Flightline Travel Management Ltd

Data Processing Agreement

Version 1 – updated 01/03/2018.

This sets out the rights and responsibilities under UK data protection law to be agreed between Flightline Travel Management Ltd and its Client/Suppliers.

Version control:

Version	Change	Author	Date
1.0	Initial Agreement	Jim McDaid	12/10/2017

Contents

Data Processing Agreement

This document may form part of a Client/Supplier Agreement or Contract between Flightline Travel Management Ltd and a new Client/Supplier, or as a standalone agreement.

This agreement is based on UK state laws, and on the assumption that the Client/Supplier and Flightline Travel Management Ltd are both acting in the course of business. This agreement sets out the general arrangements around data protection in line with the EU's General Data Protection Regulation coming into force, May 25th 2018, and will be applicable whenever you are contracted to provide services to us.

Definitions

Below is a list of specific terms that are used throughout the Agreement, and their given meanings.

- **Agreement/Contract** – means a signed contract between (i) Flightline Travel Management Ltd and the Client/Supplier, including any Annexes;
- **Order** – means Flightline Travel Management purchase order or a written agreement with the Client/Supplier regarding the purchase or supply of services together with all documents referred to therein and including any variations thereto made by an Amendment Order.
- **Data** – any work that involves classified materials (i.e. proprietary, trade secrets, sensitive, confidential, personal/private information and data) generated to or accessed by the Client/Supplier in the performance of the Contract.
- **Personal Data** – means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- **Processing –** means any operation or set of operations performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Controller –** means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data, such as Flightline Travel Management Ltd; where the purposes and means of processing are determined by EU or UK state laws, the Controller (or the criteria for nominating the Controller) may be designated by those laws.
- **Processor** – means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller, such as the Client/Supplier.
- **Consent (of the Data Subject)** – means any freely given, specific, informed and unambiguous indication of his or her wishes by which the Data Subject, either by a statement or by a clear affirmative action, signifies agreement to Personal Data relating to them being processed.
- **Data Subject** – is a natural person whose Personal Data is processed by a Controller or Processor.

Scope

The Client/Supplier is made aware that the enacted General Data Protection Regulation (Regulation 2016/679/EU) on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, will supersede the Data Protection Directive (Directive 95/46/EC) from the date of its entering into force i.e. 25 May 2018. The General Data Protection Regulation will therefore apply to any ongoing and active relationship between Flightline Travel Management Ltd and its Client/Suppliers where Personal Data is processed upon the signing of this Agreement by both parties, upon such time the GDPR enters into force in EU and UK state law, or whichever is sooner.

Purpose of the Data Processing Agreement

This Data Processing Agreement is therefore applicable for Client/Suppliers who provide services to or from Flightline Travel Management Ltd which involves the processing, management, storage or transfer of any Personal Data provided by Flightline Travel Management Ltd staff or its clients. As detailed in the Definitions, these kinds of Client/Suppliers will be referred to as a **Processor** (of Personal Data), and Flightline Travel Management Ltd will be referred to as the **Controller** (of Personal Data).

This Data Processing Agreement governs the processing of Personal Data as defined by the Data Protection Act 1998 and the GDPR Article 4(2). Hence the objective of the Data Protection Agreement is to ensure compliance with the relevant data protection laws in force at any time of the Agreement, including the safeguard for the protection of privacy and the fundamental human rights and freedoms in connection with the Processer being granted access to process Personal Data.

In the event that tasks performed and supported by the Processor involve the processing, including storage of Personal Data, the Processor must ensure the safeguards of the Personal Data it stores. The Processor is therefore responsible for implementing the correct and appropriate safeguards for the protection of their storage, database, networking, computing and infrastructure necessary for the security their IT systems and processes. The Processor must also take adequate measures to protect against any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Types of data covered by the Data Processing Agreement

The Data Processing Agreement covers the processing of all Personal Data relevant to the fulfillment of the Order, including but not limited to information on:

- **Genetic data** – data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- **Biometric data** – data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- **Data concerning health** – data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

- **Employment data** – data relating to a Data Subject's act of employing or the state of being employed, the work or occupation in which a Data Subject is employed, the purpose for which they are employed, or other details about their employment and employer that is identifiable to a specific individual or group of individuals.

