

**Millennium & Copthorne Hotels plc ("M&C")**  
**General Data Protection Regulation (GDPR) – Status Update**  
**31 May 2018**

What is "GDPR"?

GDPR refers to the EU General Data Protection Regulation that applies to all member states of the European Union and came into effect on the 25<sup>th</sup> of May 2018. The changes ushered in by the GDPR are substantial and ambitious. At over 200 pages long the GDPR is one of the most wide-ranging pieces of legislation passed by the EU in recent years. GDPR expands the territorial scope of European data protection legislation to make it applicable not only to EU-based companies and organisations, but also to non-EU organisations offering goods and/or services to people in the EU or which are monitoring their behaviour (to the extent that the behaviour takes place in the EU). This means GDPR will capture virtually all of M&C's subsidiaries and operations globally, to varying degrees. The GDPR is based on seven key principles that underpin the regime, outlined below, whilst introducing many new governance and compliance requirements or reinforcing existing ones.

Article 5(1) of the GDPR requires that personal data shall be:

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(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').”

It is up to the data controller to demonstrate its compliance with these principles.

In addition, the GDPR significantly raises the stakes in terms of compliance, with maximum penalties of 4% annual global turnover (c. **£40m** based on M&C's 2017 results) or up to 20m Euros, whichever is higher, for significant violations.

#### What was M&C's process for becoming GDPR compliant?

M&C's Group General Counsel and Company Secretary led the GDPR implementation project, with support from the European legal team in the UK and external counsel. As least four global working group calls were convened over the past year, with regional and functional heads. Beyond that, regional and functional heads had appointed GDPR champions for their respective areas and the legal team members, in conjunction with external counsel, have been working with those champions on a day-to-day basis. In short, the process was broken down into four stages, outlined below:

1. *Data inventory and data mapping* – This work has been completed, as required by the GDPR, through surveys and interviews with members of the working group and their teams in order to understand what data we gather, why or for what purposes we gather it, how we gather it, and what we actually do with it.
2. *Gap analysis* – The work produced from the data inventory and data mapping exercises was reviewed and gap analyses for the various functions were prepared. These identified the areas where further work needed to be done in order to become compliant with GDPR.
3. *Implementation* – The initial implementation phase—in which the key requirements identified during the gap analysis phase were operationalised and incorporated into M&C's policies, procedures and practices—was substantially completed by the 25<sup>th</sup> of May 2018, in anticipation of the GDPR going live.
4. *Ongoing compliance* – Generally, we have adopted and will continue to follow a risk-based approach to compliance, with the greatest focus on higher risk areas or areas where larger amounts of personal data are processed. Since the GDPR imposes many, many ongoing administrative obligations on organisations, our compliance efforts did not stop on the 25<sup>th</sup> of May. These ongoing requirements include obligations to (among other things):
  - ✓ continually assess our processing of personal data to ensure it is accurate, up-to-date, used for the purposes for which we've collected, stored securely, etc.
  - ✓ prepare formal (written) Data Protection Impact Assessments for each new business initiative that will involve the processing of personal data,
  - ✓ continually review and update the myriad of policies and procedures that are being put in place for GDPR compliance,
  - ✓ regularly audit our processing of personal data to ensure compliance with applicable policies and procedures,
  - ✓ respond to suspected data breaches and report them to regulators (sometimes within a period of 24 hours from first learning of the potential breach),
  - ✓ respond to information requests by data subjects in a timely manner,
  - ✓ provide training to corporate and hotel staff to make sure they understand our, and their, obligations under GDPR and under M&C's policies, and
  - ✓ ensure that we obtain proper consents (to the extent required) from guests, suppliers, employees and other stakeholders for the processing of their personal data, and store these consents such that they can be retrieved easily and quickly, or ensure that we have other appropriate legal bases under GDPR for processing any such personal data.

### What have we done so far?

As matters of priority, the following key steps were implemented during the implementation phase of our GDPR compliance efforts. This work required input from many teams, including M&C's e-commerce, IT, commercial, marketing, human resources, operations and legal departments.

