

Bookassist Data Processing and Security Terms

These Data Processing and Security Terms, including the Annexes, ("Terms") shall be effective and replace any previously agreed data processing and security terms as from the effective date. These terms supplement any contract ("Contract") in which Automatic Netware Ltd T/A Bookassist, 1st Floor South Block, Rockfield Central, Dublin D16 R6V0, Ireland, and its branches and subsidiaries ("Processor") agreed to provide the Client ("Controller") with services involving the processing of Personal Data. Together the Processor and the Client are referred to as "the Parties".

Effective date: 25 May 2018

§1 Definitions

"Client Customer Data" means the Personal Data in which the Client is the Controller.

"Controller" means the entity that determines the purposes and means of the Processing of Personal Data as defined in Article 4 GDPR.

"Corporate Group" means all parent companies, subsidiaries, branches and affiliates linked to the subject entity. Affiliate entities are limited to entities that hold direct or indirect ownership or control of more than 50% of the voting interests of the subject entity or where the subject entity holds such ownership or control of the affiliate.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"Data Protection Law" means all laws and binding regulations of the European Union (EU), the European Economic Area (EEA) and their member states, Switzerland and the United Kingdom, which are applicable to the Processing of Personal Data, including, but not limited to, the GDPR.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information that relates to an identified or identifiable natural person, to the extent that such information is protected as Personal Data under the GDPR.

"Processing" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity that processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the agreement pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-Processor" means the entities authorised under these Terms to process Personal Data in order for the Processor to carry out the Contract.

"Client Third Party" means any entity engaged by the Processor at the request of the Client, either via an addendum or direct communication, where the Client specifically requests the Processor to provide such entity with access to Personal Data.

§2 Terms, Purpose and Scope

- (1) The Terms set out herein are additional to and are duly incorporated into the Contract. Other terms, conditions, rights and obligations set forth in the Contract continue in full force and effect unless otherwise expressly varied herein. In case of any conflict with the Contract, these terms shall take precedence.
- (2) Any prior references within the Contract to data protection laws in force prior to 25 May 2018 shall hereinafter be construed as reference to the GDPR.
- (3) The purpose of these Terms is to detail the Parties' respective obligations with regards to Personal Data in compliance with the GDPR including, but not limited to, the use of and protection of Personal Data, associated with the processing of Personal Data by the Processor on behalf of the Client.
- (4) These Terms shall apply to any and all activities associated with the Contract, where the Processor's employees and or agents process Personal Data on behalf of the Client.
- (5) Whenever consent is required or a reference is made to written form or notification, electronic communication is sufficient.
- (6) The English version is the authoritative text of these Terms. For informational purposes only, these Terms may be provided in a language other than English.

§3 Duration and Specifications of Processing

- (1) The Processor shall process Personal Data in accordance with the specifications laid down in the Contract and for such a duration as specified in the Contract or, if unspecified, until the Contract comes to an end or is terminated. A breakdown of the Personal Data specifications (the type of Personal Data, the nature, purposes and subject matter of the data processing, the categories of data subjects and retention details) is provided in ANNEX 1.
- (2) Such instructions and specifications of processing may be altered, modified or added to by written instruction only.

§4 Basis on which Processor can process Personal Data

The Processor shall only process Personal Data on the basis of written instructions established with the Client, either via the Contract, Addendums, Supplemental Agreements, these Terms or via instructions to be established in the future, set forth in writing and agreed to by the Parties.

§5 Confidentiality

The Processor shall ensure that persons processing Personal Data are under a duty of confidentiality.

§6 Security

The Processor shall ensure that they have in place adequate controls, processes, and systems by which to ensure that the Personal Data is held securely at all times and ensure proper use, storage and maintenance of the Personal Data. A breakdown of such measures is provided in ANNEX 2. The Processor must inform the Client if there are any alterations to the measures laid down in ANNEX 2.

§7 Sub-Processor access to the Personal Data

- (1) The Processor utilises Sub-processors to carry out processing on behalf of the Client. A list of the existing Sub-processors is set out in ANNEX 3. The Client hereby provides consent to the use of the

Sub-processors listed in ANNEX 3. The Processor shall obtain the Client's consent to the replacement of any of these existing Sub-processors or the use of any new Sub-processors.

- (2) The Client shall be entitled to withhold consent only for material reasons related to the GDPR. Such consent will not be required if the transfer is necessary in accordance with the law; in such cases, the Processor shall inform the Client of that legal requirement before the transfer, unless that law prohibits such disclosure on important grounds of public interest.
- (3) The Processor shall impose the same data protection obligations set out herein on every Sub-processor with whom they disclose or transfer the Personal Data. The Processor must ensure that such Sub-processors have an appropriate level of data protection and information security.
- (4) Where Personal Data in the Processor's possession becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties, the Processor shall notify the Client where it involves Client Customer Data.

