



DATA PROCESSING AGREEMENT

PARTIES

This agreement between has been concluded on by and between

HotSpot System Ltd. a company registered in Hungary under company number 01-09883187 whose registered office is at Liszt Ferenc ter 10.

5/6 H-1061 Budapest, Hungary.

Hereinafter referred to as "**HotspotSystem**" and "**Processor**".

and

Name:

Registered seat (address):

Operator Username:

Hereinafter referred to as "**Hotspot Operator**" and "**Controller**".

Together referred to as the "**Parties**".

This Data Processing Agreement ("**DPA**") will be effective as of the signing date of this Agreement.

Unless otherwise defined herein, all capitalised terms shall have the meaning given to them in the Service Agreement.

CONSIDERING

- On Parties entered into a Service Agreement for the provision of Internet access allocation and related services (the "**Service Agreement**"). Hotspot Operator has been appointed as Controller and HotspotSystem as Processor of the Personal Data as further described in this DPA.
- Data Protection Laws require that any Processing of Personal Data shall be governed by an agreement between Processor and Controller, therefore Parties wish to further define their data processing relationship under the Service Agreement in this DPA.

This DPA shall form an integral part of the Service Agreement. In the event of any inconsistency arising between the provisions of this DPA and the Service Agreement, the provisions of this DPA shall prevail.

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

THE PARTIES HAVE AGREED AS FOLLOWS

1. DEFINITIONS AND INTERPRETATIONS

In this DPA the following words and phrases shall have the following meaning:

“Affiliate” means, as to any entity, any other entity that, directly or indirectly, for at least 50% controls, is controlled by or is under common control with such entity;

“Data Protection Laws” means the applicable data protection laws:

- (i) until May 24 2018, Directive 95/46/EC and the implementation thereof in national laws, and;
- (ii) as of May 25 2018, the EU Regulation 2016/679 on the protection natural persons with regard to the processing of personal data and on the free movement of such data (the **“GDPR”**).

“Data Subject” means any identified or identifiable natural person whose Personal Data is Processed by Processor on behalf of Controller in accordance with the Service Agreement;

“EEA” means the European Economic Area;

“Employee” means any employee, agent contractor, work-for-hire or any other person working under the direct authority of a Party;

“Instruction” means the documented instruction from Controller to Processor to perform a specific action in accordance with the Service Agreement, which directly or indirectly entails the Processing of Personal Data;

“Personal Data” means any information relating to a Data Subject (as defined under Data Protection Laws);

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed (in each case as defined under the GDPR);

“Pseudonymisation” shall be interpreted in accordance with the GDPR;

“Processing”, **“Process”** or **“Processes”** shall be interpreted in accordance with the Data Protection Laws; and

“Sub-Processor” shall mean any entity engaged by Processor to Process Personal Data on Processor’s behalf.

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

2. SCOPE OF PROCESSING AND GENERAL OBLIGATIONS

2.1 For the Processing of Personal Data under this DPA, Controller shall be regarded as the data controller and Processor shall be regarded as the data processor as defined under the Data Protection Laws, respectively.

2.2 Each Party undertakes to comply with its obligations under the Data Protection Laws. Each Party is solely responsible for compliance with the Data Protection Laws that apply to it.

2.3 Processor shall Process Personal Data in a manner consistent with this DPA, the Instructions of Controller, and/or to the extent necessary to provide the Services to the Controller under the Service Agreement. In order to perform the Services to Controller, Processor shall Process the Personal Data to comply with applicable laws and regulations. The Service Agreement and this DPA shall be seen as Instructions from Controller to Processor for the Processing of Personal Data.

2.4 Controller is responsible for ensuring that:

- (i) the Instructions it provides to Processor to Process the Personal Data are in compliance with any applicable laws (including Data Protection Laws); and
- (ii) where relevant, permission for such Instructions is obtained from the relevant Customers.

Processor is not responsible and not liable for Controller's Instructions.

