Data Processing Agreement

Version 1
Last modified: 23 th May, 2018

Contents

1. Introduction

A. In this Data Processing Agreement ("**Agreement**") "**Clock**" means Clock Software Ltd. registered in England, with a registered office at 27 Redcliffe Gardens, London, SW109BH, United Kingdom and with company number 08008667; Klok OOD registered in Bulgaria, with a registered office at 20 Strandzha Street, 9000 Varna, Bulgaria, with company number 103135417, and any affiliated company of theirs. The main operating company is Klok OOD, which data processing activity is regulated by the legislation of the European Union and Bulgaria.

B. Clock is developing and owing various software products hosted and operated on hardware under its control; and provides various software services to Clock's customers via Internet. In particular Clock has developed its hotel reservation system and is using it to provide services to hospitality industry (hotels, other accommodation premises, restaurants etc) as well as to payment processing companies and other business entities. In Clock's General Terms and further in this Agreement Clock's customers are named "**End Users**".

C. Clock is and has always been committed to keeping confidential and to protecting the security of any information about End Users and End Users' Customers. Clock is especially focused on protecting the Personal Data of the individuals who contact Clock or End Users via the Services (as defined below). To that end Clock has developed its privacy policy and is doing its best to maintain and update the said policy in accordance with the applicable legislation and the leading practices in the software industry.

D. Clock provides the Services to End User under the terms of an agreement made either by signing a particular agreement, or by accepting Clock's General Terms (as defined below) or using the Services by End User ("**Main Agreement**"). Such Main Agreement is also named "Subscription" in the General Terms. By entering into Main Agreement End User acceps this Agreement and vice versa. By using the Services or by browsing Clock's Websites End User accepts this Agreement.

2. Definitions

In this Agreement:

(a) "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**" and any other terms defined in Article 4 of the Regulation (ES) 2016/679 have the same meaning as in the said Regulation.

(b) "**End User**", "**Services**", "**Software**" and any terms defined in the General Terms have the same meaning as in the General Terms.

(c) "**Customer**" means any individual who is either End User's customer or employee or subcontractor or other servants or other person who collaborates and communicates with End User and transmits data via the Services.

(d) "**Subprocessor**" means any third party authorized by Clock to have logical access to and process Customer Personal Data in order to provide parts of the Services or technical support to Clock.

(e) "**General Terms**" means Clock's General Terms and Conditions for End-Users of Clock PMS – Labeled Software available at the Website.

(f) "**Website**" is Clock's web site at the address www.clock-software.com.

3. Data Controller

3.1 Controller is the respective End User - business entity which uses the Services for carrying out its commercial activities (for hotel reservations, payment processing etc.) on the ground of Main Agreement.

3.2 Any and all Customer Personal Data shall be processed via the Services for the sole purpose of End User's business. End User sets all terms and conditions for processing Customer Personal Data (particular categories of data, purpose of processing, duration of storage etc.).

3.3 All Customer Personal Data processed via Services shall be property of End User.

4. Data Processor

4.1 Clock is a Processor for and on behalf of End User.

4.2 Clock shall process Customer Personal Data submitted, stored, sent or received by End User via the Services solely for provision of the Services to End User in accordance with the Main Agreement.

5. Data Subject

Customer is a Data Subject.

6. Scope of Data Processing

6.1 Categories of Data
Customer Personal Data submitted, stored, sent or received by End User or Customer via the Services may include the following categories of data: names, ID number, address, age, email, telephone, documents, credit card details, presentations, images, calendar entries, tasks and other data.

6.2 Duration of the Processing
Clock shall process Customer Personal Data for the entire duration of the Main Agreement plus the subsequent period of 12 months, unless otherwise agreed between Clock and End User or required by the applicable legislation. This Agreement shall remain valid until the deletion of all Customer Personal Data.

7. Non-Disclosure Commitment

7.1 Clock, without End-User's prior explicit approval in writing, shall not:

(a) disclose a copy of Customers Personal Data to any third party;

(b) use Customers Personal Data for any purposes different from providing Services to End User;

unless such disclosure or use is required by a competent authority in accordance with the applicable legislation.

7.2 Without prejudice to the above Clause 7.1 Clock's shall be entitled to disclose Customer Personal Data to Subprocessors, consultants and other service providers. The disclosed Customer Personal Data shall be subject to the respective recipients of data protection policy.

8. Security Measures

Clock shall implement and maintain security measures to protect Customer Personal Data against unauthorized disclosure or access, accidental or unlawful destruction, loss, alteration. Clock will be continuously monitoring the functionality and the adequacy of the security measures and may from time to time modify and update the security measures.

