Policy Statement

Brook Green UK DMC Ltd (the company)

Data Protection Policy Statement

A. The rationale for holding personal data.
   Sufficient detailed data should be held for a reasonable but not excessive period of time:
   a) To help facilitate travel and accommodation arrangements and attendance at meetings and events for individuals and groups organised and supervised by the company.
   b) To comply with legislation.
   c) To maintain contact with clients, and industry and update appropriately.
   d) To safeguard the company's assets.

B. The General Data Protection Regulation 2018
   1) Brook Green UK DMC Ltd is appropriately registered with the UK Information Commissioner.
   2) The basis on which information is held: information is generally held in the legitimate interests of the company – see Appendix 1;
      Some information is also held by consent.
   3) Data Personnel
      It is understood that there is no requirements for the company to appoint a Data Protection Officer as it does not engage in large scale processing of sensitive data, however the reference for all data issues is the Office Manager Isabel Leal.. The Data Controller is Brook Green UK DMC Ltd. Data Processors include NatWest Bank, Credit Card companies, Hotels and Suppliers.
   4) Where has the company's data come from and is any information sensitive?
      All personal information has been supplied by the individual, their employer, travel or event organiser or with their express agreement.
      Sensitive information as defined by the ICO is rarely held and only by consent.
   5) With whom is information shared?
      Information is shared with travel accommodation, meetings and events service providers with whom the company is contracted for the provision of such services to the individual concerned or with the individual's express agreement.
      No information is shared externally in any other circumstances.
   6) What information is held by the company?
      Personal information held by the company may include:
      a) For individuals, to whom travel accommodation meetings and events services are provided all relevant personal details required to facilitate the provision of such services or to comply with legal requirements
      b) For employers – contract, family, salaries, income tax and national insurance details, both paper and electronic.
      c) For other businesses – contact information.

7) Other relevant documents or notices
    a) The company has adopted a privacy statement which is attached as Appendix 2 and is also published on our website.
    b) Consent to hold information (including children's consent) – see Appendix 3.
    c) The company's Personal Data Breach Procedure policy is set out in Appendix 4.
    d) The company's lead data protection supervisory authority is The Information Commissioners Office (ICO).

Appendix 1

The Legitimate Interest Assessment (LIA)

a) Individuals
   1) What is / are the legitimate interests?
      To facilitate the travel, accommodation meetings and events services which the company is contracted to provide.
   2) Applying the necessary test.
      Processing of the information furthers the above process and there is no other way of achieving the same result.
   3) Undertake the balancing test.
      No private information is retained and individuals would expect their personal information to be used to ensure the proper enjoyment of the travel, accommodation and other services provided.

b) Corporate Contacts and Suppliers
   1) What is / are the legitimate interests?
      To respond to requests for proposals from agents and corporate entities.
   2) Apply the necessary test.
      Processing enables such requests to be met in a timely fashion and there is no other way of achieving the same result.
   3) No private information is retained and agents and corporate entities would expect their information to be used in this way.

c) Employees
   1) What is the legitimate interest?
      To effect appropriate employment checks, to monitor performance and effect appropriate communication.
      To facilitate payment of salaries, tax, national insurance and pension contributions.
      To maintain accurate records of all such payments for compliance purposes.
   2) Apply the necessary test.
      Processing furthers the above interests and there is no other way of achieving the same result.
   3) Undertake the balancing test.
      Only private information relative to compliance and good governance is retained.
      Individuals would expect their information to be used in this way and we are happy to explain our processing of their information to them.

Appendix 2

Policy Statement web site

This Privacy Policy ("Policy") sets out how Brook Green UK DMC Ltd protects the privacy of your personal information.

We need to collect, use and disclose personal information in order to perform our business functions and activities, including making and managing travel bookings on behalf of our customers. We are firmly committed to protecting the privacy and confidentiality of personal information and to maintaining various physical, electronic and procedural safeguards to protect personal information in our care.

By providing personal information to us (either directly or allowing another person to do so on your behalf), you agree that this Policy will apply to how we handle your personal information and you consent to us collecting, using and disclosing your personal information as detailed in this Policy. If you do not agree with any part of this Policy, you must not provide your personal information to us. If you do not provide us with your personal information, or if you withdraw a consent that you have given under this Policy, this may affect our ability to provide services to you or negatively impact the services we can provide to you. For example, most travel bookings must be made under the traveller's full name and must include contact details and appropriate identification (e.g. passport details). We cannot make bookings for you without that information.

There may be instances where your local data protection laws impose more restrictive information handling practices than the practices set out in this Policy. Where this occurs, we will adjust our information handling practices in your jurisdiction to comply with these local data protection laws.

