representations, §§1.8-1.9.
[72] See, in particular, Marriott's Second Representations, paras 3.15-3.18.

the Attack. What the Attack disclosed was the failure by Marriott to put in place appropriate security measures to address attacks of this kind and/or other identifiable risks to the system.

6.56. Furthermore, Marriott was wrong to state[73] that the fact that the relevant Starwood IT system was due to be retired shortly means that it was not necessary to put in place the types of appropriate measures identified above in order to comply with Articles 5(1)(f) and/or 32 GDPR.

6.57. In particular, Marriott relies on the fact that it originally intended to decommission the Starwood system in the first quarter of 2018 in response to the concerns raised about its security measures. It is important to note that the intended decommissioning was due to take place approximately a year and half after the acquisition of Starwood, a long period of time during which data continued to be processed on the system. In fact, the intended decommissioning did not take place in the first quarter of 2018; the timetable was altered such that it was only to be achieved by the end of 2018. Whilst the Commissioner accepts that Marriott could not have known about the delay to the decommissioning timetable at the outset,[74] in early 2018 Marriott was aware that the GDPR was coming into force and that it would be continuing to process data within the Starwood network for a number of months after that. During this period, appropriate monitoring (including logging), and alerting tools could have been implemented relatively quickly in order to secure the systems until their decommissioning at the end of 2018.

6.58. Many of the measures identified in the discussion of the 4 principal errors above could have been easily implemented as part of the security improvements which Marriott was already making over this period. With regards to logging, the appropriate changes to what was in fact being logged could have been made as part of Marriott's SIEM and SOC projects. No additional steps as part of the "*general IT lifecycle process*" would have been required.[75] Similarly, changes to the Guardium alert settings could have been made relatively quickly and easily when IBM Guardium was deployed. The appropriate server hardening measures could have been

[73] Marriott's Second Representations, para 3.32-3.36.
[74] Marriott's Second Representations, paras 3.35-3.36.
[75] Marriott's Second Representations, para 3.38.

implemented within 6-12 months (depending on which measures Marriott selected and how it chose to implement them).

6.59. The fact that an IT system is due to be retired shortly does not disapply the GDPR to the data being processed through that system. Marriott was still obliged to decide what appropriate measures should be in place in the light of the continued use of the system. While the fact that a system is to be decommissioned may be a relevant factor in determining what measures would be appropriate in a given case, this ultimately does not remove the basic obligation to put in place security measures appropriate to the risk posed by the continued processing. This may mitigate against, for example, a requirement that a controller, even one of the size and scale of Marriott, put in place expensive, state-of-the-art measures, where the system is to be decommissioned in the near future. However, where other appropriate measures are available without entailing disproportionate cost or delay, they should be put in place if they are required to ensure a level of security appropriate to the risks posed by continued processing. As explained above, the specific measures identified in the discussion of the four principal errors above are all ones which could have been put in place in a short amount of time, and which would not have entailed excessive cost.

(2) A holistic approach

6.60. The Commissioner has had regard to Marriott's detailed submissions on the security measures it had in place generally, and those it implemented after its limited due diligence on the Starwood systems.[76] However, the investigation has identified a number of appropriate measures or steps that should have been taken by Marriott to address the identified security risks within its system. The Attack, and/or other attacks which could have occurred as a result of the deficiencies in Marriott's systems, identified above, mean that, even judged holistically, Marriott's technical and organisational data security arrangements cannot be regarded as sufficient or appropriate.

6.61. The Commissioner has also considered Marriott's submissions about the improvements made to Starwood's systems post-acquisition, which are said to show that it engaged in appropriate due

[76] See, in particular, para 1.35 and paras 1.39-1.70 of Marriott's First Representations.

diligence.[77] However, it is notable that none of those steps identified the relevant, easily detectable, deficiencies in Marriott's security, which could have been easily addressed but were exploited during the Attack. Marriott's submissions in this regard focus on improvements it made to its own systems, and which the Starwood systems' data would benefit from when they were migrated to its network (paras 1.35(b)-(c) of Marriott's First Representations). But this does not meet the concern that Marriott continued to use the Starwood system without remedying the clear deficiencies in its security arrangements. It is clear from Marriott's Representations[78] that only limited changes were made to the Starwood system because it was expected to be decommissioned sometime in the future. It is apparent that these changes were not sufficient to address the failings described above which should have been addressed given the ongoing processing that was to take place prior to decommissioning.

(3) Pre-GDPR conduct and due diligence

6.62. Marriott is wrong to argue that the NOI relied upon Marriott's failure to appropriately secure its systems and the personal data stored on them, prior to the period covered by the GDPR. The fact that no such reliance was placed on the pre-GDPR conduct was made clear in the NOI itself.[79]

6.63. Marriott's argument in this regard relies on the claim that any duty to undertake a due diligence process is one which would have to be discharged prior to or shortly after acquisition. Marriott submitted that it is not tenable to proceed on the basis that acquisition due diligence is a "*seemingly endless*" process.[80]

6.64. While the Commissioner accepts that the acquisition of a company's data processing operations are *a* trigger for a controller to carry out due diligence, either immediately prior to acquisition or shortly thereafter, this is not the only trigger point for such activity. The need for a controller to conduct due diligence in respect of its data operations is not time-limited or a 'one-off' requirement. In

[77] Marriott's First Representations, paras 1.15 and 1.30-1.35.
[78] See paras 1.34 and 1.35(d) of Marriott's First Representations and paras 3.35-3.36 of Marriott's Second Representations. See also para 6.56 above.
[79] Marriott's First Representations, paras 2.4-2.10; see also Marriott's First Representations, para 1.20.
[80] Marriott's First Representations, para 1.20(a) and (b).

particular, the coming into effect of the GDPR was, for a global business like Marriott, a highly relevant factor.

6.65. Controllers such as Marriott would have been aware for some time that the GDPR was going to come into effect on 25 May 2018. It was incumbent on such controllers to ensure that their data processing complied with the provisions of EU law from that date. However, after May 2018 Marriott continued to process personal data using a system that was deficient in a number of respects, and those deficiencies only came to light following the discovery of the Attack some months later.

6.66. Given Marriott's ongoing duty to ensure that the systems it had acquired from Starwood were GDPR compliant, it is no answer to claim that certain due diligence steps were, or only needed to be, taken in the period immediately after acquisition. Controllers cannot process personal data without appropriate security measures being in place on the basis that the system was deficient prior to May 2018 and has not been remedied. Even if adequate due diligence had been undertaken at the point of acquisition, that would not have removed Marriott's obligation to ensure, on a continuing basis, that it complied with the GDPR, once that Regulation came into force.

6.67. Marriott recognises this, but relies upon *inter alia* its PCI DSS assessment process as the means by which this continuing obligation was discharged.[81] However, PCI DSS assessments are limited in their ability to detect and mitigate vulnerabilities within a network, for the reasons given at paragraph 6.29 above. Rather, adequate and appropriate due diligence would have included reviewing the adequacy of the monitoring (including logging) systems within the network.

6.68. Thus, for the avoidance of any doubt, this decision relates solely to Marriott's failures after 25 May 2018. The Commissioner has not issued a decision under the Data Protection Act 1998 (**"DPA 1998"**), despite the historic, pre-2018 nature of the concerns in respect of the Starwood system.

[81] Marriott's Second Representations, page 47.

(4) Article 25

6.69. The Commissioner acknowledges that the NOI, at para 58, included an erroneous reference to Article 25 GDPR. This was a typographical error. The penalty figure set out in the NOI did not take into account any breach of Article 25.

(5) Article 33

6.70. At the NOI stage, a provisional finding of breach of Article 33 GDPR was proposed. However, this finding no longer forms part of the decision against Marriott.

6.71. In reaching this decision, the Commissioner did consider Marriott's claims that (i) the Commissioner failed to identify the date on which Marriott became aware of the breach;[82] and (ii) the Commissioner misapplied the GDPR rules on when a controller must be taken to be aware of a personal data breach.[83]

6.72. However, it is not accepted that the NOI failed to identify the date on which Marriott became aware of the breach for the purposes of Article 33 GDPR. The Commissioner identified 8 September 2018 as the relevant date at para 52 of the NOI: "*Marriott had been aware of unauthorised access to the Starwood systems since the Guardium alert on 8 September 2018… It would have been reasonable at that point for Marriott to conclude that personal data was likely to have been accessed by an unauthorised party.*" The reference to the "dmp" files in para 53 of the NOI cannot reasonably be read as referring to the identification of the dmp files on 13 November 2018.[84] Rather, this was a reference to the fact that on 7 September 2018 the Attacker exported the "Guest_Master_Profile" table – a table that Marriott knew to contain personal data – into a "dmp" file. Marriott was alerted to the presence of the Attacker by Accenture on 8 September 2018, the day after this took place.

6.73. Marriott was also incorrect to submit that the GDPR requires a data controller to be reasonably certain that a personal data breach has occurred before notifying the Commissioner. Rather, a data controller must be able reasonably to conclude that it is likely a

[82] Marriott's First Representations, paras 2.1-2.3.
[83] Marriott's First Representations, paras 2.4-2.10.
[84] Marriott's First Representations, para 2.1.

personal data breach has occurred to trigger the notification requirement under Article 33.

6.74. Nevertheless, the Commissioner took into account, in particular, Marriott's explanation that a count can be performed on a database without any of the personal data held on that database being accessed, and that Marriott's position is that it was unaware of the export of the "Guest_Master_Profile" table into a "dmp" file (which took place on 7 September 2018) until 13 November 2018. [85] The Commissioner has also taken into account Marriott's submission that the "Guest_Master_Profile" contained non-personal data, and therefore it was only with decryption of that file on 19 November 2018 that it became aware of the personal data breach.

6.75. Thus, in this particular case, and in the light of Marriott's Representations, the Commissioner has decided not to make a finding that Marriott breached Article 33 GDPR.