8.1 Data centres

8.1.1 Clock maintains all Customer Personal Data and processing on servers hosted at data centres of Amazon Web Services (AWS). AWS demonstrate compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5). AWS continues to pursue the certifications. AWS's Terms of Use, Privacy Policy and AWS Customer Agreement are available at AWS's web site: https://aws.amazon.com/.

8.1.2 All Customer Personal Data based in the European Union are processed and stored on servers in the European Union.

8.1.3 For the purpose of this Agreement the servers used by Clock shall be referred to as Clock's servers.

8.1.4 Clock monitors Clock's servers to ensure that there is no unauthorised access to any data stored thereon. Clock implements various methods and technologies for prevention and detection of any intrusion or intrusion attempt.

8.2 Clock’s staff control

8.2.1 Clock has implemented and maintains a data security policy for its staff and provides security training as part of the training package for its staff. Clock’s employees and partners are required to conduct themselves in a manner consistent with Clock’s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

8.2.2 Only authorised staff will have access to Customer Personal Data only in relation with the execution of their direct duties on operating and supporting the Services. Each member of the staff has signed special data security addendums to their agreements and undergoes periodic instructions and trainings about data security. Clock’s staff will not process Personal Data without authorization.

8.2.3 Clock’s security staff is responsible for the ongoing monitoring of Clock’s security infrastructure, the review of the Software and Services, and responding to security incidents.

8.3 On-site control

Clock controls and restricts the access to its premises, hardware and documentation. Clock’s premises require electronic cod key access and are monitored by TV cameras. Only authorized employees and contractors have access to these premises. Entrants are required to identify themselves.

8.4 Encryption

8.4.1 All data records in the databases are protected with credentials and all data transmission between End User’s and Customer’s hardware and Clock’s servers is encrypted, so that it is only readable through the graphical user interface (“GUI”) or the application programming interface (“API”) and only after a successful submission of valid credentials - eg. username, password, PIN, multi-factor authentication, API secret key, etc. Open public features may not require customers to submit credentials in order to visualise data intended for public visualisation.

8.4.2 Clock is applying data encryption that meets the highest requirements for encryption and encrypting keys. The new class of encryption complies with the strict and practice-oriented requirements of PCI DSS.

8.5 Credit card data security
Credit card data storing and retention is a subject of specific regulations like PCI or End User’s agreement with respective payment processor or acquirer. End User shall collect, process, access and destroy credit card data according to all applicable standards, agreements, guidelines and regulations. End User shall follow Clock’s PCI DSS guidance (available at the Website) and meet its obligations stipulated there.

8.6 End User control
Clock shall assist End User in ensuring compliance with End User’s obligations as to Personal Data protection. In order to assist End User Clock shall implement and maintain application features which shall included as but shall not limited to those listed below.

8.6.1 Levels of access. Clock has redesigned the Software to enable End User precisely determine the level of access of its employees to Customer Personal Data. Fore example, the staff having the lowest level of access shall be able to work with anonymized (masked) Customer Personal Data only. Generally the levels of access shall be:

(a) Prohibited access. Employees will only see [********] instead of Personal Data.

(b) Basic access. Employees will partially see Customer's details in order to process Customer's booking of End User's services (hotel booking, card payment etc.) but will not be able to identify the Customer.

(c) Operational access. Employees will be able to view full Personal Data of each Customer on the booking, profile and other screens.

(d) Full access. Employees will be able to view, export and copy full Personal Data of each Customer.

8.6.2 Access Control. End User and End User's administrators are required to authenticate themselves via an authentication system in order to use the Services. Software checks credentials in order to allow the display of data to an authorized End User or authorized End User's administrator.

8.6.3 Anonymisation. Partially masking or restricting the visible information of each Customer on the screens and in the reports to the minimum. The Customer Personal Details are hidden in the below manner and are only accessible when having additional access rights:

- A first name initial and surname [J Smith].
- The first 4 letters of the email address [jsmi********])
- The last 4 digits of the telephone number [********1234]

8.6.4 Consent to marketing emails or giving information to third parties. In the creation of a booking, a field and related consent text will be displayed in the WRS customer self-service portal, customer profiles and any other point where personal data is collected for the first time in relation with the particular booking to ask for the Customers' permission to send them marketing emails and/or provide their data to third parties. In the Guest Mailer, Clock has also added an option to filter Customers who have not agreed to receive marketing emails.

9. Data Deletion

9.1 Unless otherwise explicitly agreed in writing between Clock and End User, Clock shall delete all Customer Personal Data from its systems not later than 3 months of expiry of the Main Agreement.

9.2 Clock shall enable End User to delete Customer Personal Data prior to expiry of the Main Agreement. End User shall be able to search for and erase Customer Personal Data from bookings and profiles without deleting the bookings. Furthermore End User shall have the option to forbid automatic deletion for certain profiles (e.g. participants in End User's client loyalty programmes).