- *Changes to the booking process and M&C's global website privacy policy* – We updated our booking process to communicate more clearly how we use the personal data of our website customers and to give them greater control over marketing consents. At the same time we have endeavoured to make our external global data privacy and cookie policies, located at <https://www.millenniumhotels.com/en/utilities/privacy-and-cookie-policy/privacy-and-cookie-policy/>, more clear and comprehensive so that we don't have multiple conflicting policies for different consumer-facing elements of our business. The new website privacy policy was launched on Tuesday 22 May 2018 and a revised cookie policy will be launched shortly. A communication will then go out to all My Millennium members and those who have elected to receive marketing communications from M&C informing them of the updated policies.
- *Changes to our loyalty programme registration processes and marketing consent procedures* – Due to variations in previous consent procedures, we were required to “cleanse” our marketing database by asking members to re-consent to receive marketing, from M&C and third parties (via M&C). This was consistent with the approach adopted by Hilton, Four Seasons, Belmond, Mandarin Oriental and other hospitality companies. This campaign was launched on 21 May 2018 and ending on 24 May. As part of this work, we instituted stricter controls so that marketing campaigns will be run through a centralised process and will be handled in compliance with GDPR requirements. It's important to note that members of the My Millennium programme were not removed from the programme if they did not reaffirm their marketing consents, they simply were removed from the marketing database.
- *Changes to M&C's CRM system* – Bespoke and practical guidelines were developed for our CRM and central reservation system activities. These guidelines included data retention requirements and marketing consent procedures, and they were vetted with the relevant business teams that have responsibility for the CRM system. Technical changes to the CRM system are being scoped out, and will be implemented in due course, to make sure the system will be able to handle the various GDPR requirements.
- *Changes to M&C's guest registration cards globally* – Since the guest registration/check-in process is the one single point of contact for all of M&C's guests, the marketing consents on our guest registration cards are being aligned globally, subject to local legal requirements. All major operating regions of M&C have implemented the required changes. We also are testing an IT solution in the UK that would allow all guest registration cards to be digitised and inventoried by the hotels so evidence of consents provided by individuals can be retained for many years (and retrieved when necessary) without incurring large storage costs. We have adopted a policy to retain such consent information for a period of at least 6.5 years, subject to certain additional requirements and exceptions.
- *EU employment contracts and recruiting processes* – We have informed all EU employees of amendments to the data privacy provisions in their employment contracts arising from GDPR, and we have adopted a new employee data privacy notice that applies to all EU employees. Finally, we are working on a new external privacy policy to be used for recruitment efforts in the EU.

- *Supplier and intra-company data processing agreements* – In order to process guest, employee and other personal data, we are in the process of including GDPR compliant clauses in our supplier and other contracts and putting in place internal/intra-company data processing agreements among the relevant M&C entities around the world to the extent they process personal data. All of these clauses and agreements will include required protections for data subjects.

With regard to existing contracts, we are negotiating GDPR-related amendments to those and have created a log of the highest priority contracts pursuant to which suppliers or service providers process personal data of M&C guests or employees. These will include companies such as Microsoft (Office 365 email hosting and systems), Equiniti (shareholder information), ADP (payroll processing), Oracle (property management systems), and many others. We also have received and are reviewing dozens of data processing addendums from other parties, such as corporate clients, where we process personal data on behalf of other parties.

- *New or updated internal policies and procedures* – In conjunction with functional stakeholders, we are revamping our internal data protection policies and creating new ones as well, including a fully revised global data protection policy applicable to all employees within the Group, a data retention policy, an information security policy, an EU employee privacy notice (mentioned above), a data protection impact assessment policy, a comprehensive data breach policy, among others.
- *Confirmation of data controllers and registration with the authorities* – We are finalising the analysis and identification of the data controller and data processor entities within the Group. To the extent any new data controllers (those M&C entities that collect and control personal data of others) are identified as a result of GDPR, then we will proceed to register those entities with the UK Information Commissioner's Office as appropriate.

**Jonathon Grech**  
**Group General Counsel and Company Secretary**  
**31 May 2018**