(6) Article 34

6.76. The NOI contained a provisional finding of a breach of Article 34 GDPR. Marriott submitted detailed submissions in response to that proposal.[86]

6.77. The Commissioner recognises that Marriott established a dedicated website regarding the breach, and issued a press release which was widely-reported.[87] Marriott claims in its Representations that a dedicated website and press release would have been sufficient for it to have discharged its obligations under Article 34.[88] This is incorrect.

6.78. Article 34(1) requires Marriott to "*communicate the personal data breach to the data subject*" (emphasis added). Where this would involve "*disproportionate effort*", Marriott may issue a public communication or similar measure (Article 34(3)(c)). Sending an email to data subjects whose current email addresses are stored on Marriott's systems is not, on any view, a disproportionate measure. It is a routine commercial activity. This is supported by the fact that Marriott did inform the data subjects, via email, very soon after it

[85] Marriott's First Representations, paras 2.4-2.10.
[86] Marriott's First Representations, paras 2.11-2.16.
[87] Marriott's First Representations, para 2.12.
[88] Marriott's First Representations, para 2.14.

identified the breach. The Commissioner accepts that some data subjects will not have been contactable in that way; the most obvious example being individuals who had changed their contact details. In these cases, it may have involved a disproportionate effort to track those individuals down in order to communicate the breach and, for such individuals, Marriott will have discharged its duty by way of its press release and dedicated website. However, Marriott is not entitled to rely upon communications which are addressed to the world at large (such as its press release and website) as discharging its duties under Article 34(1) in relation to all data subjects.

6.79. The Commissioner is accordingly entitled to consider Marriott's direct communications (including emails) with the affected data subjects as the means by which Marriott sought to satisfy its obligations under Article 34 GDPR.

6.80. The email sent by Marriot referred to a "dedicated call centre", this being a specific telephone line set up for affected data subjects to contact for further information, but it did not include the telephone number. The email, having communicated the "name" of the contact point, did not communicate the "contact details" of the point where more information could be obtained. While plainly not deliberate, these omissions to some extent undermined the effectiveness of the notification.

6.81. The Commissioner has taken into account the fact that the email contained a link to the dedicated website, which in turn provided the telephone number for the dedicated call centre,[89] although the email itself did not. On this occasion, and in light of the information that Marriott did in fact provide to affected data subjects, this Penalty Notice does not include any finding that Marriott breached Article 34 GDPR.

7. REASONS FOR IMPOSING A PENALTY & CALCULATION OF THE APPROPRIATE AMOUNT

7.1. For the reasons set out above, the Commissioner's view is that Marriott has failed to comply with Articles 5(1)(f) and 32 GDPR. These failures fall within the scope of section 149(2) and 155(1)(a)

[89] Marriott's First Representations, para 2.14(a).

DPA. For the reasons explained below, the Commissioner has decided that it is appropriate to impose a penalty in the light of the infringements she has identified.

7.2. In deciding to impose a penalty, and calculating the appropriate amount, the Commissioner has had regard to the matters listed in Articles 83(1) and (2) GDPR and has applied the five-step approach set out in her RAP.

The imposition of a penalty is appropriate in this case

7.3. Both the RAP and Article 83 GDPR provide guidance as to the circumstances in which it is appropriate to impose an administrative fine or penalty for breaches of the obligations imposed by the GDPR.

7.4. Article 83(2) GDPR lists a number of factors that must be taken into account. These are each discussed in detail below in determining the appropriate level of fine, in accordance with the steps outlined in the RAP. The points made below are also relied upon in justifying the Commissioner's decision to impose a penalty, in the light of the findings of infringement set out above.

7.5. The RAP provides guidance on when the Commissioner will deem a penalty to be appropriate.[90] In particular, the RAP explains that a penalty is more likely to be imposed where, *inter alia*, (a) a number of individuals have been affected; (b) there has been a degree of damage or harm (which may include distress and/or embarrassment); and (c) there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it).

7.6. As discussed in more detail below, each of those features is present in this case. Taking together the findings made above about the nature of the infringements, their likely impact, and the fact that Marriott failed to comply with its GDPR obligations, the Commissioner considers it appropriate to apply an effective, dissuasive and proportionate penalty, reflecting the seriousness of the breaches which have occurred.

[90] Pages 24-25, see para 2.37 above.

Calculation of the appropriate penalty

Step 1: an 'initial element' removing any financial gain from the breach[91]

7.7. Marriott did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. The Commissioner has not, therefore, added an initial element at this stage.

Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at sections 155(2)-(4) DPA

7.8. Sections 155(2)-(4) DPA refer to and reproduce the matters listed in Articles 83(1) and 83(2).

The nature, gravity and duration of the failure (Article 83(2)(a))

7.9. **Nature and gravity of the failures:** The nature of the failures is of significant concern. As set out above, there were multiple measures that Marriott could have put in place that would have allowed for the detection of or mitigated the Attack insofar as it continued after 25 May 2018.[92] What the Attack shows is that during the relevant period Marriott was processing data on a system that had multiple security failings that were exploited by the Attacker and could have been exploited by others.

7.10. In Marriott's submissions it has placed a great deal of emphasis on other security measures it had in place, criticising the NOI/draft decision for failing to look at the matter holistically.[93] This criticism is misplaced. The Commissioner has carried out a holistic analysis of the relevant systems and security processes operated by Marriott. What that analysis showed was that the measures identified in section 6 above were appropriate to secure the CDE. Marriott's implementation (or perceived implementation) of other security measures was not sufficient. It was appropriate for there to be

---

[91] Removing any financial gain the data controller may have obtained from the infringement is consistent with ensuring that the penalty is effective, proportionate and dissuasive (Article 83(1)), and has regard to Article 83(2)(k), which refers to "*financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*"

[92] Marriott's First Representations at para 3.2(a) have been considered and addressed in section 6 above.

[93] Marriott's Second Representations, para 2.2(c).

multiple layers of security in this case (for the reasons given at paragraph 6.17 above).

7.11. An extremely large number of individuals were affected by the breach, specifically, 339 million guest records, of which – for the purposes of this penalty - 30.1 million[94] were guest records associated with EEA member states. Marriott has explained that the total number of affected guests is difficult to estimate from this figure as it may hold multiple records for an individual guest.[95] Even taking into account that the true number of affected individuals may be 40% lower than initially estimated by Marriott,[96] this is still a significant number of individuals.

7.12. The mitigating steps taken by Marriott will have gone some way to reassuring Marriott's customers and therefore may have reduced or mitigated the distress that may otherwise have been caused by the data breach. The assurances given and the mitigating steps taken by Marriott are taken into account below. It is nevertheless likely that some of the affected individuals will, depending on their circumstances, still have suffered anxiety and distress as a result of the disclosure of their personal information (including payment card information[97]) to an unknown individual or individuals. The Commissioner has considered in this regard the submissions made by Marriott in its Representations.[98] She notes the following points:

a. The Commissioner has not seen any evidence of financial damage and is not required to investigate the existence or otherwise of financial damage.[99] In calculating the appropriate level of penalty, the potential existence of such damage has not been assumed or taken into account.

b. It is possible that some individuals may have cancelled their payment cards. Contrary to Marriott's submissions,[100] the Commissioner is not required to investigate or identify evidence of individuals actually cancelling their cards. In circumstances

[94] Marriott's First Representations, page 65
[95] See Marriott's Second Representations, paras 2.4-2.6.
[96] *Ibid.*
[97] Notwithstanding the fact that there was no actual financial harm to individuals, see Marriott's Second Representations para 2.7(a)(i).
[98] Marriott's First Representations, para 3.1(d) and Marriott's Second Representations, paras 2.7-2.8.
[99] A point emphasised in Marriott's First Representations, para 3.2(d)(ii)(A); and Marriott's Second Representations, para 2.7(a)(i).
[100] Marriott's Second Representations, para 2.7(a)(iii).

where a large number of individuals have been informed that their data, including some credit card data have been compromised, the Commissioner considers it likely that some individuals will have taken this step.

c. The possibility that some individuals may have been prompted to cancel their payment cards is just one element of the overall assessment of whether *the breaches of the GDPR* were likely to cause distress. The act of cancelling a card may in and of itself only cause inconvenience. It is the reason why such action was necessary, the disclosure of personal information, that can cause distress amongst some.

d. The fact that the Marriott call centre received 57,000 calls between 30 November 2018 and 31 May 2019 (7,500 of these being calls to EU-based call centres) is indicative of the potential level of concern amongst affected data subjects on learning of the breach and subsequently.[101]

e. Further, even if individuals opted not to cancel their credit cards, the Commissioner considers it likely that some individuals will have experienced distress at having their personal data exposed in a large-scale data breach. Marriott's suggestion that distress will only arise in cases where they are advised by their banks to cancel their payment cards[102] ignores the fact that all personal data (not just financial data) is of significance to individuals, a significance which is reflected in the legal protections afforded to that data under the GDPR.

7.13. **Duration:** Although the Attack itself spanned a four-year period, the infringements that the Commissioner relies on in this Notice occurred between 25 May 2018 (the date when the GDPR came into force) and 17 September 2018. The Commissioner considers this to be a significant period of time over which unauthorised access to personal data went undetected and/or unremedied.[103]

[101] See further Step 5 below.
[102] See Marriott's Second Representations, para 2.7(a)(iii), which is then contradicted by the statement in para 2.7(a)(iv), which suggests that card cancellation is merely an "inconvenience" and not, as suggested in sub-para (iii) a necessary component of a finding of distress.
[103] Marriott's First Representations at para 3.2(b) and Marriott's Second Representations at para 2.3.