In the event that the processing incudes such Personal Data as heretofore described, this, under the Data Protection Act 1998 and GDPR constitutes Sensitive Personal Data. The data processed might also include data which is not Sensitive Personal Data as defined in the Data Protection Act 1998 or in the GDPR. Such data shall however for the purposes of this Agreement be treated as Personal Data within the meaning of the Data Protection Act 1998 and/or the GDPR.

Clauses

1. Security and safeguards

1.1. The Processor shall act exclusively on documented instructions from the Controller. The Processor shall ensure that the data entrusted is not used for other purposes or processed in any other way that as stated in the Controller's instructions, including the transfer of data to a third country or international organisation.

1.2. The Processor shall process the data in accordance with the EU and UK state law in force at any time or other regulation regarding Personal Data or provisions laid down under law or other regulation. If the Processor deems an instruction to be in breach of such legislation, the Processor shall promptly inform the Controller accordingly. However, this shall not apply if the law in question prohibits such notification for reasons of substantial public interest.

1.3. The Processor may not process Personal Data for any purpose than instructed, unless the Processor is obliged to do so under EU law or UK state law. If so, the Processor shall notify the Controller of such legal obligation before commencing the processing.

1.4. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller. The record shall include the following:

1.4.1. The name and contact information of the Processor, any sub-contractor as referred to in Clause 3.5 of the Contract, Flightline Travel Management Ltd, the Data Protection Officer and, where relevant, the representative of the Processor.

1.4.2. The categories of processing carried out by the Processor or any sub-contractor on behalf of Flightline Travel Management Ltd.

1.4.3. A general description of the technical and organisational security measures undertaken by the Processor to safeguard the Data (see Article. 32(1) in the General Data Protection Regulation).

1.5. The list shall be in writing, including in electronic format. At the request of the Controller, the Processor shall at any time make the list available to the Controller or the Information Commissioner's Office (ICO).

1.6. Where the processing of Data by the Processor takes place in home offices, in whole or in part, the Processor shall lay down guidelines for the personnel's processing of Data in home offices. The guidelines shall be submitted to Flightline Travel Management Ltd for approval.

1.7. Both the Processor and Controller shall comply with all GDPR requirements in accordance with the law in force at any given time.

1.8. The Processor shall participate in discussions, if any, with the Controller or/and the ICO and implement any recommendations and/or improvement notices, etc., from the Controller or/and ICO regarding the processing of Data. The Processor shall promptly inform the Controller if the ICO contacts the Processor regarding the delivery of any services and related support services covered by the Contract.

1.9. The Processor furthermore undertakes to promptly notify the Controller in writing to jim@Flightline Travel Management Ltd.co.uk of:

1.9.1. Any request by a public authority for transfer of Data covered by the Contract, unless the notification of the Controller is explicitly prohibited by law, e.g. pursuant to rules designed to ensure the non-disclosure of investigations performed by a law-enforcement authority.

1.9.2. Any request for access received directly from the Data Subject or from a third party unless such procedure has been approved.

1.10. The Parties undertake, for the duration of the Contract, to obtain and maintain the required approvals and consent, which the Party is obliged to obtain and maintain in accordance with the law in force at any given time.

2. Technical and organisational measures

2.1. To ensure the protection of the Data in order to comply with the data protection laws in the UK, the Processor shall take the technical and orgnisational measures necessary pursuant to Principle 7 of the Data Protection Act 1998, and Article 28(3) of the General Data Protection Regulation.

2.2. The Processor must implement and thus safeguard the Data with the necessary technical and organisational measures (with regard to storage, computing, networking access, transfer, input, order and availability control). Protective measures include using state-of-the-art software, computers and encryption methods as well as the use of adequate access controls, password procedures, automatic blocking, case specific authorisation concepts, logging and documentation of processes and the implementation of a data security concept.

2.3. The measures taken shall be adequate for the protection of the specific Data, and protect against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in breach of the law in force at any time, including but not limited to the Data Protection Act 1998, and the General Data Protection Regulation. This shall also apply if the processing of Data takes place, in whole or in part, in home offices.