§8 Transfer of Personal Data outside of EEA

- (1) For the purposes of performing the Contract, the Client authorises the Processor to transfer Personal Data outside of the EEA to anywhere where the Bookassist Corporate Group, its Sub-processors as listed in Annex 3, or Client Third Parties are located.
- (2) Bookassist shall ensure that any transfers occurring under §8(1) shall be either (i) to a country that has been formally recognised by the European Commission as providing an adequate level of data protection safeguards or (ii) the transfer is otherwise safeguarded by mechanisms, such as Standard Contractual Clauses or the EU-US Privacy Shield.
- (3) For situations not covered by §8(1), Bookassist shall seek the consent of the Client before transferring Personal Data outside of the EEA. No consent will be required if the transfer is necessary in accordance with the law; in such cases, the Processor shall inform the controller of that legal requirement before the transfer, unless that law prohibits such disclosure on important grounds of public interest.

§9 Retention

The Processor shall delete the Client Customer Data in accordance with the retention periods set out in Annex 1. The Processor shall delete all existing copies of such Personal Data unless EU or national law requires storage of the Personal Data.

§10 Assistance with GDPR obligations and Compliance

- (1) The Processor shall support the Client insofar as is possible, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Article 33 to 36 GDPR.
- (2) The Processor confirms that they shall immediately inform the Client if, in the Processor's opinion, an instruction from the Client infringes data protection law.
- (3) The Processor confirms that they shall immediately inform the Client of any suspected infringement of data protection law or of any other irregularities arising from activities carried out by the Client or any Client Third Party.
- (4) Upon request from the Client, the Processor will make information available that is necessary to demonstrate compliance with the obligations laid down in the GDPR. In this regard, the Processor shall allow for and contribute to audits, including inspections, conducted by the Client and or another auditor appointed by the Client at the Client's cost and expense. Such audits and inspections will be conducted during regular business hours, and without interfering with the Processor's operations and upon one month prior notice. The Processor's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

- (5) The Client shall notify the Processor without undue delay of any defect or irregularity found with the Processor's work regarding compliance with data protection law.
- (6) The Processor shall immediately investigate and rectify any data breach, non-compliance with data protection law or other irregularity of which the Processor was notified or was aware of.
- (7) The Processor reserves the right to immediately stop data processing and cease transferring the Personal Data at any time and without penalty should the Processor become aware of any data protection issues which could impact on the business and or reputation of the Processor.

§11 Enquiries by data subjects

Where a data subject requests the Processor to rectify, erase or access their Personal Data, and where the Processor is able to correlate the data subject to the Client, based on the information provided by the data subject, the Processor shall forward the data subject's request to the Client without undue delay. It shall be the obligation of the Client to respond to the data subject. The Processor shall support the Client, where possible, with the data subject's request. The Processor shall not be liable in cases where the Client fails to respond to the data subject's request in total, correctly, or in a timely manner.

§12 Control and Client Responsibilities

- (1) The Client acknowledges and agrees that it shall at all times be the Controller and remain in control of all Personal Data.
- (2) As the Controller, the Client shall be responsible for compliance with data protection law, including, but not limited to, the lawfulness of contracting the Processor to process Personal Data on behalf of the Client and the lawfulness of requesting the Processor to use a Client Third Party.
- (3) It is the Client's responsibility to determine whether a data processing agreement or similar is required with any Client Third Party in accordance with Article 28 GDPR. The Client acknowledges that any Client Third Party is not a Sub-Processor of the Processor.

§13 General

- (1) The Client and the Processor shall be liable to the data subject in accordance with Article 82 GDPR and be subject to such indemnities as set out in Article 82 GDPR.
- (2) If any dispute arises in relation to the subject matter of these Terms, in particular the attribution of liability arising out of §13(1), such dispute shall be resolved in accordance with the dispute resolution clauses within the Contract.
- (3) If any provision of these Terms should be or become invalid, the validity of the remaining provisions shall not in any way be affected or impaired. Invalid provisions shall be replaced by valid provisions formulated in such a way that the intended purpose will largely be achieved.
- (4) Any costs arising out of these Terms that cause an unreasonable burden on the Processor shall be notified to the Client and an agreement shall be made as to any reimbursement owed to the Processor.
- (5) If the Processor makes any changes to these Terms, the Client shall be notified and will be given an opportunity to object.