The intentional or negligent character of the infringement (Article 83(2)(b))

7.14. The Commissioner has had regard to the guidelines provided by the Article 29 Working Party in relation to assessing the character of the infringement in issue. It explains that:

> *… In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law*.
>
> *It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case…*[104]

7.15. The Commissioner recognises that the infringement was not an intentional or deliberate act on the part of Marriott. This has been taken into account in assessing whether a fine is appropriate in this case.

7.16. The Commissioner does, however, consider that Marriott was negligent (within the meaning of Article 83(2)(b) GDPR) in maintaining systems that suffered from the vulnerabilities and shortcomings identified in Section 6 above.[105]

7.17. In making this determination, the Commissioner places some weight on the relevant context: a company of the size and profile of Marriott is expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise. Marriott must be aware that the nature of its business involves processing large volumes of personal data, including sensitive personal data. The risk of any compromise of that information may have significant consequences for Marriott's customers and its own business.

[104] Pp.11-12.

[105] Marriott's general claim at paragraph 2.9(b) of its Second Representations refers to its specific explanations in section 3 of those representations, which have been addressed in section 6 above.

7.18. In view of these factors, the Commissioner: (a) would expect Marriott to have taken appropriate steps or a combination of appropriate steps to secure the personal data of its customers; and (b) considers that Marriott failed to comply with the standards imposed by the GDPR in failing to do so. Beyond this, the Commissioner has not treated the nature of Marriott's conduct under Article 83(2)(b) as an aggravating factor in assessing whether to impose a penalty, or how much that penalty should be. However, she is obliged to take into account the character of the infringement under Article 83(2)(b). Thus, she does not consider that she has erred in *"applying this factor"*, as Marriott submitted in its First Representations.[106]

7.19. Marriott relied upon the Article 29 WP Guidelines to argue that the draft decision failed to treat the fact that the breaches were not deliberate as a positive factor in favour in assessing whether to impose a fine.[107] These Guidelines state that intentional breaches are more likely to warrant the application of a fine. Marriott submitted that if this is the case, the absence of intention must weigh in the controller's favour.

7.20. It is unclear what additional weight Marriott considers the absence of intention should attract in this case. The mere recognition in the Article 29 WP Guidelines of the obvious point that a deliberate breach is more likely to result in certain consequences does not alter the fact that a penalty may be imposed for a breach of a different nature (and nor would it be consistent with Article 83 GDPR if fines only applied to deliberate conduct). The Commissioner has taken into account the fact that the breaches were not deliberate as part of her overall assessment (as Marriott recognises[108]). However, in circumstances where, as here, the breaches were negligent within the meaning of Article 83(2)(b), that fact must also be taken into account when assessing whether to impose a fine and, if so, at what level.

7.21. Marriott also criticised the Commissioner's analysis as being duplicative because she had regard to, *inter alia*, the scale of Marriott's processing operations in assessing whether its actions

[106] Marriott's Representations, para 3.3.
[107] Marriott's Second Representations, para 2.9(a).
[108] *Ibid.*

were negligent under Article 83(2)(b), as well as in assessing whether it complied with Articles 5 and 32 GDPR.[109] While it is true that the Commissioner considered some of these factors when concluding whether there was a breach of Articles 5 and 32, these factors are relevant in both contexts. The issue of whether a breach has arisen, and the nature of Marriott's responsibility for it, are clearly related issues.

Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))

7.22. The Commissioner has carefully considered Marriott's submissions to the effect that it could not discern from the draft decision how the mitigation action it took in response to the Attack has been taken into account because it was dealt with at this Step, rather than at Step 5.[110]

7.23. The Commissioner remains of the view that it makes no difference to the ultimate decision on what, if any, penalty to impose whether the action taken by the controller to mitigate the damage is taken into account here, or under Step 5 in this Penalty Notice. However, she has decided to consider this issue separately under Step 5 in this Penalty Notice.

The degree of responsibility of the controller or processor (Article 83(2)(d))

7.24. As a controller, Marriott is responsible under the GDPR for the security of its systems and the protection of personal data stored within those systems. It is required by the GDPR to implement security measures to reduce the vulnerability of those systems, and the vulnerability of the personal data processed within those systems, to attack. While the entry of the Attacker into Starwood's systems pre-dates Marriott's acquisition of that company, Marriott had an ongoing duty to ensure the safety and security of the systems it was using to process personal data.

7.25. As is clear from Section 6 above, there were multiple deficiencies in the security measures in place in respect of the Starwood system, which Marriott continued to operate to process personal data after

[109] Marriott's Second Representations, para 2.9(c).
[110] Marriott's Second Representations, paras 1.9-1.10, and 1.34.

the GDPR came into force. As a result, the Attacker was able to remain present and undetected in the system after 25 May 2018 until the triggering of the Guardium alert in September 2018.

7.26. The Commissioner therefore considers that, for the duration of the infringement on which this penalty is based, Marriott is wholly responsible for the breaches of Articles 5(1)(f) and 32 GDPR described above.

7.27. In its Representations, Marriott highlighted the fact that the NOI did not mention that Accenture provided it with third-party IT services.[111] In response to the draft decision, Marriott explained that in its view, the fact that it engaged Accenture to assist in the security management of the Starwood network should be taken into account in assessing Marriott's responsibility for the Attack.

7.28. It is acknowledged that Accenture is an experienced provider of security services and that it provided services in relation to Marriott's security environment. However, the fact that it was charged with implementing, maintaining or managing certain elements of the system does not reduce Marriott's responsibility for the breaches of the GDPR that have been identified. In circumstances where Marriott accepts that it is the relevant data controller, and significant failures in its security measures have been identified, the engagement of third parties cannot reduce its degree of responsibility.

7.29. For the avoidance of doubt, however, in taking a holistic view of the security measures put in place, account has been taken of, for example, the fact that Guardium was in place and certain alerts were applied under that system (which Accenture monitored).

7.30. Finally, Marriott is correct to state in its Representations that the Article 29 WP Guidelines provide that "*industry standards… are important to take into account*" when assessing compliance with the GDPR. The Commissioner has taken into account Marriott's detailed submissions on its compliance with PCI DSS standards, in particular in respect to the concerns which arose in respect of the application

[111] Marriott's First Representations, para 3.5, and Marriott's Second Representations paras 2.10-2.11.

of MFA across the Starwood network.[112] However, Marriott's obligations under Article 5(1)(f) and Article 32 GDPR go beyond the requirements of the PCI DSS and extend to all personal data, not just cardholder information with which those standards are concerned. The fact that Marriott may have complied with certain industry guidance focusing on specific types of personal data does not obviate or reduce its responsibility for the security of all of the personal data it holds.

Relevant previous infringements (Article 83(2)(e))

7.31. Marriott has no relevant previous infringements or failures to comply with past notices.

7.32. Marriott claims that this fact should weigh positively in its favour, rather than neutrally.[113] The fact that Marriott has no relevant previous infringements is a matter that has been taken into account in the Commissioner's decision whether to impose a penalty, and in her decision as to the appropriate level of that penalty.

Degree of cooperation with supervisory authority (Article 83(2)(f))

7.33. Marriott has cooperated fully with her investigation and this has been taken into account.

Categories of personal data affected (Article 83(2)(g))

7.34. The Commissioner has identified the relevant categories of personal data in Section 4 above. As noted there, the data included in some (but not all) cases unencrypted passport details, details of travel, and various other categories of personal information including name, gender, date of birth, VIP status, address, phone number, email address, and credit card data.

Manner in which the infringement became known to the Commissioner (Article 83(2)(h))

[112] See Marriott's First Representations, para 3.6 and Marriott's Second Representations, para 2.12 and Section 3.
[113] Marriott's First Representations, para 3.7.

7.35. Marriott notified the Commissioner of the Attack on 22 November 2018 and is considered to have complied with its obligations in this respect.

Conclusion at step 2

7.36. Taking into account: (a) the matters set out in Sections 2-4 and 6 above; (b) the matters referred to in this section; and (c) the need to apply an effective, proportionate and dissuasive fine in the context of a controller of Marriott's scale and turnover, the Commissioner considers that a penalty of £28 million would be appropriate, before adjustment in accordance with Steps 3-5 below and the application of the Commissioner's Covid-19 policy. This amount is considered appropriate to reflect the seriousness of the breach and takes into account in particular the need for the penalty to be effective, proportionate and dissuasive.

Step 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))

7.37. The amount of the penalty, as identified at Step 2, may be increased where there are 'other' aggravating factors.[114] In this case, the Commissioner does not consider there to be any other relevant aggravating factors. Thus, no adjustment is made to the penalty level determined at Step 2.

Step 4: Adding in an amount for a deterrent effect on others

7.38. The Commissioner is under an obligation to impose a penalty which is *"dissuasive"*. The need for the penalty to be dissuasive in relation to Marriott itself is addressed by the analysis at Step 2. Having regard to the amount of the penalty identified under step 2, the Commissioner does not consider it necessary to increase the penalty further under Step 4 to dissuade others.[115]

7.39. The Commissioner is not aware of widespread issues of poor practice that may be particularly deterred by the imposition of a higher penalty. Given Marriott's size and the scale of its operations, and the fact that the Commissioner has decided to impose a penalty that already takes those factors into account as part of the need to ensure that any penalty is proportionate, effective and dissuasive

[114] In accordance with Article 83(2)(k) GDPR, section 155(3)(k) DPA. and page 11 of the RAP.
[115] This makes redundant the points about this Step made by Marriott in its Representations.

and to reflect the seriousness of the breach, the Commissioner considers that no adjustment is necessary under Step 4.

Step 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship) (Article 83(2)(k))

7.40. As explained above, in principle, other relevant mitigating factors could be taken into account under Step 2 or Step 5 of the RAP. Previously the Commissioner considered such matters in the round under Step 2 of the RAP, taking into account the factors in Article 83 GDPR and section 155(3) DPA 2018. However, in the light of Marriott's representations for the purposes of this Penalty Notice the Commissioner has considered the relevant mitigating factors under Step 5.