2.4. If the Processor is established in another EU Member State, the Processor shall comply with both the security requirements laid down in applicable UK state law and the security requirements laid down in the EU Member State of the Processor.

2.5. On transferring the Data, data carriers, electronically transmitted Data or Data made available for download shall be secured against unauthorised access, including unauthorised access by members of the commissioned transport service providers.

3. Monitoring of information security and data protection

3.1. At the Controller's request, the Processor shall give the Controller sufficient information for the Controller's monitoring and documentation of the Processor's implementation of the necessary technical and organisational security measures.

3.2. The determination of the necessary technical and organisational security measures shall be with due observance of:

3.2.1. Any special requirements on information security (if applicable) are laid down in Appendix A.

3.2.2. The Controller's instructions based on the data protection impact assessment in force at any time pursuant to Article 35 of the General Data Protection Regulation and this Data Processing Agreement.

3.3. Where the Processor (and any sub-contractor) processes Sensitive Personal Data on the Controller's behalf for a period of 12 months or more, the Processor shall arrange for an independent third party to provide a statement to the Controller regarding compliance with the requirements of this Data Processing Agreement on a recurring 36-month cyclical basis.

3.3.1. The statement shall include an assessment of the Processor's compliance with the requirements laid down in this Agreement and any requirements otherwise following from data protection law in force in the UK at any time.

3.3.2. The statement may be provided at any point within each 36-month cycle so that the Controller is in receipt of the statement no later than the end of the 36th month commencing from the signing this Agreement, or the Controller's receipt of the previous statement.

3.3.3. The Processor's requirement to provide this statement will end upon the termination or expiry of the Client/Supplier Agreement or Contract between the Controller and the Processor, and the Processor having ceased all processing of Sensitive Personal Data on the Controller's behalf.

3.4. The Processor is obliged, on proof of identity, to give access to the Processor's physical facilities to the Controller and the authorities which under applicable law have access to the Controller's and the Processor's facilities or to representatives acting on behalf of such authorities.

4. Information security breach and data breach

4.1. The Processor shall inform the Controller immediately and in writing of any infringements of the obligations specified in the Contract and in this Data Processing Agreement. This shall also apply if there are substantive disruptions of the normal course of operations and if there are actual grounds to suspect data privacy infringements.

4.2. The Processor shall be obliged to provide the Controller with any and all information necessary for the compliance with the Controller's obligations pursuant to the Data Protection Act 1998 on the conditions for processing Personal Data and the General Data Protection Regulation.

4.3. The Processor shall without undue delay, but not later than 24 hours after the information security breach, report to the Controller.

4.3.1. In this connection, the Processor shall notify the Controller of the background of the security breach and the extent thereof as well as information about initiatives to safeguard against future security breach.

5. Correction, deletion and blocking / specific obligations to assist the Controller

5.1. Upon instruction by the Controller and pursuant to the relevant provisions of statutory law and regulations, the Processor shall facilitate the correction, deletion and blocking of Data processed on behalf of the Controller until these Data are ultimately deleted.

5.2. The Processor shall support the Controller in safeguarding the rights of the Data Subjects concerning correction, deletion or blocking of the Data by immediately making available any requested information and immediately implementing all instructions.

5.3. In case a Data Subject contacts the Processor directly, the Processor shall immediately notify the Controller.

5.3.1. The Processor shall promptly assist the Controller with the handling of any inquiry from a Data Subject, including request for access, correction, blocking or deletion if the relevant Data are processed by the Processor.

5.4. The Processor shall at the Controller's request assist the Controller in observing any obligations that may be incumbent on the Controller pursuant to the data protection law in force in the UK at any time where the Processor's assistance is assumed and where the Processor's assistance is necessary for the Controller's observance of its obligations.

5.4.1. In this context, the Processor shall assist the Controller in ensuring observance of the obligations under Articles 32-36 of the General Data Protection Regulation. The Processor's tasks in this respect shall be performed to the extent necessary and to this end at no cost to the Controller.

6. Agreement with other data processor (sub-contractor)

6.1. The Processor's right to enter into agreements with another data processor, e.g. a sub-contractor, regarding the processing of Data covered by the Data Processing Agreement, will be subject to the provisions of Appendix A. If the Processor in accordance with said Appendix A has the right to use a sub-contractor, the engaging of such sub-contractor shall take place in accordance with the provisions stipulated below.