ANNEX 1

Data Specifications

Type of Data	Nature, Purpose and subject matter of data processing	Categories of Data Subjects	Retention
Client Customer's reservation details	<p>This data processing is for Bookassist's booking engine, to fulfil the reservation process as requested by the Client.</p> <p>Customer's Personal Data obtained during the reservation process includes customer's name and contact details, credit card details, reservation details including booking reference.</p>	<p>Client Customer Personal Data.</p> <p>It's possible that sensitive data may be specified by the customer during reservation completion in the "Special Requests" box.</p>	<p>Personal data is anonymised 12 months after departure date.</p> <p>Credit card data is deleted no later than 1 month after reservation departure date.</p> <p>The booking reference is retained indefinitely for statistical purposes.</p>
Client Customer's voucher purchase details	<p>This data processing is for Bookassist's Voucher Purchase facility as requested by the Client.</p> <p>Voucher Purchase details contain the purchaser's name and contact details and credit card details, voucher recipient's name and may contain the recipient's contact details.</p>	<p>Client Customer Personal Data.</p> <p>It's possible but unlikely that sensitive data may be specified by the purchaser in the "Message" box.</p>	<p>Personal data is anonymised 12 months after voucher expiry date.</p>
User login data	<p>This data processing is for management of logins to Bookassist's Extranets – the Bookassist Hotel Administration and the Bookassist Content Management System (CMS).</p> <p>Includes name, username, password, email address, phone, log records of all accesses and activities.</p>	<p>Client Employee (or other person authorised by Client) Personal Data.</p>	<p>User login data is retained for 14 months after expiry date.</p>
Client Customer data obtained via Client's website	<p>This data processing is for the provision and hosting of webpages, forms or pop-ups, such as Newsletter subscription or any other webpage that provides for the website visitor to enter their contact details, on the Client's web-site – this is only relevant for Clients using Bookassist's Web Design service to host and maintain their website.</p> <p>Includes name and email address, may include other fields requested by the Client.</p>	<p>Client Customer Personal Data.</p>	<p>Data obtained via this form/page is sent to the Client via email. The data is not stored in Bookassist.</p>

ANNEX 2

Security Measures

1. Data centre location

Personal data is stored and processed at Bookassist servers in trusted data centres located in Dublin and London under our hosting partners control AWS (Amazon Web services) and Rackspace ("Hosting Partners"):

AWS

<https://aws.amazon.com/compliance/programs/>
<https://aws.amazon.com/compliance/data-center/controls/>

Rackspace

<https://www.rackspace.com/compliance>

2. Physical data centre security

Our Hosting Partners are qualified with high security standards like ISO/IEC 27001 and PCI DSS, providing the required data centre access procedures to avoid any unauthorised physical access to Bookassist servers.

3. Network Security

The network is segmented in different layers of security, keeping the private network and internal network only accessible to Bookassist and our Hosting Partners personnel.

Firewalls monitor and keep control of any access to Bookassist network based on the defined security rules.

IDS (Intrusion Detection System) monitors and prevents any suspicious and unauthorised network traffic.

4. Data Transmission Security

Bookassist uses strong cryptography protocols such as TLS/HTTP for Personal Data transmission across open public networks, keeping the communications secure.

5. Remote and application access

Remote access to Bookassist servers and applications are under strong access control measures preventing any unauthorised access to Personal Data.

6. Server OS security

Bookassist has strong procedures implemented for monitoring, scanning and patching the servers in order to keep the servers updated.

Bookassist actively monitors the server and logs metrics to guarantee security and the correct performance of the servers and applications.

7. Data storage and backups

Personal Data is stored under database servers located on segregated networks under strong control access.

Bookassist has backup policies that ensure a data recovery in case of failure or disaster. As such, Bookassist retains copies in different secured locations provided by our Hosting Partners.

8. Credit card information

Bookassist follows the PCI DSS standard.

ANNEX 3

Approved Third Parties utilized by the Processor

Company Name	Country	Address	Purpose
Amazon Web Services AWS	Ireland and USA	Burlington Road, Dublin 4, Ireland; and 410 Terry Ave North, Seattle , WA 98109-5210 , USA.	Server hosting
Rackspace	UK	Hyde Park Hayes, 5 Millington Rd, Hayes UB3 4AZ, UK	Server hosting
Google Analytics	Ireland	Google Ireland, Barrow Street, Dublin 4.	Web-site traffic and conversion reporting
Figaro	Italy	Via del Santuario, 95028 Valverde (CT), Italy	Channel manager software
Clickatell	UK	Bank House, 81 St Judes Road Englefield Green , Surrey TW20 0DF, UK	SMS text messaging
Atlassian (Jira)	USA	San Francisco, California, USA	Ticketing and knowledge base
Socketlabs	USA	22 Essex Way #8203, Essex, VT 05451 USA	Email gateway
Realex Payments (Global Payments)	Ireland	Sir John Rogerson's Quay, Dublin 2, Ireland	Payment solutions
Google G Suite	Ireland	Google Ireland, Barrow Street, Dublin 4.	Email, communication and document management
Solve	Canada	Norada Corporation, Calgary, Alberta, Canada	Client Relationship Management system
Mailchimp	USA	675 Ponce de Leon Ave NE, Atlanta, Georgia, USA	Email marketing
Questback	Norway	Bogstadveien 54, 0366 Oslo, Norway	Online survey and feedback software
Dropbox	Ireland	Dropbox International Unlimited, Upper Hatch St., Dublin 2	Data storage
Backupify (Datto)	USA	101 Merritt 7, Norwalk, CT 06851, United States	Data backup
Docsend	USA	351 California St, San Francisco, CA 94104, USA	Publication platform