Version December 2019

DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT ("**AGREEMENT**") IS A LEGAL AGREEMENT WHICH FORMS AN INTEGRAL PART OF AND APPLIES IN ADDITION TO THE EXISTING LIGHTSPEED SERVICE AGREEMENT ("**SERVICE AGREEMENT**") CONCLUDED BY AND BETWEEN THE CUSTOMER AND LIGHTSPEED (BOTH AS DEFINED IN THE SERVICE AGREEMENT) IN CONNECTION WITH THE PROVISION OF SERVICES WHICH INCLUDES VARIOUS DATA PROCESSING SERVICES TO CUSTOMER ("**SERVICES**").

(1) LIGHTSPEED MAY, AT ANY TIME, AND AT LIGHTSPEED'S SOLE DISCRETION, MAKE IMMATERIAL CHANGES TO THIS AGREEMENT. LIGHTSPEED WILL INFORM CUSTOMER OF SUCH CHANGES.

(2) Terms used in this Agreement have the same meaning as those used in the Service Agreement, unless explicitly provided otherwise. If there are any conflicts or inconsistencies between the Service Agreement and this Agreement, this Agreement prevails.

(3) When carrying out the Services, Lightspeed may be provided access to or otherwise obtain or handle information relating to identified or identifiable individuals ("**Personal Data**"). The engaged processors, subject-matter, duration, nature and purposes of the processing, as well as the type of Personal Data and categories of individuals whose data are processed are set forth in Annex 1, which forms an integral part of the Agreement.

(4) Lightspeed may only process Personal Data on behalf of Customer and solely for the purposes identified in this Agreement.

(5) Lightspeed may engage the processors stipulated in Annex 1 and any other processors to process Personal Data on Customer's behalf. Lightspeed shall inform Customer of any intended changes concerning the addition or replacement of (sub-) processors that process Personal Data of Customer and give Customer the opportunity to object to such changes.

(6) Lightspeed shall ensure that any processing shall be fair, lawful, and consistent with Lightspeed's obligations under this Agreement and compliant with applicable data protection law. In particular, Lightspeed shall ensure that any person engaged in providing the Services on its behalf, shall:

a. process Personal Data only on the documented instructions of Customer; If Lightspeed is required to process Personal Data in compliance with a law of the European Union or a Member State to which Lightspeed is subject, it will inform Customer of such legal requirement prior to such processing, unless a law of the European Union or a Member State to which Lightspeed is subject prohibits it from doing so;

b. ensure appropriate protection of Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves a transmission of Personal Data over a network, and against all other unlawful forms of processing;

c. comply with the security requirements set forth in Annex 2, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of processing;

d. assist the Customer in ensuring compliance with the obligations regarding security measures and conducting data protection impact assessments, where necessary pursuant to Articles 32-36 of of the General Data Protection Regulation, 2016/679;

e. not disclose Personal Data to any third party or unauthorized persons, unless Customer has given its prior written consent to such disclosure and subject to the conditions laid down under section 6 of this Agreement;

f. hold Personal Data in strict confidentiality and require employees and any other person under its authority who will be provided access to or will otherwise process Personal Data are held to the same level of confidentiality in accordance with the requirements of the Agreement (including during the term of their employment or engagement and thereafter);

g. promptly notify Customer if it receives a request from an individual with respect to Personal Data, including but not limited to information access requests, information rectification requests, requests for blocking, erasure, or portability of Personal Data and shall not respond to any such requests unless expressly authorized to do so by Customer or unless required under a law of the European Union or a Member State to which Lightspeed is subject; Additionally, Lightspeed shall ensure that it has implemented technical and organizational measures to assist Customer in fulfilling its obligation to respond to any such requests from an individual with respect to Personal Data processed;

h. promptly notify Customer if in Lightspeed's view an instruction given by Customer infringes applicable laws and regulations, including data protection laws, or a change in the applicable laws and regulations is likely to have a substantially adverse effect on its ability to comply with its obligations under this Agreement;

i. promptly (and in any event within thirty-six (36) hours) after becoming aware, notify Customer of any facts known to Lightspeed concerning any actual or suspected accidental or unauthorized access, disclosure or use, or accidental or unauthorized loss, damage or destruction of Personal Data by any current or former employee, contractor or agent of Lightspeed or by any other person or third party;