7.41. Following the guidance set out at page 11 of the RAP, and having considered Marriott's Representations, the Commissioner has taken into account the following mitigating factors:

a. Marriott had, prior to becoming aware of the Attack, confirmed in 2018 a new $19 million security investment for 2019, which raised Marriott's budgeted spend for that year on security to $49.5million. Subsequent investment decisions in 2019 have raised Marriott's forecasted IT security budget spend on IT security for 2020 to $108.5million;

b. Marriott took immediate steps to mitigate the effects of the Attack and protect the interests of data subjects by implementing remedial measures;

c. Marriott cooperated fully with the Commissioner's investigation, including responding promptly to requests for information;

d. Widespread reporting in the media of the Attack is likely to have increased the awareness of other data controllers of the risks posed by cyber-attacks and of the need to ensure that they take all appropriate measures to secure personal data; and

e. The Attack and subsequent regulatory action has adversely affected Marriott's brand and reputation, which will have had some dissuasive effect on Marriott and other data controllers.

7.42. More specifically, the Commissioner has taken into account the fact that, upon being alerted to the Attack, Marriott acted promptly to mitigate the risk of damage suffered by data subjects, by way of the following technical remedial measures:

a. The deployment of real-time monitoring and forensic tools on 70,000 devices on the Starwood network;

b. Implementing password resets;

c. Disabling known compromised accounts; and

d. Implementing enhanced detection tools.

7.43. These measures should allow Marriott to prevent similar breaches in the future, including by identifying any additional attackers or malicious software being utilised on its servers.

7.44. The Commissioner has also taken into account the fact that Marriott also took steps to: (a) establish a notification and communication regime; (b) create a bespoke incident website in numerous languages; (c) send 9.2 million notification emails to data subjects whose country of residence was recorded in the Starwood Guest Reservation Database as being in the EU); (d) establish a dedicated call centre; (e) provide web monitoring to affected data subjects; (f) enhance its data subject rights programme; (g) engage with card networks; and (h) improve its technical and organisational measures generally.[116] It is also noted that Marriott informed a number of other regulatory and law enforcement agencies.

7.45. It is acknowledged that the steps outlined above will have gone some way to reassuring Marriott's customers, and therefore may have reduced or mitigated any distress caused by the breach. However, the fact that the Marriott call centre received 57,000 calls between 30 November 2018 and 31 May 2019 (7,500 of these being calls to EU-based call centres)[117] is indicative of the level of concern amongst affected data subjects on learning of the breach and subsequently.[118]

[116] Marriott's First Representations, para 3.4.
[117] Marriott's Second Representations, para 2.7(b)(ii).
[118] Contrary to para 2.7(a)(b)(i) of Marriott's Second Representations, it is not being suggested that all of those who called Marriott's call centre were suffering from distress or damage, but it is likely

7.46. Contrary to Marriott's submissions,[119] the fact that very few of these calls were escalated internally or resulted in a complaint is irrelevant. The information provided by Marriott suggests that call handlers had FAQs available to advise customers on how to respond to the breach etc, which was presumably intended to address most situations arising.[120] Thus, the fact that only a certain number of individuals had their calls escalated / resulted in a complaint does not provide any real indication of the extent to which individuals were distressed or harmed by the loss of their data.

7.47. Marriot also relied in this regard on a claim that the Commissioner's findings of distress and harm were materially undermined because the centre only received 57,000 calls when millions of individuals were affected by the breaches.[121] However, in circumstances where: (a) Marriott had established a dedicated website to address concerns; and (b) individuals may have sought advice from third parties and/or acted on their own knowledge and experience, the comparison between these figures does not undermine the Commissioner's findings. The number of calls is sufficiently large to suggest that there were data subjects who were concerned.

7.48. Thus, while the Commissioner has taken into account, as outlined below, the steps taken by Marriott to mitigate the impact of its breaches of the GDPR, she remains of the view that those actions would not have immediately neutralised all the concerns on the part of data subjects about their data being in the hands of criminals / outside of Marriott's control.

7.49. Having regard to the mitigating factors set out above, it is appropriate to reduce the £28 million penalty by 20%, i.e. to £22.4 million.

7.50. As a result of the Covid-19 pandemic, Marriott has also argued that any penalty should be reduced because of the financial hardship it would cause.

7.51. The Commissioner has considered Marriott's representations, and the evidence it has provided. Although the Covid-19 pandemic has

---

that – as stated here – the majority of callers were at least sufficiently concerned to make the call, which is inconsistent with Marriott's position that no or only trivial harm at all would have arisen.

[119] Marriott's Second Representations, para 2.7(b)(iii).

[120] Marriott's Second Representations, para 2.7(b)(iii).

[121] Marriott's Second Representations, para 2.7(b)(iv).

had a significant impact on Marriott's revenues, Marriott's overall financial position is such that the Commissioner does not consider that the imposition of a penalty in the range being proposed will cause financial hardship, or that Marriott will be unable to pay such a penalty.

7.652. However, the Commissioner has published guidance entitled "*The ICO's regulatory approach during the Coronavirus public health emergency*".[122] That guidance indicates that "*As set out in the Regulatory Action Policy, before issuing fines we take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces.*" While the proposed penalty will not cause financial hardship for Marriott, the Commissioner considers it appropriate to reduce the penalty that would otherwise have been imposed, in light of the current public health emergency and associated economic consequences. This is addressed below, separately from Step 5.

7.653. The Commissioner has carefully considered Marriott's submissions that there are other additional mitigating factors that should be taken into account in this case.[123] However, none of the points raised justify a further reduction of the appropriate penalty beyond the discount set out above. In particular:

a. The Commissioner does not consider it appropriate to further reduce the penalty by reference to costs to Marriott of taking measures to rectify or mitigate the impact of its infringement, including the cost establishing a bespoke website, call centre, web monitoring, the enhancement of Marriott's data subject rights programme, and any other customer-facing remediation activities. The fact that Marriott was required to expend a large amount – on Marriott's assessment in excess of $50 million[124] - in customer-facing remediation activities is not directly relevant to the amount of any penalty. The fact that mitigating measures were taken, in accordance with Marriott's obligations as a controller, has already been taken into account.

[122] Version 2.1, 13 July 2020.
[123] Marriott's First Representations, para 3.13(c).
[124] Marriott's First Representations, paras 3.4(a) and 3.13(c)(vi).

b. Marriott's preparations for the introduction of GDPR are noted.[125] However, these do not address the Commissioner's conclusions on Marriott's failure to implement appropriate security measures in relation to the systems it acquired from Starwood.

c. The Commissioner has recognised that the Attack involved persistent criminal activity.[126] But this does not alter the fact that the security of Marriott's network was inadequate in a number of respects, and that those failings could and should have been addressed on a prospective basis through the implementation of appropriate measures. It is Marriott's breaches of Articles 5(1)(f) and 32 GDPR for which it is being penalised, not the actions of third parties.

d. The security measures that were deployed on the Starwood security environment and on the Starwood Guest Reservation Database are noted.[127] However, the existence of these measures do not detract from the Commissioner's conclusions on Marriott's failure to implement appropriate security measures (see section 6). That Marriott took some steps to secure the Starwood system is not considered to be a mitigating factor in the circumstances of an infringement of this scale and severity.

7.54. Accordingly, having carefully considered the mitigating factors raised by Marriott, which are relevant to the assessment of the appropriate level of any penalty, the overall penalty payable by Marriott after Step 5 is £22.4 million.

Application of Covid-19 Policy

7.55. As described above, having regard to the impact of the Covid-19 pandemic (on Marriott and more generally), and consistently with the Commissioner's published guidance, a further reduction is appropriate and proportionate. The final penalty payable will therefore be reduced to £18.4 million.

[125] As relied upon at paras 3.13(c)(iii) of Marriott's First Representations.
[126] Marriott's First Representations, para 3.13(c)(iv).
[127] Marriott's First Representations, para 3.13(c)(i)-(ii).

Application of the fining tier(s) (Articles 83(4) and (5) GDPR)

7.56. The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) GDPR, whereas Article 32 falls within Article 83(4)(a). The appropriate tier is therefore that imposed by Article 83(5)(a) as this is the gravest breach in issue in this case.

7.57. In any event, for the year ended 31 December 2017 Marriott has confirmed that its relevant worldwide annual turnover is $4.997 billion. The penalty the Commissioner has decided to impose on Marriott is the sum of £18.4 million. This is considerably less than 4%, indeed considerably less than 1%, of Marriott's total worldwide annual turnover, and accordingly well within the cap imposed by Article 83(5) GDPR.

Marriott's other representations on the decision to impose a penalty and the appropriate Penalty amount

7.58. Marriott's Representations contained detailed submissions in response to: (a) the Commissioner's decision to impose a penalty at all; and (b) the proposed penalty amount, as indicated in the Notice of Intent. The Commissioner has carefully considered those submissions and, to the extent they have not been addressed above, responds to them below.

7.59. In summary, Marriott submitted as follows:

a. **First,** the Commissioner misapplied Article 83(2) in deciding to impose a fine and in determining the appropriate level of penalty. A proper application of that Article should result in no fine being imposed at all or, in the alternative, it should result in the imposition of only a low level of penalty;[128]

b. **Second,** the Commissioner unlawfully applied an unpublished internal document, entitled "*Draft Internal Procedure for Setting and Issuing Monetary Penalties*", in setting the proposed penalty on Marriott which was included in the NOI.[129] However, setting a proposed penalty amount without the Draft

[128] Marriott's First Representations, Executive Summary, para 8 and Section 3; and Marriott's Second Representations, Section 2.
[129] Marriott's First Representations, Executive Summary, para 9(a) and paras 4.2-4.12, 4.14(e), 4.19.