1. **What personal information do we collect?**

Personal information has the meaning given under your local data protection law. Personal information generally means information which relates to a living individual who can be identified from that information, or from that information and other information in a person's possession, including any expression of opinion, whether true or not, and whether recorded in material form or not, about an identified or reasonably identifiable individual, and any indication of intention in respect of an individual.

Generally, the type of personal information we collect about you is the information that is needed to facilitate your travel arrangements and bookings and to arrange travel related services and/or products on your behalf. For example, we may collect details such as your name, residential/mailing address, telephone number, email address, credit/debit card details (including card type, card number, security number and expiry date), passport details, loyalty program / frequent flyer details, information about your dietary requirements and health issues (if any), and other details relevant to your travel arrangements or required by the relevant travel service provider(s) (e.g. airlines and accommodation or tour providers).

When you make contact with us for other purposes, we may also collect personal information about you in relation to those purposes. For example, we may collect your personal information so we can

contact you about a competition you have entered (e.g. if you win) or to respond to an enquiry or feedback you have sent to us. We also collect information that is required for use in the business activities of Brook Green UK DMC Ltd, including for example, financial details necessary in order to process various transactions, video surveillance footage used for security purposes, and other relevant personal information you may elect to provide to us.

Wherever possible we avoid requesting information which may be sensitive in nature. However In some circumstances, we may collect personal information from you which may be regarded as sensitive information under your local data protection laws. We will only hold sensitive information with your express consent.
We will not use sensitive information for purposes other than those for which it was collected.

2. **How do we collect personal information?**

We will collect personal information directly from you unless it is unreasonable or impracticable to do so. Generally, this collection will occur when you deal with us either in person, by telephone, letter, facsimile, email, when you visit any of our websites or when you connect with us via social media. We may collect personal information about you when you purchase or make enquiries about travel arrangements or other products and services; when you enter competitions or register for promotions; when you subscribe to receive marketing from us (e.g. e-newsletters); when you request brochures or other information from us; or when you provide information, or use our services, on social media. Unless you choose to do so under a pseudonym or anonymously, we may also collect your personal information (other than sensitive information) when you complete surveys or provide us with feedback.

In some circumstances, it may be necessary for us to collect personal information about you from a third party. This includes where a person makes a travel booking on your behalf which includes travel arrangements to be used by you (e.g. a family or group booking or a travel booking made for you by your employer). Where this occurs, we will rely on the authority of the person making the travel booking to act on behalf of any other traveller on the booking. By providing your personal information to us, either directly or through a family member, employer or other agent or representative in connection with a travel booking or related service, you will be deemed to have consented to your personal information being collected by us and used and disclosed in accordance with this Policy.
Where you make a travel booking on behalf of another person (e.g. a family or group booking or a travel booking made for an employee), you agree you have obtained the consent of the other person for Brook Green UK DMC Ltd to collect, use and disclose the other person's personal information in accordance with this Policy and that you have otherwise made the other person aware of this Policy. You should let us know immediately if you become aware that your personal information has been provided to us by another person without your consent or if you did not obtain consent before providing another person's personal information to us.

3. **When we act as agent for a travel service provider**

When we book and otherwise arrange travel related products and services for you, we usually do so as agent for or on behalf of travel service providers. In this case, we usually collect personal information about you both for our internal purposes as described in this Policy, including the purpose of us processing your booking, and for the travel service provider for whom we act as agent

for their internal purposes (e.g. to provide you with the booked services). As an agent, all bookings are made on your behalf subject to the terms and conditions, including privacy policy, imposed by these travel service providers. We will provide you with copies of all relevant travel service provider terms, conditions and privacy policies on request.

Accordingly, you are deemed to consent to the collection, use and disclosure of your personal information by us to the relevant travel service providers, and the use and disclosure of your personal information by the relevant travel service providers, for the purposes set out in this Policy and, to the extent permitted under your local data protection laws, for other purposes specified in their privacy policy. For example, if you book a hotel through us, then under this Policy you consent to us collecting your personal information and disclosing that information to the hotel to enable your room to be booked and for the hotel to provide accommodation to you, and, to the extent permitted under your local data protection laws, for other purposes specified in their privacy policy. We act as agent for or on behalf of many thousands of travel service providers around the world, so it is not possible for us to set out in this Policy all of the travel service providers for whom we act or their locations. For more information about the disclosure of personal information to travel service providers located overseas, please contact us.

If you have any concerns regarding the transfer of your personal information to a travel service provider, or you wish to contact us for further information, please contact us.

