Last Modified: October 1, 2019

SPOTLIO Data Processing Addendum

Table of Contents

1. General

PLEASE READ THE EU GENERAL DATA PROTECTION REGULATION (“GDPR”) COMPLIANT DATA PROCESSING ADDENDUM (“DPA”) AND ALL REFERENCED OR LINKED MATERIALS CAREFULLY BEFORE USING ANY SPOTLIO SUBSCRIPTION SERVICE (“Services”), AND BEFORE ACCEPTING OUR OFFER AND INVOICE AND BEFORE DISTRIBUTING MOBILE APPS FROM THE SPOTLIO APP BUILDER PLATFORM. BY ACCEPTING OUR OFFER OR INVOICE OR USING ONE OR SEVERAL OF OUR SOFTWARE AS SERVICE PLATFORMS , YOU INDICATE YOUR ACCEPTANCE OF ANY UPDATES TO THESE DPA.

This DPA supplements the SPOTLIO Terms of Service that are active between SPOTLIO AG, Switzerland or one of its subsidiaries or affiliates (“SPOTLIO” or “we”, “us” or “our”) and you or the entity you represent (“Customer” or “You” or “Your”), if SPOTLIO processes Data Subject data for the Customer as a Data Controller, and when the GDPR* or any other data protection law (“Data Protection Laws”) applies to Your use of the SPOTLIO Services to process Your Data Subjects Personal Data. It shall be effective on the date Customer accepts the published Terms of Service by accepting a SPOTLIO offer or invoice or using one of our Services or one of the SPOTLIO related websites.

This DPA shall replace any existing DPA that parties may have previously entered into in connection with the Services.

Except for the changes made by this DPA, the SPOTLIO Terms of Service remains unchanged and in full force and effect. If there is any conflict between this DPA and the Terms of Service, the Terms of Service shall prevail to the extent of that conflict.

Our Services are continuously evolving and the form and nature of the Services and its elements may change from time to time without prior notice.

All capitalized terms not defined in this DPA shall have the meanings set forth in the GDPR, Terms of Service and the Privacy Statement.

**The GDPR is also known as (i) Regulation 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 (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it as may be amended, superseded or replaced.*

2. Roles for Processing Data

Between SPOTLIO and the Customer, Customer is the Data Controller of Data Subject data (“Personal Data”), and SPOTLIO shall process Personal Data only as a Data Processor acting on behalf of the Data Controller.

The Customer agrees that
(i) it shall comply with its obligations as a Data Controller under data protection laws in respect of its processing of Personal Data and any processing instructions it issues to SPOTLIO; and
(ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under data protection laws for SPOTLIO to process Personal Data and provide the Services pursuant to the SPOTLIO Terms of Service and this DPA.

Notwithstanding anything to the contrary in the Terms of Service including this DPA, Customer acknowledges that SPOTLIO shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, SPOTLIO is the Data Controller of such data and accordingly shall process such data in accordance with the SPOTLIO Privacy Policy and Data Protection Laws.

3. Customer Instructions

The parties agree that this DPA and the Terms of Service constitute Customer’s documented lawful instructions regarding SPOTLIO’s processing of Personal Data (“Documented Instructions”).

4. Scope of Processing Data

SPOTLIO will process Personal Data only in accordance with Documented Instructions. If there are any additional instructions outside the scope of the Documented Instructions, these require prior written agreement between SPOTLIO and the Customer, including agreement on any additional fees payable by Customer to SPOTLIO for carrying out such instructions. The Customer is entitled to terminate the agreement to process Personal Data under the Terms of Service and this DPA if SPOTLIO declines to follow instructions requested by the Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

Details of data processing:
(a) **Subject matter;** The subject matter of the data processing under this DPA is the Personal Data.
(b) **Duration;** As between SPOTLIO and Customer, the duration of the data processing under this DPA is until the termination of agreed data processing under the Terms of Service in accordance with its termination terms.
(c) **Purpose;** The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of SPOTLIO's obligations under the Terms of Service including this DPA.
(d) **Nature of the processing;** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
(e) **Categories of Data Subjects;** The Data Subjects may include Customer's customers, employees, suppliers and end-users. Any individual (i) whose information is stored on or collected via the Services, or (ii) to whom Customer engages or communicates with via the Services (collectively, "End Users").
(f) **Types of Personal Data processed;** Identification and contact data (name, date of birth, gender, general occupation or other demographic information, address, title, contact details, including email address, social media data, payment data), personal interests or preferences (including marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data, device data).