Internal Procedure (or similar), as the Commissioner did in the draft decision, also offends the principle of legal certainty.[130]

c. **Third,** the Commissioner erred by relying on turnover as the sole metric in determining the level of fine proposed in the NOI, and in continuing to treat turnover the most important factor in its quantification analysis in the draft decision;[131]

d. **Fourth**, the Commissioner has applied the wrong fining Tier under Article 83 GDPR in calculating the proposed fine;[132]

e. **Fifth,** the Commissioner erred in the NOI by applying an uplift to ensure an appropriate deterrent effect;[133]

f. **Sixth**, the Commissioner breached Marriott's legitimate expectation that she would operate her fining powers under the GDPR in accordance with past precedents, i.e. decisions made, under the DPA 1998 and/or only applying incremental increases to the fines that would have been imposed under the 1998 Act (which was subject to a £500,000 maximum fine limit).[134] This same failure, which Marriott described as a failure to comply with the *"Precedents-Based Approach",* is also said to amount to a breach of the principle of legal certainty.[135] In its Second Representations, in particular, Marriott contends that in the absence of any new guidance providing clear and specific quantification methodology determining how fines are to be calculated, any decision to issue a fine would breach that principle.[136] In this regard Marriott also relies on a comparison with a case decided by the Financial Conduct Authority (the "**FCA**") in respect of Tesco Bank.[137] It also relies on an alleged inconsistency between the penalty proposed in this case and those imposed through other decisions issued by the

[130] Marriott's Second Representations, Executive summary, para 1, and paras 1.1-1.5.
[131] Marriott's First Representations, Executive Summary, para 9(b), and paras 4.14-4.15 and Marriott's Second Representations, paras 1.35-1.38.
[132] Marriott's First Representations, Executive Summary, para 9(b), and paras 4.16-4.17.
[133] Marriott's First Representations, paras 4.24-4.30
[134] Marriott's First Representations, Executive Summary, para 9(c), and paras 4.36-4.41; Marriott's Second Representations, Executive Summary, para 1, and paras 1.1, and 1.28-1.31.
[135] Marriott's First Representations, Executive Summary, para 9(c), and paras 4.50-4.73; and Marriott's Second Representations, Executive Summary, para 1, and para 1.1.
[136] Marriott's Second Representations, Executive Summary, para 1, and paras 1.6-1.11.
[137] Marriott's First Representations, paras 4.31-4.35; and Marriott's Second Representations, paras 1.26-1.27

Commissioner and by other European supervisory authorities.[138]

g. **Seventh,** the Commissioner has acted contrary to the RAP because she has failed to calculate the penalty proposed in the NOI and the draft decision in accordance with its terms;[139] and

h. **Eighth,** the Commissioner proposed a penalty in the NOI which is disproportionate on its face NOI, and the revised penalty set out in the draft decision remains disproportionate.[140]

(1) Application of Article 83(2)

7.60. The Commissioner has described at paragraphs 7.3-7.53 how the factors listed in Article 83(2) apply to the facts of this case. In its Representations, Marriott criticised the Commissioner's findings in this regard. Where necessary those criticisms have been addressed at each step of the analysis set out above and/or in Section 6 above.

(2) Draft Internal Procedure

7.61. Prior to issuing the NOI in this case, the Commissioner had developed a Draft Internal Procedure for calculating proposed fines, as a supplement to the RAP. Its purpose was to provide an indicative guide, by reference to the turnover of the controller, as to the appropriate penalty. As the GDPR is a new regime, this additional tool was intended to assist the decision-makers in applying Article 83 GDPR and the RAP to the facts of a particular case.

7.62. Marriott made detailed submissions on this issue.[141] The Commissioner has considered those submissions in deciding how to approach the calculation of the penalty to be imposed in the draft decision, and ultimately in this Notice.

7.63. The Commissioner remains of the view that the controller's turnover is a relevant consideration in determining the appropriate level of penalty (see below), but she has decided that the Draft Internal Procedure should not be used. Therefore, in deciding the appropriate

[138] Marriott's Second Representations, Executive Summary, para 1, and paras 1.12-1.19.
[139] Marriott's First Representations, paras 4.42-4.49; and Marriott's Second Representations, Executive Summary, para 2, and paras 1.32-1.34.
[140] Marriott's First Representations, Executive Summary, para 9(d), and paras 4.74-4.77, and Executive Summary, para 1, and paras 1.39-1.41 of Marriott's Second Representations.
[141] See paras 4.2-4.12 of Marriott's First Representations and paragraphs 1.2-1.5 of Marriott's Second Representations in particular.

penalty in this case the Commissioner has not relied on the Draft Internal Procedure (she did not rely upon it for the purposes of her draft decision, and the same approach was adopted in preparing this Penalty Notice). She has instead relied only on Article 83 GDPR, section 155 DPA and the RAP. The approach taken to the calculation of the penalty for the purposes of this Notice is set out above.

7.64. Marriott is wrong to assert that, but for its pressing for disclosure in correspondence, the Commissioner would not have disclosed the draft guidance document.[142] The policy was provided on 2 August 2019 in response to a request made in a letter from Marriott dated 24 July 2019. The NOI set out how the penalty was arrived at. The Commissioner also provided further information about how the penalty was calculated in her letter of 17 July 2019. The Commissioner is obliged to consult the controller on the NOI and she did so. Marriott took the opportunity to make detailed submissions, and the Commissioner has carefully considered all those submissions, and acted upon them to address the concerns raised.

7.65. Marriott's First Representations also criticised the use of a percentage range as part of its process for calculating the proposed penalty (applying the Draft Internal Procedure) and/or the way in which the Commissioner applied the turnover bands at the NOI.[143] As this approach has not been adopted in this Notice, nor has the Draft Internal Procedure been applied, the Commissioner does not respond to the individual points made by Marriot on the application of the Draft Internal Procedure further here.

7.66. In its Second Representations, Marriott states that whilst it welcomes the fact that the Draft Internal Procedure is no longer relied upon by the Commissioner, (a) the Commissioner cannot rely upon the £99.2m figure proposed in the NOI as a reference point when assessing the legality or proportionality of the present proposed penalty figure;[144] (b) the RAP cannot constitute an adequate basis for the calculation of a penalty in circumstances where the Commissioner had previously devised the Draft Internal Procedure;[145] and (c) in the absence of the Draft Internal Procedure, there is a lack of clarity governing penalty calculation and

[142] Marriott's Representations, paras 4.2 and 4.8.
[143] Marriott's Representations, paras 4.19-4.23.
[144] Marriott's Second Representations, para 1.3.
[145] Marriott's Second Representations, para 1.4.

undermines legal certainty.[146] These points are not accepted for the following reasons.

7.67. First, the Commissioner does not seek to use the figure of £99.2m, as proposed in the NOI, as a "*reference point*" for the penalty set in the draft decision, or the present penalty. Rather, the Commissioner carried out a fresh calculation exercise having regard to the factors listed under Article 83 of the GDPR and the RAP. See further para 7.128 below.

7.68. Second, the Draft Internal Procedure was not developed to 'cure' any gap in legal certainty left by the RAP. It was intended to be a helpful supplement to the RAP for internal decision-making purposes. In deciding what level of penalty may (at the consultation stage) or is appropriate in this case, the Commissioner has always applied the approach set out in the RAP, and considered the factors under Article 83 GDPR. The fact that a document was created to provide supplemental detail to the RAP does not render the RAP so deficient so as to prevent a penalty being calculated in this case. Marriott's submissions on legal certainty are addressed in more detail below.

(3) The Commissioner's reliance on Marriott's turnover

7.69. Marriott advanced a number of criticisms of the Commissioner's reliance on turnover in calculating her proposed penalty in its First and Second Representations (see, for example, para 4.14 of its First Representations).

7.70. First, Marriott submitted that the only metric the Commissioner used to calculate the penalty proposed in the NOI was turnover. This is incorrect. As is clear from the NOI itself, while turnover was used as a starting point in seeking to assess the appropriate penalty, a range of other relevant factors were considered in accordance with the RAP and the GDPR. In any event, the turnover-bandings set out in the Draft Internal Procedure has not been used in preparing this Notice.

7.71. Second, Marriott submitted that turnover cannot be regarded as a core metric in a case such as this where the wrongdoer has not profited from the breach. Marriot claimed that there is no logical relationship between the breach and the controller's turnover. The

[146] Marriott's Second Representations, para 1.5.

Commissioner's approach, Marriott said, simply punishes a controller for being a large undertaking. Marriott compares the penalty proposed in this case to the Commissioner's decision regarding Doorstep Dispensaree Ltd, dated 20 December 2019, suggesting that this shows that the Commissioner is treating turnover, unjustifiably, as the most important factor.[147]

7.72. The Commissioner does not accept these arguments. She considers turnover to be a relevant consideration in determining the appropriate level of penalty in this case (as well as in other cases not involving a controller profiting from a breach), for the following reasons:

a. A turnover-based approach is consistent with the approach taken to penalties in the GDPR. The Data Protection Directive did not prescribe the level of fines that Member State authorities should impose for data breaches. The GDPR departs from that approach. In doing so, it expresses the maximum penalty in terms of a percentage of turnover. Turnover is therefore a relevant factor in determining the appropriate level of penalty to be imposed. This is also reflected in the Recitals, which make clear that the economic position of the controller is relevant even where the controller is a private person and not an undertaking: *"… Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine."*

b. Further, and in any event, the Commissioner is obliged to ensure that any penalties imposed are "*effective, proportionate and dissuasive*". Having regard to a data controller's turnover complies with this principle by ensuring that the level of any penalty is not only proportionate, but is also likely to be an effective and dissuasive deterrent for the undertaking on which it is imposed, and other equivalent controllers. It is self-evident that imposing the same penalty on an undertaking with a turnover of billions of pounds as would be imposed on a small or medium sized business would not be effective, proportionate or dissuasive. Comparable regulatory regimes that share the GDPR's emphasis on deterrence, such as under competition

[147] Marriott's Second Representations, paras 1.36-1.37.

law, also take turnover into account in in some form in setting penalties.

c. Marriott's claim that the introduction of the maximum amount safeguard caps in Articles 83(4) and (5) does not mean that turnover can be treated as a relevant metric is incorrect, for the reasons articulated in points (a) and (b) above.[148] In particular, Marriott's claim that treating turnover as a relevant metric *"outside of disgorgement of profits cases is illogical and perverse"*, does not withstand scrutiny. It is plain from the relevant provisions of the GDPR, read as a whole, that the economic position of a controller is one relevant factor in determining what penalty is appropriate on the particular facts of any case. The GDPR does not limit the relevance of turnover to cases involving disgorgement.

d. As to the decision in *Doorstep*, the difference between the turnover of that controller and Marriott is obviously relevant. However, each case is considered on its individual facts. Marriott's attempts to compare the number of records involved, and then scale up the appropriate level of fine (60 times the number of records, results in a maximum 60 times higher level of fine), are misconceived. See further paras 7.116-7.119 below.