4. **How do we use and disclose your personal information?**

Where you contact us in relation to a travel booking or query, the primary purpose for which we collect your personal information is generally to provide you with travel advice and/or to assist you with booking travel and/or travel related products and services. However, the purpose for collection may differ depending on the particular circumstances as disclosed in this Policy (e.g. collection of your personal information for the purpose of your participation in a competition, provision of feedback, etc).

By continuing to use our services and/or by providing us with personal information (or allowing another person to do so on your behalf), you consent to us using and disclosing your personal information for the purpose for which it was collected, and, where permitted by your local data protection laws, for any related secondary purpose which we believe you would reasonably expect.

The purposes for which we collect personal information, and those secondary purposes which we consider to be directly related, include:

- providing you with any additional travel products and services you might request us to organize for you;
- identification of fraud or error;
- regulatory reporting and compliance;
- developing and improving our products and services and those of our related entities;
- servicing our relationship with you by, among other things, creating and maintaining a customer profile to enable us to service you better or presenting options on our website we think may interest you based on your browsing and preferences;
- involving you in market research, gauging customer satisfaction and seeking feedback regarding our relationship with you and/or the service we have provided;
- to facilitate your participation in loyalty programs;
- for research and analysis in relation to our business and services, including but not limited to trends and preferences in sales and travel destinations and use of our websites;
- internal accounting and administration;

- to comply with our legal obligations and any applicable customs/immigration requirements relating to your travel; and
- other purposes as authorised or required by law (e.g. to prevent a threat to life, health or safety, or to enforce our legal rights).

Promotional/marketing material

Where permitted by local data protection laws, we may use your personal information to send you targeted marketing activities relating to our products and services (and those of third parties) that we think may interest you, unless you have requested not to receive such information. These may include, but are not limited to, mail outs, electronic marketing (including online targeted marketing) and notifications as described below, and telephone calls). We will only use your personal information to send electronic marketing materials to you (including e-newsletters, email, SMS, MSM and iM) if you have opted-in to receive them. You can subscribe to receive e-newsletters and other electronic promotional/marketing materials by following the relevant links on our website or requesting one of our consultants to do so for you.

Should you no longer wish to receive promotional/marketing material from us, participate in market research or receive other types of communication from us, please contact us. You can unsubscribe from receiving electronic marketing materials by following the unsubscribe prompt in your email, or other form of electronic marketing.

5. **Is personal information disclosed to third parties?**

In some circumstances we may disclose your personal information to third parties, as set out below, and in accordance with your local data protection laws. By continuing to use our services and/or by providing us with your personal information (or allowing another person to do so on your behalf), you consent to that personal information being processed, transferred and/or disclosed by us for the purpose for which it was collected and, where permitted by your local data protection laws, for any related secondary purpose which we believe you would reasonably expect. Note that, in this Policy, where we say "disclose", this includes to transfer, share (including verbally and in writing), send, or otherwise make available or accessible your personal information to another person or entity.

Your personal information may be disclosed to the following types of third parties:

- our contractors, suppliers and service providers, including without limitation:
- in each of the circumstances set out in the section titled "How do we use and disclose your personal information?";
- suppliers of IT based solutions that assist us in providing products and services to you (such as any external data hosting provider(s) we may use);
- publishers, printers and distributors of marketing material;
- event and expo organisers;
- marketing, market research, research and analysis and communications agencies;
- mailing houses, freight services, courier services; and
- external business advisers (such as lawyers, accountants, auditors and recruitment consultants);
- our related entities and brands;
- travel service providers such as travel wholesalers, tour operators, airlines, hotels, car rental companies, transfer handlers and other related service providers;
- a prospective purchaser, in connection with a merger, acquisition, reorganisation or sale of DMC, business lines, or related bodies corporate and franchisees;
- a person making your travel booking on your behalf, where you are travelling on a booking made on your behalf by another person (for example, a family member, friend or work colleague);

- your employer, where you are an employee of one of our corporate, business or government clients and you are participating in an event or travelling for work purposes;
- a person who can verify to us that they have a relationship with you (e.g. a family member) where you are not contactable, the person correctly answers our required security questions and the request is, in our opinion, in your interest (for example, where the person is concerned for your welfare or needs to undertake action on your behalf due to unforeseen circumstances);
- as required or authorised by applicable law, and to comply with our legal obligations;
- customs and immigration to comply with our legal obligations and any applicable customs/immigration requirements relating to your travel;
- government agencies and public authorities, to comply with a valid and authorized request, including a court order or other valid legal process;
- various regulatory bodies and law enforcement officials and agencies, including to protect against fraud and for related security purposes; and
- enforcement agencies where we suspect that unlawful activity has been or may be engaged in and the personal information is a necessary part of our investigation or reporting of the matter.