j. cooperate fully with Customer in the event of any accidental or unauthorized access, disclosure or use, or accidental or unauthorized loss, damage or destruction of Personal Data by any current or former employee, contractor or agent of Lightspeed or by any other person or third party, to limit the unauthorized disclosure or use, seek the return of any Personal Data, and assist in providing notice to competent regulators and affected individuals if requested by Customer;

k. promptly and properly deal with enquiries and requests from Customer in relation to the processing of Personal Data under this Agreement and provide other reasonable assistance and support;

l. assist and support Customer in the event of an investigation by a data protection regulator or similar authority, if and to the extent that such investigation relates to the processing of Personal Data under this Agreement;

(7) Upon termination or expiration of the Services for whatever reason, or upon request by Customer, Lightspeed shall immediately cease to process Personal Data and shall promptly return to Customer all such Personal Data, or delete the same, in accordance with such instructions as may be given by Customer at that time, unless it is required to store the Personal Data under a law of the European Union or a Member State to which Lightspeed is subject or unless explicitly agreed otherwise with Customer. The obligations set out in this section shall remain in force notwithstanding termination or expiration of this Agreement.

(8) Lightspeed shall ensure that any employee, agent, independent contractor, or any other person engaging in the provision of the Services and who has access to Personal Data of Customer, shall comply with all information protection and privacy laws and regulations (including any and all legislative and/or regulatory amendments or successors thereto), applicable to Lightspeed.

(9) Lightspeed may only subcontract (part of the) Services to third parties (including Lightspeed's establishments outside the EEA) if Lightspeed ensures that such third parties are bound in writing to the same obligations and Customer is awarded the same rights contained in this Agreement with regard to such third parties.

(10) In the event that (i) Lightspeed is unable to comply with the material obligations stated in this Agreement, where any obligation required by law (including, but not limited to, Article 28 of the General Data Protection Regulation, No. 2016/679) is considered material, or (ii) Lightspeed becomes aware

of any circumstance or change in applicable data protection law that is likely to have a substantial adverse effect on Lightspeed's ability to meet its obligations under the Agreement, Lightspeed shall promptly notify Customer to this effect, and Customer shall then be entitled, at its option, to (i) suspend all transfers of Personal Data until such time that the non-compliance is remedied, (ii) require Lightspeed to cease processing relevant Personal Data until such time that the non-compliance is remedied, and/or (iii) immediately terminate this Agreement.

(11) Lightspeed will make available to the Customer all information necessary to demonstrate compliance with the obligations regarding the processing of Personal Data provided to Lightspeed as a data processor.

(12) Audit and Compliance.

a. Lightspeed shall make the processing systems, facilities and supporting documentation relevant to the processing of Personal Data available for an audit by Customer or a qualified independent assessor selected by Customer and provide all assistance Customer may reasonably require for the audit. If the audit demonstrates that Lightspeed has breached any obligation under the Agreement, Lightspeed shall immediately cure that breach;

b. In case of inspection or audits by a competent governmental authority relating to the processing of personal data, Lightspeed shall make available its relevant processing systems, facilities and supporting documentation to the relevant competent public authority for an inspection or audit if this is necessary to comply with applicable laws. In the event of any inspection or audit, each party shall provide all reasonable assistance to the other party in responding to that inspection or audit. If a competent public authority deems the processing of Personal Data under this Agreement unlawful, the parties shall take immediate action to ensure future compliance with applicable data protection law;

c. Lightspeed shall promptly inform Customer if: (i) it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the processing of Personal Data under this Agreement, except where Lightspeed is otherwise prohibited by law from making such disclosure; or (ii) it intends to disclose Personal Data to any competent public authority.

Annex 1: Description of Lightspeed's processing activities

Details of the processing

Lightspeed is a provider of software as a service for point of sale solutions for the retail and hospitality industry as well as the provider of an online platform that can be used for eCommerce purposes. Lightspeed shall process Personal Data on behalf of the Customer to provide these services to the Customer pursuant to the Service Agreement and any additional purposes as instructed by Customer when using the Services.