7.73. Third, Marriott submitted that any penalty regime engages the fundamental rights of controllers, including their fundamental right to property as provided for under Article 1 of Protocol 1 of the European Convention on Human rights, and Article 17 of the EU Charter of Fundamental Rights.[149] The Commissioner recognises that in imposing a penalty on a controller, she must comply with any relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. However, it is not accepted that taking into account a controller's turnover in determining the appropriate penalty is incompatible with those rights because it is arbitrary or results in grossly disproportionate levels of penalty (as Marriott contended at para 4.14(c) of its First Representations). It is an approach that complies with the regime established by the GDPR.

[148] Marriott's First Representations, para 4.14(d).
[149] Marriott's First Representations, para 4.14(c).

7.74. Fourth, Marriott contended that the turnover approach is inconsistent with the RAP.[150] This is incorrect.

7.75. As explained above, the calculation of the proposed penalty in the NOI was not exclusively based on turnover, contrary to Marriott's claim. It took account of the various factors discussed in the RAP. This Notice addresses each step of the process of the RAP in turn to make even clearer that the penalty has been set in accordance with its terms. Turnover is relevant to establishing whether a penalty is appropriate, proportionate, effective and dissuasive in applying the steps set out in the RAP, as explained above.

7.76. Moreover, Marriott's reliance in this regard on reference in the RAP to circumstances in which the Commissioner will convene an advisory panel is misplaced.[151] The RAP describes "*very significant*" penalties as those *"expected to be those over the threshold of 1M"* in that particular context, i.e. the context in which the Commissioner may convene an advisory panel. This was not intended to be - and in any event cannot objectively be read as giving - an indication to controllers of the likely penalty they may face in the event of a data breach, particularly in light of the provisions of GDPR. The section of the RAP setting out how penalties will be calculated does not refer to the concept of "*very significant*" penalties at all.

7.77. Consequently, the RAP's discussion of when an advisory panel may be convened is no basis for saying that turnover is not a relevant factor in determining penalty. Marriott was also therefore wrong to claim in its Representations that: (a) the £1million figure referred to in the discussion of when an advisory panel may be appropriate should be the starting point for calculating fines in the most serious and significant cases before the Commissioner;[152] and (b) the Commissioner must justify imposing any fine above that threshold figure. This is a misreading of the RAP, see further below.

7.78. Firth, Marriott contended that what the Commissioner should have done in quantifying the appropriate penalty was to "*(a) start with what an infringement of this nature is objectively worth in penalty terms having regard to its nature, gravity and duration, irrespective of the financial stature of the wrongdoer; then (b) add or take away*

---

150 Marriott's First Representations, para 4.14(f).
151 Page 26 of the RAP. See also para 4.46 of Marriott's First Representations.
152 Marriott's First Representations, para 4.46.

amounts to reflect respectively aggravating and mitigating factors; before moving at the final stage of the analysis to (c) the question of whether, in view of all the circumstances, some increase in the penalty is required to ensure a deterrent effect."[153]

7.79. The Commissioner's approach is set out above. She has considered each step of the RAP, and all of the factors listed in Article 83 GDPR, in order to arrive at the overall appropriate penalty. Given that the financial stature of the wrongdoer would need to be taken into account at least in considering whether an increase in fine would be necessary to secure a deterrent effect, it is not clear that adopting the alternative structure proposed by Marriott would make any material difference to the outcome.

(4) The appropriate tier

7.80. In response to the NOI, Marriott submitted that the Commissioner had applied the wrong fining tier. It was said that the Commissioner incorrectly categorised the breaches in issue as a Tier 2 infringement, allowing for a maximum fine of 4% of turnover.[154] This submission was based, in summary, on the following points:

a. Article 5(1)(f) is simply a shorter, summary version, of the more detailed and specific obligation in Article 32. Article 32 GDPR therefore amounts to the *lex specialis* of Article 5(1)(f) and should therefore take precedence.

b. The maximum fine should be 2% in this case because:

i. Any ambiguity in the wording of a provision of law imposing a civil penalty should be resolved in favour of the controller.

ii. The wording of Article 83(4) makes clear that the intention was to impose this lower maximum cap for breaches of Article 32, which is the *lex specialis.*

7.81. The Commissioner does not accept these submissions, for the following reasons.

[153] Marriott's First Representations, para 4.15.
[154] Marriott's First Representations, paras 4.16-4.17.

7.82. First, the GDPR addresses expressly what the appropriate maximum fine should be when a controller breaches the *"basic principles of processing"* under Article 5 GDPR. Article 5(1)(f), as one of the basic principles of processing, cannot be dismissed as simply a summary of a later new provision included in the GDPR. The EU legislature has made it clear that a higher penalty is appropriate where a controller is found to have breached the basic principles of processing that underpin the regime. Contrary to Marriott's submissions, Article 83(5)(a) provides in clear in explicit and unambiguous terms that 4% is the appropriate cap for breaches of Article 5, including Article 5(1)(f).

7.83. Second, the GDPR also recognises that the same or linked processing operations may give rise to infringements of several provisions of that Regulation. It addresses this by making clear that the total amount of any penalty is to be the subject of the amount specified for the gravest infringement (see Article 83(3)).

7.84. Third, the principle of *lex specialis* means that "*where a legal issue falls within the ambit of a provision framed in general terms, but is also specifically addressed by another provision, the specific provision overrides the more general one.*"[155] The Commissioner does not accept that the application of the *lex specialis* principle precludes the Commissioner from treating this case as a Tier 2 infringement.

7.85. Article 5(1)(f) and Article 32 are evidently distinct provisions of the GDPR, *notwithstanding* the degree of overlap. Article 32 applies to processors, whilst Article 5 does not. Contrary to Marriott's submission, there is no basis upon which to give Article 32 precedence over Article 5(1)(f). They can be applied to controllers at the same time: Article 32 does not override the basic requirements laid down in Article 5(1)(f), read with Article 5(2), which establish the responsibility of the controller for demonstrating compliance with the security obligation and any breach of that principle.

7.86. Further, and in any event, the provisions in Article 83(4) and Article 83(5) are distinct provisions which make explicit provision for

[155] *R (Hallam) v Secretary of State for Justice* [2019] UKSC 2 at [144]. See also Case T-60/06 RENV II *Italy v Commission* (2016), at [81].

different fining tiers to apply to breaches of Articles 5 and 32 GDPR. It is clear that any infringement of Article 32 falls within the scope of Article 83(4) whilst an infringement of Article 5(1)(f) falls within the scope of Article 83(5). Article 83(4) is not more specific than Article 83(5). It is incapable of overriding or taking precedence over it. Rather, any issue as to which maximum penalty applies is resolved by the application of Article 83(3) which states in terms that in these circumstances "*the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*" The legislation itself provides the mechanism for addressing circumstances in which processing engages more than one obligation.

7.87. The Commissioner notes that her interpretation of Articles 83(4)-(5) is supported by the Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of the GDPR, which states:

> *Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case…*
>
> *The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12….*[156]

7.88. Fourth, in any event, Marriott's main objection to the use of the 4% maximum penalty appears to be its impact on the turnover-bands applied under the Draft Internal Procedure, which was applied in calculating the proposed fine included in the Notice of Intent. As this

[156] Pages 9-10.

approach has not been adopted in determining the final level of penalty to be imposed by this Notice, the same concerns do not arise. It is noted that the final penalty imposed is well below the 2% cap, and so the application of that cap in reaching the final decision, as opposed to a 4% cap, would have made no difference.

7.89. Marriott also asserted in a single paragraph of its First Representations that the Commissioner's approach to quantification is *"wholly arbitrary"*.[157] This is not accepted, either as a criticism of the NOI or this Notice. It appears that this argument rested on Marriott's contention that there are no clear and precise rules in place governing the setting of the penalty by the Commissioner. This claim is addressed below.

(5) An uplift to ensure a deterrent effect

7.90. Marriott claimed that the proposal in the NOI to increase the proposed penalty for the infringement to 2.5% to ensure that it would have a sufficient deterrent effect was arbitrary and unlawful.[158] This is not accepted. The Commissioner is obliged to consider whether such an uplift should be made under the RAP and Article 83 GDPR.

7.91. Marriott's criticisms of the NOI in this regard relied heavily on its criticisms of the previous use made of the Draft Internal Procedure's turnover-based approach in setting the proposed penalty at that stage.[159] These points have been addressed above. It is, however, important to note that para 61(d) of the NOI explained that in the light of the scale and severity of the infringement and factors discussed in para 61(a)-(c), a penalty of between 1.5 and 2% would be appropriate and proportionate. Para 61(f) then went on to consider what an appropriate uplift would be to ensure a deterrent effect, which was a separate issue that warranted individual consideration at a later stage of the analysis. These are separate steps under the RAP (see Section 2 above). It is therefore incorrect to assert, as Marriot did, that any uplift from the judged starting point means that the Commissioner: *"is knowingly imposing a disproportionate penalty sum."*[160]

---

[157] Marriott's First Representations, para 4.18.
[158] Marriott's First Representations, para 4.24.
[159] Marriott's First Representations, paras 4.25-4.30.
[160] Marriott's First Representations, para 4.25.