For more information in relation to collection by travel service providers and their privacy practices and policies, see the section above titled, "When we act as agent".

Other than the above, we will not disclose your personal information without your consent unless we reasonably believe that disclosure is necessary to lessen or prevent a threat to life, health or safety of an individual or to public health or safety or for certain action to be undertaken by an enforcement body (e.g. prevention, detection, investigation, prosecution or punishment of criminal offences), or where such disclosure is authorised or required by law (including applicable privacy / data protection laws).

6. **Security of information**

Brook Green UK DMC Ltd has implemented various physical, electronic and managerial security procedures in order to protect the personal information it holds from loss and misuse, and from unauthorized access, modification, disclosure and interference. Brook Green UK DMC Ltd regularly reviews security technologies and will strive to protect your personal information as fully as we protect our own confidential information. Brook Green UK DMC Ltd is not responsible for any third party's actions or their security controls with respect to information that third parties may collect or process via their websites, services or otherwise.

We will destroy or de-identify personal information once we no longer require it for our business purposes, or as required by law.

7. **Access to and correction of personal information**

You are entitled to access any personal information we may hold about you in accordance with your local data protection laws. Where personal information we hold about you is not accurate, complete or up-to-date or the information is irrelevant or misleading, you may ask us to correct that personal information, and we will respond to your request within a reasonable time. We reserve the right to confirm the identity of the person seeking access or correction to personal information before complying with such a request. We reserve the right to deny you access for any reason permitted under applicable law. If we deny access or correction, we will provide you with written reasons for such denial unless it is unreasonable to do so and, where required by local data protection laws, will note your request and the denial of same in our records. If you wish to access or seek correction of

any personal information we hold about you, please refer to the "Feedback / Complaints / Contact" section below.
You must always provide accurate information and you agree to update it whenever necessary. You also agree that, in the absence of any update, we can assume that the information submitted to us is correct, unless we subsequently become aware that it is not correct.

8. **Social Media Integrations**

Our websites and mobile applications may use social media features and widgets (such as "Like" and "Share" buttons/widgets) ("**SM Features**"). These are provided and operated by third party companies (e.g. Facebook) and either hosted by a third party or hosted directly on our website or mobile application. SM Features may collect information such as the page you are visiting on our website/mobile application, your IP address, and may set cookies to enable the SM Feature to function properly.
If you are logged into your account with the third party company, then the third party may be able to link information about your visit to and use of our website or mobile application to your social media account with them. Similarly, your interactions with the SM Features may be recorded by the third party. In addition, the third party company may send us information in line with their policies, such as your name, profile picture, gender, friend lists and any other information you have chosen to make available, and we may share information with the third party company for the purposes of serving targeted marketing to you via the third party social media platform. You can manage the sharing of information and opt out from targeted marketing via your privacy settings for the third party social media platform.
Your interactions with these SM Features are governed by the privacy policy of the third party company providing them. For more information about the data practices of these third party companies, and to find out more about what data is collected about you and how the third party uses such data, please refer to their privacy policy directly.

9. **IP addresses**

When you access our website, use any of our mobile applications or open electronic correspondence or communications from us, our servers may record data regarding your device and the network you are using to connect with us, including your IP address. An IP address is a series of numbers which identify your computer, and which are generally assigned when you access the internet. Alone, IP addresses are not personal information, as any one computer or device may be used by multiple people (i.e. it is not possible to ascertain the identity of a user simply from the computer or device being used).
We may use IP addresses for system administration, investigation of security issues and compiling anonymised data regarding usage of our website and/or mobile applications. We may also link IP addresses to other personal information we hold about you and use it for the purposes described above (e.g. to better tailor our marketing and advertising materials, provided you have opted in to receive electronic marketing).

10. **Linked Sites**

Our websites may contain links to third party websites over which we have no control. We are not responsible for the privacy practices or the content of such websites. We encourage you to read the privacy policies of any linked third party websites you visit as their privacy policy and practices may differ from ours.

11. **Feedback / Complaints / Contact**

If you have any enquiries, comments or complaints about this Policy or our handling of your personal information, please contact your account manager or consultant, or contact us at: 020 7371 4155. We will respond to any enquiries or complaints received as soon as practicable.

12. **Changes to our Policy**

We may amend this Policy from time to time. If we make a change to the Policy, the revised version will be posted on our website at www.brookgreenuk.com. It is your responsibility, and we encourage you, to check the website from time to time in order to determine whether there have been any changes.