6.1.1. The Processor shall draw up a written sub-contracting agreement with another data processor. In its agreement with another data processor, the Processor shall ensure that the other data processor as a minimum accepts the same data protection obligations as those undertaken by the Processor in this Data Processing Agreement as regards the sub-processing of the Controller's Data handled by the other data processor.

6.1.2. The Processor shall guarantee the lawfulness of another data processor's sub-processing of Data. If another data processor fails to fulfill its data protection obligations, the Processor shall remain fully liable towards the Controller for the fulfillment of such other data processor's obligations.

6.1.3. The fact that the Controller has consented to the Processor entering into an agreement with another data processor shall be of no consequence to the Processor's obligation to comply with the Data Processing Agreement.

6.1.4. When an agreement with another data processor regarding the sub-processing of Data comprised by the Data Processing Agreement terminates, the Processor shall notify the Controller thereof.

6.1.5. Any costs of the establishment of an agreement with another data processor, including costs in connection with the drawing up of sub-processing agreements, shall be borne by the Processor and shall be of no concern to the Controller.

7. Transfer of Data

7.1. The Processor may not transfer or authorise the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without prior consent from the Controller.

7.1.1. Consent from the Controller for the transfer of Data outside of the outside the EU and/or the European Economic Area (EEA) may take the form of a data transfer consent notice under the framework of Binding Corporate Rules, an intra-group agreement, or other similar formal agreement between the two parties to provide a general justification for cross-border data transfers.

7.2. In the event it is necessary to transmit Data internationally in the performance of the Contract, the Processor will ensure an adequate level of protection is in place to protect and safeguard Data.

8. Further obligations of the Processor

8.1. For the performance of the obligations in relation to this Data Processing Agreement, the Processor shall only appoint such employees who were informed about all relevant data privacy obligations and instructed to comply with data secrecy pursuant to the data protection law in the UK prior to performing their duties.
8.2. The employees shall be sufficiently trained in order to be able to comply with their data protection and contractual obligations.
8.3. The Processor shall ensure an adequate level of training by implementing suitable controls.

9. The Controller's rights of control

9.1. The Controller has the right to monitor the technical and organisational measures taken by the Processor at any time, including by on-the-spot-checks.
9.2. Upon request, the Processor shall provide the Controller with the necessary information as well as facilitate and permit any controls. The controls may also be conducted by a third party appointed by the Controller, if this is communicated in advance by the Controller.
9.3. The Processor shall also support the Controller in cases of inquiries and controls conducted by the ICO.
9.4. The Processor shall provide the Controller with documentation of the technical and organisational measures taken in compliance with the Contract and this Data Processing Agreement prior to the processing of the Data and on a regular basis.
9.4.1. Officially recognised certifications may serve as documentation.
9.5. The Controller's rights to carry out controls in regard to information security (if applicable) are detailed Appendix A and shall remain unaffected.

10. Return and deletion of the Data

10.1. Upon instruction by the Controller and pursuant to the relevant provisions of statutory law and regulations, the Processor shall facilitate the correction, deletion and blocking of Data processed on behalf of the Controller until these Data are ultimately deleted.
10.2. Upon termination of this Data Processing Agreement, the Processor shall regardless of the legal reasons of the termination transfer any and all Data (including in e-mails, from communication servers, clients or production computers as well as all intermediate files created in the course of the data processing and manual files) to the Controller.
10.3. After receiving a confirmation of the receipt of the Data, the Processor shall delete the Data permanently or destroy the manual files.
10.3.1. The deletion shall be confirmed in writing by the Controller. Upon written instructions from the Controller, the Processor shall carry out the deletion without prior transfer of the Data.

11. Duty of confidentiality

11.1. The Processor and the Processor's personnel shall observe unconditional confidentiality as regarding the processing of Data, and the Processor and the Processor's personnel are thus only entitled to process Data in the performance of the Contract, including this Data Processing Agreement.