Type of personal data

Depending on how the Customer chooses to use the Services, Lightspeed may process the following types of personal data:

- First name, Last name
- Contact information (e-mail address, home address, phone number)
- Language
- Gender
- Date of Birth
- IP Address
- Geographical data
- Social security number
- Bank account details

Duration (retention terms)

Each type of personal data will be deleted upon receipt of an instruction thereto from the Customer

Categories of individuals whose data are processed

- Persons who are using the Customer's services.
- Employees and other persons authorized by the Customer who have access to and use the Services.

(Sub-)processors

Customer hereby gives Lightspeed permission to engage the following (sub-) processors on Lightspeed's behalf:

Type of Services	Name (sub-) processor	Description of processing	Country of establishment
All Services	Zendesk, Inc.	Storing of personal data received from the Customer to perform Customer support services	United States

All Services	Snowflake Computing, Inc.	Analysis of non-personal data for statistical purposes.	United States
All Services	Elasticsearch B.V.	Storing of logs and performing search queries on product database.	Netherlands
eCommerce (EU Customers)	KPN Internedservices B.V.	Storing of personal data in Data Center	Netherlands
Hospitality Retail eCommerce (non-EU Customers)	Amazon Web Services, Inc.	Storing of personal data on cloud servers	United States
iKentoo / K-Series	Amazon Web Services Inc.	Storing of personal data on cloud servers	Ireland & Germany
eCommerce	Hotjar Limited	Perform behavioral analysis of our customer when using our services.	Malta
eCommerce Hospitality	Mixpanel, Inc.	Perform behavioral analysis of our customer when using our services.	United States

Annex 2: Description of Lightspeed's Security Measures

Lightspeed has taken appropriate and sufficient technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves a transmission of Personal Data over a network, and against all other unlawful forms of processing.

The following description provides an overview of the technical and organizational security measures implemented. Such measures shall include, but are not limited to :

Data Protection

Lightspeed will process the Personal Data as a Data processor, only for the purpose of providing the Services in accordance with documented instruction from the Customer (provided that such instructions are commensurate with the functionalities of the Services), and as may be agreed to with you.

Lightspeed implements and maintains appropriate technical and organizational measures to protect the Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure.

Lightspeed ensures that its personnel who access the Personal Data are subject to confidentiality obligations that restrict their ability to disclose the Personal Data.

In-transit: Lightspeed makes HTTPS encryption available on every one of its login interfaces and on every customer site hosted on the Lightspeed products. Lightspeed's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Lightspeed stores user passwords following industry standard practices for security.

Access control

1. Preventing Unauthorized Product Access

Outsourced processing: Lightspeed hosts its services on third party Hosting infrastructure in form of data centers and Infrastructure-as-a-Service (IaaS). Additionally, Lightspeed maintains contractual relationships with vendors in order to provide the service in accordance with our Data Processing Agreement. Lightspeed relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Lightspeed hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II, ISO 27001 and PCI DSS compliance, among other certifications.

Authentication: Lightspeed implemented a uniform password policy for its customer products. All users who needs to interact with the products via any interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Lightspeed's product is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

2. Preventing Unauthorized Product Use

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented

differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Lightspeed implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available services.

Vulnerability scanning: Lightspeed regularly scans its infrastructure and web services for known vulnerabilities and remediate on them in a timely manner.

3. Limitations of Privilege & Authorization Requirements

Product access: A subset of Lightspeed's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employees are granted access by role. Log-ins to data storage or processing systems are logged.

Database access: Customer data is accessible and manageable only by properly authorized staff. Direct database query access is restricted, and application access rights are established and enforced.

Incident Management Control

Detection: Lightspeed designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Lightspeed personnel, including security, operations, and support personnel are responsive to known incidents.

Response and tracking: Lightspeed maintains a record of known security incidents that includes descriptions, dates and times of relevant activities, and incident remediation. Suspected and confirmed security incidents are investigated by security, operations or support personnel, and appropriate resolution steps are identified and documented. For any confirmed incidents, Lightspeed will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Lightspeed becomes aware of unlawful access to Customer data stored within its products, Lightspeed will: Notify the affected Customers of the incident; Provide a description of the steps Lightspeed is taking to resolve the incident; Provide status updates to the Customer contact, as it deems necessary or is legally required. Notification of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Lightspeed selects, which may include via email or telephone.

For more detailed information on the latest state of art measures, please contact us directly.