Customer acknowledges that in connection with the performance of the Services, SPOTLIO employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable SPOTLIO to deploy Tracking Technologies lawfully on, and collect data from the devices of End Users in accordance with and as described in the SPOTLIO Privacy Statement.

5. Sub Processing

Customer agrees that SPOTLIO may engage Sub Processors to process Personal Data on Customer's behalf. The Sub Processors currently engaged by SPOTLIO and authorized by Customer are listed in Annex A of this DPA.

SPOTLIO shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts

or omissions of the Sub-processor that cause SPOTLIO to breach any of its obligations under this DPA.

SPOTLIO shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer, and (ii) notify Customer by email if it adds or removes Sub-processors at least 10 days prior to any such changes.

Customer may object in writing to SPOTLIO's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a focus on achieving resolution. If this is not possible, the Customer may suspend or terminate the agreement to process Personal Data under the Terms of Service and this DPA without prejudice to any fees incurred by Customer prior to suspension or termination.

6. Security of Data Processing

SPOTLIO implements and maintains appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with SPOTLIO's security standards described in Annex B ("Security Measures").

The Customer is responsible for reviewing the data security information made available by SPOTLIO. Customer has to perform an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that SPOTLIO may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

SPOTLIO ensures that any person who is authorized by SPOTLIO to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality whether a contractual or statutory duty.

Upon becoming aware of a Security Incident, SPOTLIO notifies the Customer without undue delay and provides timely information related to the Security Incident as it becomes known or as is reasonably requested by Customer.

7. Data Subject Rights

Taking into account the nature of the Services, SPOTLIO offers Customer certain controls that Customer may elect to use to comply with its obligations towards Data Subjects. Should a Data Subject contact SPOTLIO with regard to correction or deletion of its Personal Data, SPOTLIO will use commercially reasonable efforts to forward such requests to Customer.

8. Return or Deletion of Data

Upon termination or expiration of the agreement to process Personal Data under the Terms of Service and this DPA, SPOTLIO deletes or returns to the Customer all Personal Data in its possession or control, save that this requirement shall not apply to the extent SPOTLIO is required by applicable law to retain some or all of the Personal Data, or Personal Data it has archived on back-up systems, which Personal Data SPOTLIO shall securely isolate and protect from any further processing, except to the extent required by applicable law.

9. Cooperation

The Services provide the Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Personal Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations responding to requests from Data Subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Personal Data within the Services, SPOTLIO shall at Customer's expense provide reasonable cooperation to assist Customer to respond to any requests from individual Data Subjects or applicable data protection authorities relating to the agreed processing of Personal Data. In the event that any such request is made directly to SPOTLIO, SPOTLIO shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If SPOTLIO is required to respond to such a request, SPOTLIO shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

If a law enforcement agency sends SPOTLIO a demand for Personal Data, e.g. through a subpoena or court order, SPOTLIO shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SPOTLIO may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then SPOTLIO shall give Customer reasonable notice of the

demand to allow Customer to seek a protective order or other appropriate remedy unless SPOTLIO is legally prohibited from doing so.

To the extent SPOTLIO is required under EU Data Protection Law, SPOTLIO shall at Customer's expense provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law

10. For Additional Information

If you have any questions about the rights and restrictions above, please contact SPOTLIO.

Annex A - List of SPOTLIO's Sub Processors

SPOTLIO uses third party Sub Processors to assist it in providing the Services as described in the DPA and other legal documents. The Sub Processors set out below provide cloud hosting or storage services, content delivery or review services or they assist in providing customer support as well as in incident tracking, response, diagnosis and resolution services.

SPOTLIO partners with organizations that, like itself, adhere to global standards and regulations. Apart from evaluation for technical requirements, SPOTLIO ensures examination of data protection measures, compliance with SPOTLIO's security requirements and security audit reports before close of contract. Initial agreements include review and approval of provisions for breach notification in the event of unwarranted data incidents, and necessary security measures for data protection.