11.2. The Processor warrants that the Processor's personnel and any other data processor and the personnel of such other sub-contractor who are authorised to process Data under this Data Processing Agreement will be subject to the duty of confidentiality set out in Appendix A as regards Data which may come to their knowledge in connection with the performance of the Contract.

12. Duration

12.1. The Data Processing Agreement shall enter into force upon signature thereof and shall remain in force for as long as the Processor processes on behalf of the Controller, or until the Contract expires/terminates.

12.2. Upon expiry or termination of the Data Processing Agreement, regardless of the legal reasons of the termination, the Processor shall provide the necessary services to the Controller in accordance with any information security requirements (if applicable) detailed in Appendix A.

13. Precedence

13.1. The Data Processing Agreement contains only the data protection rights of the Controller and the obligations of the Processor in accordance with EU and UK state law. In the event of any discrepancy between the terms of this Data Processing Agreement and any other agreement on data protection rights and responsibilities between the parties, whether in writing or oral, this Data Processing Agreement shall take precedence.

14. Flightline Travel Management's information stored and who we share it with…

Company and Traveller Personal Data

Company and Traveller Personal Data makes up the majority of our stored data. The traveller and company voluntarily complete a form agreeing for us to their data on supplier and internal systems. Part or all of this data may include, Company Name, Traveller Name, Address, Date of Birth, Passport Details, E-mail, Telephone Number, Supplier Loyalty Cards, Seating Preferences and Credit Cards. We transfer this data to Airlines, Hotels, and Rail companies via their own secure platform. Our Accounting system produces client Invoices and Our CRM database communicates E mails and Newsletters to our travellers and clients.

Employee Data

Stored includes Name, Date of Birth, Home Address, Telephone, NI number, E-mail. The employee supplies this data at the start of employment and is shared with our payroll accountants and tax office.

Bank details of suppliers and employees

Stored on our Nat West Bankline include Company or Individual name, Bank, Sort code and Account number. Suppliers and Employee supplied the data and is used to make payments.

Communicating Privacy Information - Data Protection:

Flightline Travel Management Ltd is registered under the UK Data Protection Act 1998. Registered with Information
you agree that your data will be retained by us for the purposes of:

- making a booking for you and providing you with confirmation of that booking (including a booking reference);
- providing and developing ancillary services and facilities;
- direct marketing by us or other third party agents, subject to your right to withdraw your authority at any time;
- facilitating immigration and entry procedures;
- accounting, billing and auditing;
- checking credit or other payment cards;
- security, administrative and legal purposes;
- systems testing, maintenance and development;
- statistical analysis;
- ensuring our compliance with legal and regulatory obligations applicable to us; and
- helping us in any future dealings with you.

Individuals' legal rights

Without prejudicing your rights to withdraw your consent and/or to alter your own data, purposes set out above you authorise us to retain for an indefinite period or until you request the deletion and use your personal data to transmit it to our own offices, authorised agents, government agencies, other carriers or the providers of the services mentioned above wherever they may be located. Should you be unsatisfied you have the right to complain to the "ICO" Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF. More information on www.ico.org.uk.

We may transmit your data to the third party providers of any additional services you decide to purchase. We may use your personal information to process your booking and to notify you about our new services and special offers we think you may find valuable. If you would prefer not to receive information regarding our services and special offers or to view or amend your individual personal data please contact us in writing or by Email to reservations@flightline-travel.co.uk allowing three working days to update and complete your request. Should the data exceed 30 individuals data requests we may take up to 14 working days to complete and maybe required to provide the data electronically and in a commonly used format.

Advanced Passenger Information

As a result of legislation introduced by the European Union, when you are travelling between certain countries in Europe and surrounding countries, we are required to provide Advanced Passenger Information (API) to certain destination airports in advance of your flight. The provision of this information by the Carrier to destination airports does not imply any acceptance or eligibility for you to enter any state or territory.

Access Request

No charge will be made for individual data requests addition/deletion or amendment. We may charge a fee or refuse any excessive data other than stated in "**Company and Traveller Personal Data".**

Legal Basis for Processing Data

The processing of data is necessary for us to be able to issue an airline ticket where the authorities and/or airlines require passport details to be entered into the booking process. In the event of disruption the E mail and Mobile phone number are also entered so the supplier can contact the individual should their arrangements alter.