9.3 Upon End User's explicit request in writing Clock shall delete Customer Personal Data from Clock's systems prior to expiry of the Main Agreement, not later that 3 months of receipt of the request.

9.4 Without prejudice to the above Clauses Clock may store Customers' Personal Data if such a storage is required by the applicable legislation.

10. Data Incidents

10.1 If Clock becomes aware of a data incident, Clock shall notify End User promptly and without unreasoned delay; and shall promptly take reasonable steps to minimize harm and secure Customer Personal Data.

10.2 End User shall be solely responsible for complying with applicable incident notification legislation and fulfilling its notification obligations related to data incidents (incl. notification of the persons concerned the data incident) .

10.3 Clock’s notification of or response to a data incident shall not be construed as an acknowledgement of any fault or liability with respect to the data incident.

11. End User’s Responsibilities

11.1 Clock’s commitments under this Agreement shall not release End User from its obligations as Controller. End User undertakes to develop, implement, control update its internal data protection and privacy policies.

11.2 End User undertakes to comply with any requirements of the applicable legislation as well as to follow Clock’s instructions related to data protection. End user shall continuously take all reasonable security action, such as but not limited to implementing virus protection software, network security policies or periodic update of passwords, to improve the general system security of your hardware and networks which are in a direct relation with the data protection.

11.3 Customer is solely responsible for its use of the Services, including:

(a) setting the character of Customer Personal Data to be processed;

(b) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;

(c) securing the account authentication credentials, systems and devices End User uses to access the Services; and

(d) backing up its Customer Personal Data;

(e) securing Customer Personal Data that End User elects to transfer or store End outside of Clock’s Systems.

(f) evaluating for itself whether the Services, including Cock’s security measures and control meets End User’s needs and obligations as a Controller.

11.4 Clock has no obligation to protect Customer Personal Data that End User elects to store or transfer outside of Clock’s systems (for example, offline or on-premise storage).

11.5 End User accepts and agrees that Clock provides a level of security appropriate to the risk in respect of the Customer Personal Data and meets all requirements of the data protection legislation of the country where End User’s business is based. If the said legislation requires from Clock any registration, permission or licensing End User shall promptly notify Clock and Clock shall be entitled to terminate Main Agreement at its sole discretion without any liability for Clock. Failing to notify, End User shall indemnify Clock against any penalties imposed or damages incurred in relation with any inconformity with the said legislation.

11.6 End User accepts and agrees that despite Clock’s reasonable efforts data incidents are possible (fore expample, as a result of technical malfunction, programming error, or hacker attack etc.) End User shall implement all reasonable efforts to protect itself against consequences of such data incidents, which measures shall include but shall not be limited to:

(a) downloading periodically the CSV report exports, available in the Software;

(b) taking appropriate measures to minimise the impact of data incident to Customers and any third parties.

12. End User’s Audit

12.1 Clock will allow End User or independent auditor mandated by End User to conduct audits (including inspections) to verify Clock’s compliance with its obligations under this Agreement.
Following receipt of End User’s request for audit Clock and End User will agree upon the terms and conditions of the audit. In no circumstances the audit shall prejudice Clock’s ordinary course of business and/or shall require disclosure of Clock’s trade secrets or any other confidential information. Audits shall be conducted at the expense of End User and Clock may charge a reasonable fee advised in advance to End User.

12.2 Clock may object in writing to an auditor mandated by End User if the auditor is, in Clock’s reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection will require End User to appoint another auditor or conduct the audit itself.

13. Customer’s Requests

If Clock receives any request from a Customer in relation to Customer Personal Data, Clock will advise the Customer to submit his/her request to End User. End User shall be solely responsible for responding to any such request including, where necessary, by using the Services. As far as it is possible and practical Clock will assist End User in fulfilling any obligation to respond Customer’s requests.

14. Subprocessors

14.1 End User specifically authorizes Clock to engage any Subprocessors. Clock shall make information about Subprocessors, including their functions and locations, available at its Website.

14.2. Clock will ensure that any Subprocessor has an access and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it.

14.3 If End User disagrees with appointment of a Subrocessor End User may terminate main Agreement by a 3- months notice in writing, with no liability for Clock.

15. Liability

Liability clauses of main Agreement shall apply to Clock’s liability under this Agreement.

16. Delivery of Notification

Notifications under this Agreement shall be delivered to the announced postal address notification email address of the recipient party. Recipient party is solely responsible for ensuring that is notification address/email address is current and valid.

For and on behalf of the end-user

Company name as per the subscription: ……………………………………………………………………

Authorized representative: ……………………………………………………………………………….

Position: ……………………………………………………………………………………………………….

Date: ………………………………………………………………………………………………………...

Signature: ………………………………………………………………………………………………...