7.92. In any event, as set out above under Step 4, no additional amount has been added in this case for deterrent effect.

(6) Legitimate Expectation and Legal Certainty

The alleged legitimate expectation

7.93. In response to the NOI and draft decision, Marriott relied on selective quotes from public statements made by the Commissioner or her office about the new GDPR regime to contend that fines under the GDPR should be set in accordance with past precedents, i.e. decisions made under the DPA 1998.[161] What Marriott seeks, in effect, is for the Commissioner unilaterally to impose the previous domestic cap and approach to fines which applied in the UK prior to the harmonised regime under the GDPR.

7.94. Plainly it is not open to the Commissioner, as a matter of domestic or EU law, to adopt unilaterally an approach that would undermine the object and purpose of the new EU regime.

7.95. The GDPR, and consequently the DPA, represent a significant departure from the regime under DPA 1998 and the 1995 Directive. The GDPR was expressly intended to harmonise the rights of, and protections afforded to, data subjects across the EU. It differs markedly from the 1995 Directive, most obviously in that it introduces significantly higher and more effective penalties, with maximum penalties defined expressly by reference to turnover. The GDPR also imposes new obligations on controllers, including new organisational requirements such as the designation of a data protection officer and new provisions on the lawfulness of processing. The GDPR and the DPA have significantly changed the legal landscape in data protection and enforcement.

7.96. Marriott's submissions are to the effect that public statements made by the Commissioner override these changes, and as such she is bound to apply in effect the DPA 1998 and/or only apply incremental increases to the level of fine that would have been issued under that Act. Public statements made by the Commissioner or her staff, which are in any event quoted selectively and/or taken out of their proper context by Marriott, are incapable of achieving this outcome.

[161] Marriott's First Representations, paras 4.37-4.41. See also Marriott's First Representations, paras 4.65-4.66, see also Marriott's Second Representations, para 1.28-1.31.

7.97. More specifically, the public statements referred to by Marriott in its Representations were not intended to be – and cannot objectively be read as – assurances to any controller that the Commissioner would not use her powers on a case by case basis, to impose effective, proportionate and dissuasive penalties in appropriate cases. Marriott disputes this, however, the Commissioner maintains her position for the following reasons:

a. Marriott refers to a blog post published by Elizabeth Denham on 9 August 2017.[162] Whilst it is true that the post states that the Commissioner will not "*simply scale up penalties*" issued under the DPA 1998, it also states: "*Don't get me wrong, the UK fought for increased powers when the GDPR was being drawn up. Heavy fines for serious breaches reflect just how important personal data is in the 21st century world. We intend to use those powers proportionately and judiciously.*"

b. Marriott refers to a speech made by James Dipple-Johnstone at the Data Protection Practitioner's Conference on 9 April 2018,[163] however the quotation which Marriott selectively cited is preceded by a summary of the approach the Commissioner intended to take, including "*we will look at each case on its own merits. We'll look at the features and context of each case. And, this is important, we will focus on area of greatest risk to people – potential or actual harm… The more serious, high impact, deliberate, wilful or repeated breaches can expect the most robust response.*"

7.98. There is nothing within these quotations which can be read as giving rise to a legitimate expectation that the Commissioner would either: (a) issue fines in accordance with the previous maximum limit which applied under the DPA 1998 and/or past cases issued under that Act; or (b) only apply incremental increases to the level of fine that would have been imposed under the DPA 1998.[164] As made clear in the blog and speech to which Marriott has referred, the Commissioner had always been clear that she would (in accordance with her obligations) use her full powers on a case by case basis, to

[162] Marriott's Second Representations, para 1.29(a).
[163] Marriott's Second Representations, para 1.29(b).
[164] Marriott's Second Representations, paras 1.30-1.31.

impose effective, proportionate and dissuasive penalties in appropriate cases, which includes the possibility of large fines.

7.99. Marriott accepted in its Second Representations that the Commissioner is not constrained by the previous statutory maximum of £500,000.[165] But in practice, its attempt to limit the Commissioner to only making incremental increases to the fine level that would have applied under the DPA 1998 amounts to the same thing. The starting point is the application of Article 83 GDPR, the DPA 2018 and the RAP. It is not what the decision would have been under a superseded legal regime.

The alleged lack of legal certainty

7.100. As set out above, the Commissioner recognises that in imposing a penalty on a controller, she must comply with any relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. She does not accept, however, that the penalty regime applicable under, in particular, Article 83 GDPR lacks sufficient certainty such that it cannot be lawfully applied. That is in effect Marriott's case. It contends that unless the Commissioner applies a precedents-based approach based on decisions made under the DPA 1998, it is impossible for the Commissioner to meet the requirement of legal certainty.[166]

7.101. The DPA reflects the directly applicable EU law framework for determining penalties. The Commissioner does not agree with Marriott that Article 83 GDPR or section 155 DPA are so unclear that they are unlawful. Taken together, those provisions specify the circumstances in which a data protection authority has the power to impose an administrative penalty, and the matters that are relevant to that decision and the amount of any penalty. The legislative regime is supplemented by the RAP, which provides additional guidance in this regard. Contrary to para 4.60 of Marriott's First Representations, the RAP cannot be dismissed as *"unclear and open-ended"*.

7.102. Marriott's submissions on legal certainty are wrong for the following seven reasons.

---

[165] Marriott's Second Representations, para 1.30.
[166] Marriott's First Representations, paras 4.50-4.73.

7.103. First, in accordance with section 161 DPA 2018 the RAP was laid before Parliament for approval, and was duly approved.

7.104. In its Second Representations, Marriott emphasised the fact that Articles 83(8)-(9) and 70(1)(k) GDPR *"directly envisage and expect"* that the high-level principles set out in the legislation will be the subject of national or supranational guidance.[167] Pursuant to section 160 DPA, the Commissioner is obliged to issue guidance in respect of how she will determine the amount of penalties to be imposed. She has done so through the RAP.

7.105. Second, the RAP, which must be read alongside the DPA and, in particular, Article 83 GDPR, provides sufficient clarity and legal certainty, as required under the ECHR and EU law. In particular, the RAP explains that Step 2 intends to "censure" the breach, and this requires taking into consideration its scale (including the number of data subjects affected) and the severity of the breach itself, and expressly refers to the factors set out in the DPA. Examples of aggravating factors are set out in the RAP to assist with the interpretation of Step 3, as well as mitigating factors (to be considered at Step 5). Marriott's argument appears to be that because it is possible for the RAP to be more detailed, it must follow that the RAP is insufficiently detailed to fulfil the requirements of legal certainty. That is not the case.

7.106. It is not suggested that it is impossible to produce more detailed quantification guidance.[168] The GDPR is a new regime. Whilst not necessary for the purposes of legal certainty, more detailed guidance may well be developed over time as the UK and EU Member States gain experience in applying it. The Commissioner has committed to updating the guidance available in the future. However, the fact that there is potential for further development of the guidance does not mean that the present guidance is so unclear as to be unlawful. The RAP provides sufficient guidance as to the circumstances in which penalties, including large penalties, will be applied.

---

167 Marriott's Second Representations, para 1.9.
168 Marriott's Second Representations, para 1.10.

7.107. Third, it is neither necessary nor possible to produce a specific quantification framework which tells controllers precisely what level of fine they may face.

7.108. In para 1.9 of its Second Representations, Marriott claims that the Commissioner cannot lawfully impose penalties without setting out a further quantification methodology.[169] This is incorrect. The guidance available from Article 83 GDPR, the DPA and the RAP, cannot be rejected as legally uncertain purely on the basis that it does not attempt to specify exactly what levels of penalty might attach to wrongdoing.[170]

7.109. It would be impossible for the Commissioner to specify all the types of situations, and relevant circumstances, in which a penalty may be imposed under the GDPR. Nor could any guidance permit a controller to calculate specifically what any fine might be (especially by reference to a particular fine). The guidance must be general enough in order to cover a wide range of potential situations, and respect the general discretion of the Commission (subject to public law principles). The GDPR also requires the Commissioner to take a case-by-case approach, guided by the need to ensure that any penalty is effective, proportionate and dissuasive, and subject to the prescribed turnover caps.

7.110. Fourth, contrary to Marriott's submissions,[171] there is also no flaw in the Commissioner's approach because, on the particular facts of this case, no adjustments needed to be made at certain steps in the process. The draft decision explained clearly, in particular, that: (a) the need to ensure the penalty is dissuasive was taken into account sufficiently under Step 2 such that there was no need for a further uplift reflecting the need for the penalty sum to deter others under Step 4;[172] and (b) the mitigating factors had been taken into account under Step 2, so no adjustment was made at Step 5 to avoid 'double-counting'. The fact that certain steps did not require adjustments to be made in a particular case particular case does not render the RAP, which is intended to be of general application, "*deficient*".[173]

---

169 Marriott's Second Representations, para 7.93.
170 Marriott's Second Representations, paras 1.7-1.10.
171 Marriott's Second Representations, para 1.34.
172 Marriott's Second Representations, para 1.34.
173 Marriott's Second Representations, para 1.10, see also para 1.34.

7.111. In any event, to assist Marriott, the Commissioner has dealt with the mitigating factors arising in this case under Step 5 of the analysis (rather than Step 2, see para 7.40 above) so that it can see the impact of these factors on the overall level of penalty.