Last updated May 2018.

Appendix 3

In giving us, whether directly or through your employers or tour or event organiser, the details we have requested, you are consenting to us using and processing the data in accordance with our policy statement in Appendix 2.

If you are giving details on behalf of children under the age of 16, you are giving consent to us on their behalf.

Consent to hold and process data can be withdrawn at any time by those who have previously agreed to receive information from us.

Appendix 4

Personal Data Breach Policy

Brook Green UK DMC Ltd

Overview

a) If something happens to affect the confidentiality, integrity or availability of personal data, the company will immediately assess whether a personal data breach has occurred.

b) The company is well placed to identify any such event due to the tight control mechanisms it has in place for all paper and electronic data. These are described in the detail below.

c) If a data breach is likely to put at risk the rights and freedoms of any individual, the company will notify both the ICO and the individual concerned using the contact details it holds on record. It will also take appropriate steps to investigate any possible adverse effects and deal with the breach.

Unauthorised disclosure or loss of personal data

1. Brook Green is required under the General Data Protection Regulation to ensure the security and confidentiality of all the personal and sensitive personal data it processes including that processed by third parties acting on its behalf. Every care should be taken by staff to protect the personal data they work with and to avoid the unauthorised disclosure or loss of personal data.

2. This policy applies to all personal and sensitive personal data processed by Brook Green or anyone acting on behalf of Brook Green, as defined by sections 1 and 2 of the General Data Protection Regulation.

Legislative framework

3. There are six Data Protection Principles contained in the General Data Protection Regulation which must be complied with when processing personal data. Failure to comply with any of these Principles is a breach of the General Data Protection Regulation, Article 5. This policy is concerned with the Sixth Data Protection Principle: 'Data must 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.'

4. Examples of a breach of this Principle would include:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;

- databases containing personal data being compromised, for example being illegally accessed by individuals outside of Brook Green;

• loss or theft of laptops, mobile devices, or paper records containing personal data; • paper records containing personal data being left unprotected for anyone to see, for example:

— files left out when the owner is away from their desk and at the end of the day;

— papers not properly disposed of in secure disposal bins that can then be extracted or seen by others;

— papers left at photocopying machines;

• staff accessing or disclosing personal data outside the requirements or authorisation of their job;

• being deceived by a third party into improperly releasing the personal data of another person; and

• the loss of personal data due to unforeseen circumstances such as a fire or flood.

The difference between a security breach and a data breach and the notification process to follow

5. A data breach relates to the loss of personal data and should be notified following the procedure described. A security breach relates to the loss of equipment containing personal data. Where a security breach has been notified that also involves personal data staff must also follow the data breach policy.

Action to be taken in the event of a data breach

6. On discovery of a data breach the following actions should be taken:

• Containment and recovery

• Assessing the risk

• Notification of breach to the Information Commissioner's Office (ICO)

• Evaluation and response

Containment and recovery

7. **Who is responsible for action?** The individual committing the breach, their staff manager (and work manager, if different).

Action to be taken

8. The immediate priority is to contain the breach and limit its scope and impact.

9. Where personal data has been sent to someone not authorised to see it staff should:

• tell the recipient not to pass it on or discuss it with anyone else;

• tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;

- warn the recipient of any implications if they further disclose the data; and
- inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

10. The Senior team member responsible for the area where the breach occurred must be notified and they must immediately report it to Isabel Leal, the Office Manager providing the following information:

- date and time of the breach;
- date and time breach detected;
- who committed the breach;
- details of the breach;
- number of data subjects involved; and
- details of actions already taken in relation to the containment and recovery.

11. The Office Manager or senior member of staff on duty will conduct an investigation into the breach and prepare a report. This report will follow the ICO's guidance on Breach Management and will consider the following:

- How the breach occurred.
- The type of personal data involved.
- The number of data subjects affected by the breach.
- Who the data subjects are.
- The sensitivity of the data breached.
- What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?
- What could happen if the personal data is used inappropriately or illegally?
- For personal data that has been lost or stolen, are there any protections in place such as encryption?
- Are there reputational risks from a loss of public confidence in the service Brook Green provides?

Notifying the Information Commissioner

Action to be taken

12. The Office Manager or senior member of staff on duty will determine whether the breach is one which is required to be notified to the ICO.

13. If appropriate a breach notification form will be completed and the ICO notified as soon as practible.

Evaluation and response

14. Once the breach has been dealt with, the cause of the breach will be investigated. As appropriate policies and procedures will be reviewed and any additional training of personnel undertaken.