Consent

The process of consent starts with the individual or company agreeing to voluntarily complete a profile form and e mail to our team for updating all our systems that require this information to be part of the booking process. Once completed the form is destroyed using our internal shredding machine.

Children under 13 years of age

In the rare event of receiving individual data for a person under thirteen years old we provide a letter of parental or guardian consent prior to accepting and processing.

Data Breach

We have in place a procedure if a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service occurs. We will complete a breach notification form and send to ICO within 24 hours of becoming aware of the essential facts of the breach. This notification must include at least: your name and contact details; the date and time of the breach (or an estimate); the date and time we detected it; basic information about the type of breach; and basic information about the personal data concerned.

Privacy Impact Assessment

Privacy by design is an approach we adopt to projects that promotes privacy and data protection compliance from the start of any new project whether building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications, embarking on a data sharing initiative; or using data for new purposes. Privacy Impact Assessments (PIAs) are an integral part of taking a "privacy by design" approach. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help design a more efficient and effective processes for handling personal data.

Data Protection Officer

The designated person to contact for any data protection assistance is Mr Jim McDaid jim@flightline-travel.co.uk or call +44 (0)1844 299750.

International Operations

Flightline Travel Management does not operate in other International countries only in United Kingdom.

15. Signatures

15.1. The Data Processing Agreement shall be signed in two original copies, of which the Parties shall each receive one.

Signed by **For and on behalf of the Processor (Client/Supplier)**	Name:	
	Job Title:	
	Signature:	
	Date:	
Signed by **For and on behalf of the Controller (Flightline Travel Management Ltd)**	Name:	
	Job Title:	
	Signature	
	Date:	

Appendix A

Purpose

This appendix serves to outline additional relevant data protection responsibilities of the Controller in key areas referenced in the Data Processing Agreement.

Sub-contracting

1. The Processor shall have the right to engage individuals or a company as a sub-contractor or a third-party to undertake support functions (i.e. administrative tasks) and works required in the performance of the Contract. The Processor however, must inform the Controller that it is using third parties for the sub-processing of Personal Data on behalf of the Controller, and identify them to the Controller upon request.

2. The Processor will be responsible for the cost of additional support and also ensuring that the individuals or companies that it uses understand and comply with the Processor's commitments and obligations to the Controller.

3. At the Controller's request, the Processor shall provide relevant information about sub-contractors or third parties, as a minimum including company name, contact details, name of the person appointed to represent the sub-contract or third party and a description of the tasks which the sub-contractor or third party is to perform under the Contract.

4. Notwithstanding the Processor's use of a specific sub-contractor or third party, The Controller is entitled to contact the Processor in any and all relative to the processing of Personal Data.

5. In addition, the Processor's use of sub-contractors or third parties shall not relieve the Processor of the duty to fulfil its other obligations under the Contract.

6. Sub-contractors or third parties involved in performing tasks concerning the processing or handling of Personal Data supplied by the Controller shall in particular observe the obligations laid down in the Data Processing Agreement.

Confidential Information

7. The Processor shall maintain in strict confidence all data, information and materials which have not yet been published or are otherwise not yet in the public domain and are regarded as confidential information belonging to the Controller.

    7.1. The Processor shall only use such information in connection with the Contract and/or the Order and for no other purpose whatsoever.

    7.2. The Processor shall ensure that its sub-contractors and employees are subject to the same obligations of confidentiality as the Processor under this clause.

    7.3. This shall equally apply to all information in relation to the business and affairs of the Controller, its directors, consultants and clients including financial information, products, client lists or other databases, marketing strategies, contractual terms and any other information which might reasonably be regarded as a 'trade secret' or capable of harming the business if disclosed to a competitor.

8. The Processor shall not, without the prior written consent of The Controller: (a) use The Controller's name, or any business or premises of the Controller for any purpose other than for properly fulfilling the Order; (b) advertise or publicly announce that it supplies items to the Controller; (c) photograph any part of the Controller's premises or anything situated thereon or any equipment, plant or materials used for (or to be incorporated as part of) any items; or (d) authorise or allow sub-contractors, Employees or any other person to do any of the foregoing.

Information security requirements

None applicable.