7.112. Fifth, as explained at paragraph 7.68 above, the Draft Internal Procedure was not developed and is not relied upon for the purposes of meeting the legal certainty requirement, contrary to Marriott's submissions during the course of the investigation.[174] While it was intended to be a helpful supplement to the RAP for internal decision-making purposes, it has been disregarded for the purposes of this Notice.

7.113. Sixth, for the reasons given above in respect of Marriott's legitimate expectation argument, it is not open to the Commissioner to re-impose the different, UK-only, legislative cap on fines in the manner sought by Marriott. The bands which applied under the DPA 1998, and the decisions made under it, cannot be relied upon as a justification for the Commissioner to fail to comply with EU law.

7.114. Finally, as to the claim made by Marriott that other bodies, namely the FCA and the EU Commission, apply more rigorous and more predictable rules, it is noted that each regulator must take enforcement action within the bounds of its own legal obligations, and in this case the Commissioner is bound to comply, in particular, with Article 83 of the GDPR.[175]

Other decisions by the Commissioner / Decisions by other European authorities

7.115. Marriott submitted in its Representations that the proposed penalty is inconsistent with previous action by the Commissioner and other EU supervisory authorities, contrary to the stated aim of GDPR being to create a harmonised regime.[176] In its Representations,[177] Marriott states that the proposed penalty is (a) inconsistent with action taken by other EU supervisory authorities, (b) contrary to the stated aim of the GDPR being a harmonised regime; and (c) inconsistent with

[174] Marriott's First Representations, para 4.61 and Marriott's Second Representations, para 1.4.
[175] The submissions made at paras 1.20-1.25 of Marriott's Second Representations are noted.
[176] Marriott's First Representations paras 4.69-4.73 and Marriott's Second Representations, paras 1.12-1.19.
[177] Marriott's Second Representations, paras 1.14-1.19.

the decision taken by the Commissioner in a different case. Marriott specifically refers to the following cases:

a. the decision by CNIL to impose a €50 million penalty on Google. Marriott contended that the infringements in Google's case were more serious than those considered in this Notice.

b. the Austrian Data Protection Authority against Osterreichische Post AG, which was fined €18 million;

c. a €2.6 million fine issued by the Bulgarian Commission of Personal Data Protection to the Bulgarian Revenue Agency in relation to a cyber-attack which affected over 5 million data subjects;

d. a fine of €645,000 imposed on Morele.net by the Polish supervisory authority for a cyber-attack affecting over 2 million data subjects;

e. a fine of €150,000 impose on Raiffeisen Bank by the Romanian supervisory authority concerning the misuse of customer data by employees of the bank;

f. the Romanian authority on UniCredit Bank SA. The company was fined of €130,000 for a breach of Article 25 GDPR due to the compromise of payment details, when its worldwide turnover for 2018 was of €18 billion; and

g. the Commissioner's decision regarding Doorstep Dispensaree Ltd, dated 20 December 2019.

7.116. The purpose of GDPR is, as Marriott contends, to secure a harmonised regime. However, that harmonisation is achieved through the application of harmonised rules and standards to the particular facts of the case at issue. Any cross-border processing decision must then be subject to the Article 60 process.

7.117. The Commissioner, along with other EU supervisory authorities, must comply with her obligations under Article 83 and that means that she is required to impose a penalty which, in her own judgment, having regard to all the matters listed in Article 83, and on the facts of the individual case, is effective, proportionate, and dissuasive. In principle, 'equivalent' breaches should attach 'equivalent' penalties.

But in practice, each case will turn on its own particular facts. Whilst the Commissioner has considered the limited information available about the cases to which Marriott has referred, she maintains that simple comparisons of the penalties imposed in different cases do not show that the Commissioner has erred in applying Article 83 GDPR, DPA and/or the RAP.

7.118. There is a great degree of variation in the penalties imposed by supervisory authorities even in the context of the limited fines imposed to date,[178] which are – in the Commissioner's view – indicative of a decision-making process that is fact-specific. It would be premature and not necessarily helpful to rely heavily at this juncture on a survey of the action taken by other supervisory authorities, given the relatively few decisions that have been taken under the new regime. This is particularly the case where there is limited public information available about the reasons for the decisions taken by other authorities.

7.119. In any event, as the Commissioner is acting as lead authority in this case, the way to ensure consistency is not by comparing the penalty to a selection of other penalties issued on different facts in the EU. Rather, the consistency mechanism provided for by Articles 60(4) and 63 GDPR will allow for all of the supervisory authorities concerned to cooperate with the Commissioner, make enquiries, and contribute their views in order to ensure the consistency of the ultimate penalty sum with penalties that have been (if there are any) and/or will be applied in similar situations. The Article 60 process is one of the factors which, as noted in Article 63, contributes to the consistent application of the GDPR and the Commissioner is entitled to rely on the process as a contributory factor.

(7) Application of the RAP

7.120. In response to the NOI and/or the draft decision, Marriott submitted that the Commissioner had acted contrary to the RAP by: (a) failing to consider separately the appropriate fines for the provisionally found breaches of Articles 33 and 34 GDPR, from those in relation to Articles 5(1)(f) and 32 GDPR; (b) failing to adopt the starting

[178] Notably the decision of the French SA, the CNIL, to fine Google 50 million Euros. See also https://www.enforcementtracker.com/ which suggests there is significant variation in the level of fines that have been imposed to date, ranging from a few thousand to millions of pounds.

point that any penalty of over £1 million is reserved for very significant cases; and/or (c) failing to correctly apply the factors that the RAP categorises as determining whether a higher penalty can be imposed."[179]

7.121. As to the first issue, the Commissioner has not included in her final decision a finding that Marriott breached Article 33 or 34 GDPR. Thus, this issue no longer arises.

7.122. The second issue is based on a misreading of the RAP. Marriott misunderstood the discussion of the circumstances in which she may convene an advisory panel. This point has been addressed above at paras 7.76-7.77.

7.123. In response to the draft decision, Marriott submitted that the Commissioner is seeking to *"reinterpret"* the wording of page 26 of the RAP in this regard. That is incorrect. The section of the RAP which addresses specifically the setting of a penalty does not refer to this concept of "*very significant*" penalties at all. This language is used only to describe the types of situations in which the Commissioner may convene an advisory panel."[180]

7.124. Marriott also submitted that the fact that: *"the ICO appears to have determined that this case is not significant enough to merit convening the panel, which is entirely inconsistent with the fine imposed and further demonstrates the arbitrariness of this process."* [181] This submission is unfounded. The Commissioner has discretion over whether to convene a panel. The reasons why a panel was not convened in this case was explained in correspondence, i.e. this decision would be subject to the Article 60 consultation process. In such circumstances, the panel was unnecessary. It does not imply that this case lacks significance. For the reasons outlined above, this case has been found to involve significant breaches of the GDPR.

7.125. The third issue was also based on a misinterpretation or misapplication of the RAP. Contrary to Marriott's submissions, [182] the RAP does not set out at page 27 the only categories of cases in which it is justifiable for the Commissioner to impose a high penalty. The

[179] Marriott's First Representations, paras 4.42-4.49 and Marriott's Second Representations, paras 1.32-1.34.
[180] Page 26 of the RAP.
[181] Marriott's Second Representations, para 1.33.
[182] Marriott's Second Representations, para 1.32.

examples provided are not to be applied as a list of criteria which must be met in any case before a penalty exceeding £1 million can be imposed. They provide a general indication of the circumstances in which a penalty will be higher. The Commissioner is not therefore departing from guidance in a manner which has to be justified. This Penalty Notice explains why the fine set is appropriate.

7.126. The GDPR was enacted in 2016 and came into force two years later. Data controllers, especially global undertakings of the size of Marriott, would have been fully aware of the maximum penalties permitted by GDPR. The reference to the sum of £1 million in the RAP does no more than describe the circumstances in which the Commissioner may decide to convene an advisory panel, and page 27 of the RAP cannot be relied upon to confine the Commissioner's power to impose penalties in the manner sought by Marriott. The decision as to whether a penalty should be imposed and at what level, in order to provide an effective, proportionate and dissuasive result has to be reached through the application of Article 83(2) GDPR and section 155 DPA 2018. It is clear from the RAP that the Commissioner will adopt a case-specific approach, taking into account all relevant considerations. That is the approach taken in this case.

(8) Proportionality

7.127. Marriott contends that the proposed penalty set out in the NOI was disproportionate on its face.[183] This argument is not accepted in respect of the provisional penalty that was proposed in the light of the information available at that time.

7.128. It is also not accepted that the penalty proposed in the draft decision was also disproportionate. That proposed penalty took account of and reflected the submissions made by Marriott in response to the NOI. Marriott criticised the approach taken in the draft decision on the basis that the claim that the fine proposed was proportionate rested inappropriately on a comparison with the level of penalty set out in the NOI[184]. That was not the approach taken. Section 7 of the draft decision explained clearly the basis upon which, at that time, the proposed penalty was proportionate. In any event, this Penalty Notice explains in clear terms why the level of final penalty imposed

[183] Marriott's First Representations, paras 4.74-4.77 and Second Representations, para 1.8.
[184] Marriott's Second Representations, paras 1.8 and 1.40.

is proportionate in the light of the findings reached by the Commissioner (see paragraphs 7.3-7.57 above).

7.129. The mathematical error made at para 5.43 of the draft decision is noted.[185] No such error is made at para 7.57 above.

8. HOW THE PENALTY IS TO BE PAID

8.1. The penalty must be paid to the Commissioner's office by BACS transfer or cheque.

8.2. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

9. ENFORCEMENT POWERS

9.1. The Commissioner will not take action to enforce a penalty unless:

- all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

9.2. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

[185] Marriott's Second Representations, para 1.41.

Dated the 30th day of October 2020

Signed: ……

Elizabeth Denham
Information Commissioner

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:e

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   General Regulatory Chamber
   HM Courts & Tribunals Service
   PO Box 9300
   Leicester
   LE1 8DJ

   a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).