Vendor	Purpose	Data Centers	SPOTLIO Services
Amazon Web Services Seattle, Washington, USA	Primary cloud infrastructure provider for SPOTLIO, where all SaaS applications are hosted. Almost all data stored, processed and transmitted through SPOTLIO products and services resides on Amazon Web Services data centers.	United States European Economic Area	App Platform Booking Platform Maps Platform Central Communication Platform Web Platform Data Services
Inntopia by Sterling Valley Systems Stowe, Vermont, USA	Cloud-based Central Reservation Platform to enable one-stop-shop experience in our App and Booking Platform.	Canada	Booking Platform App Platform
Apple Cupertino, California, USA	Mobile Platform provider for App Platform enabling push notifications and specific mobile identification management.	United States	App Platform
Google Mountain View, California, USA	Mobile Platform provider for App Platform enabling push notifications and specific mobile identification management.	United States	App Platform
Cloudinary Sunnyvale, California, USA	Cloud-based image and video management platform.	United States	App Platform Booking Platform Web Platform

Vendor	Purpose	Data Centers	SPOTLIO Services
Stripe Irving, Texas, USA	Cloud-based platform that builds economic infrastructure. It is integrated with our App and Booking Platform to enable customer payments with credit cards and other methods.	United States European Economic Area	App Platform Booking Platform Web Platform
Sendinblue Paris, France	Cloud-based digital marketing tools that are connected through API to our App and Direct Booking Platforms to send emails and SMS.	United States India European Economic Area	App Platform Booking Platform
Tech4Snow Asturias, Spain	Cloud-based digital platform to build and manage Your maps, real-time status and updates.	United States	Map Platform Central Communication Platform
Imagekit	Cloud-based image and video management platform.	United States India	App Platform Booking Platform Web Platform
ChatKit	Chat microservices for Spotlio application users.	United States European Economic Area Singapore India	App Platform
OVH Limburg, Germany	Web hosting for Corporate Website and Landing Pages	European Economic Area	Corporate Website Web Platform
Mailchimp Atlanta, Georgia	Email Marketing Tool to communicate with leads and customers	United States	Email Platform
Freshsales by Freshworks San Mateo, California, USA	Cloud-based CRM used to communicate with leads, customers and stakeholders.	United States European Economic Area Australia India Singapore	Business Development and Customer Experience management
Zendesk San Francisco, California, USA	SPOTLIO uses Zendesk as the SaaS Provider for everything related to support handling.	United States European Economic Area Australia Japan	Corporate Support Platform

Annex B - Technical and Organisational Security Measures

All our security measures are aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

These measures include the following:

- Multi-level firewall
- Proven anti-virus and detection of intrusion attempts
- Encrypted data transmission using SSL/https/VPN technology
- Tier 3 and PCI DSS certified data centres

Our technical and organisational security measures for the processing operations of personal data follow the principles of “data protection by design”, and “data protection by default”, in such a way that safeguards privacy and data protection principles right from the start, known as “data protection by design”. SPOTLIO ensures by default, that personal data is processed with the highest privacy protection, which means for example only the data necessary is processed, short storage period, limited accessibility. As a result, by default personal data isn’t made accessible to an indefinite number of persons, known as “data protection by default”.

Data Center Security

SPOTLIO delivers millions of pageviews for thousands of users every day through the data centers as described in the List of SPOTLIO’s Sub Processors. Our data centers manage physical security 24/7 with mandatory personal identification, and high tech security access control and access monitoring.
We have distributed denial-of-service (DDoS) mitigation and load balancing technology in place across all data centers. Our Data Center Security includes aggressive use of firewalls and network isolation where appropriate.
Access to our server systems is allowed only through secure connections by our trusted administrators at SPOTLIO.
Our systems are regularly updated and tested to search for vulnerabilities.

Protection from Data Loss and Data Corruption

We implement multiple layers of application logic that prevent corruption of data from one user account to another.
Account data is mirrored and regularly backed up off site. We secure the data in 3 different data centers.

Application Level Security

SPOTLIO account passwords are hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved, but it must be reset.
All login pages and all pages used to manage the Services (backend pages) pass data via TLSv1.2 internet security protocol. SPOTLIO platforms login pages and logins through a SPOTLIO API have brute force protection.
We perform regular external security penetration tests throughout the year using different vendors. The tests involve high-level server penetration tests, in-depth testing for vulnerabilities inside the application, and social engineering drills.

Internal IT Security

SPOTLIO offices are secured by security guards and badge access, and they are monitored with cameras throughout.
We have a dedicated internal security team that constantly monitors our environment for vulnerabilities. They perform penetration testing and social engineering exercises on our environment.

Internal Protocol and Education

We continuously train employees on best security practices, including how to identify social engineering, phishing scams, and hackers.

Protection Against Misuse

We monitor and will automatically suspend accounts for signs of irregular or suspicious login activity.
We monitor accounts and application activity for signs of abuse. In addition to our scalable algorithms, we employ another layer of human reviewers, who monitor for anomalous account and application activities.