3. DATA SUBJECT

3.1 Processor has no direct relationship with the Data Subject, and shall inform Data Subjects to contact Controller first. Processor shall notify Controller, unless specifically prohibited by applicable laws and regulations, if Processor receives:

- (i) any requests from an individual with respect to Personal Data Processed, including but not limited to opt-out requests, requests for access and/or rectification, blocking, data portability and all similar requests;
- (ii) any complaint relating to the Processing of Personal Data, including allegations that the Processing infringes on a Data Subject's rights under Data Protection Law; or
- (iii) any order, demand, warrant, or any other document purporting to compel the production of Personal Data under applicable law.

Processor shall not respond to any of the above unless expressly authorized to do so by the Controller or as obligated under applicable law or a court order.

3.2 Processor shall reasonably cooperate with Controller and assist Controller with respect to any action taken relating to such request, complaint, order or other document as described under clause 3.1 above. As far as reasonably possible and taking into account the nature of the Processing, the information available to Processor, industry practices and costs, Processor will implement appropriate technical and organisational measures to provide Controller with such cooperation and assistance.

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

3.3 Controller (and its auditors) will have access to Personal Data of Customers Processed by Processor through the administrative web interface. Where Controller is obliged under Data Protection Laws to provide information to an individual about the collection, Processing or use of its Personal Data, Processor shall reasonably assist Controller in making this information available. Where the required information can be retrieved by Controller itself from the systems of Processor through the access methods and reporting features made available by Processor to Controller, Controller will retrieve such information itself from the systems of Processor.

3.4 Processor shall not be liable, and Controller shall indemnify and hold harmless Processor, for any claim or complaint from a Data Subject regarding any action by Processor as a result of Instructions received from Controller.

4. DATA LOCATION

4.1 Processor shall store Personal Data Processed for an EEA or Switzerland entity of Controller solely in data centers located in the EU, except on specific Instruction of Controller. In addition, Personal Data Processed for non-EEA or Switzerland (Affiliates of) Controller may also be Processed on local or regional servers.

4.2 Controller shall ensure that:

- (i) Controller is entitled to receive Personal Data originating from the EEA or Switzerland and to access and/or transfer Personal Data to Controller's non-EEA or Switzerland Affiliates; and
- (ii) Processor and its Affiliates may lawfully use, Process and transfer Personal Data in accordance with the Service Agreement and this DPA on Controller's behalf.

5. SECURITY OBLIGATIONS

5.1 Processor shall implement and maintain adequate technical and organisational security measures to safeguard the security of the Personal Data in accordance with Data Protection Laws. These measures will guarantee an adequate level of security, taking into account the risks involved with the Processing and the nature of the Personal Data, prevailing industry standards and mandatory security requirements applicable to Processor.

5.2 These technical and organisational security measures shall include, as a minimum standard of protection in order to help ensure:

- a) the prevention of unauthorised persons from gaining access to Personal Data processing systems (physical access control);
- b) the prevention of Personal Data processing systems from being used without authorization (access control);

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

- c) that persons authorized to use processing system have access only to those Personal Data they need and are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during Processing (access control);
- d) that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the recipient entities for any transfer of Personal Data by means of data transmission can be established and verified (data transfer control);
- e) measures to check and establish whether and by whom Personal Data have been entered into, modified in, or removed from any processing systems (entry control);
- f) that Personal Data are Processed solely in accordance with the Instructions (control of instructions);
- g) that Personal Data are protected against accidental destruction or loss, (availability control); and
- h) that Personal Data collected for different purposes can be Processed separately (separation control).

5.3 Parties acknowledge that the adequacy of the security measures may change over time, and that an effective set of security measures demands frequent evaluation and improvement of security measures. Processor will therefore frequently evaluate and tighten, increase or improve such measures to ensure compliance.

5.4 Processor shall ensure that any Employee entrusted with Processing Personal Data has signed appropriate confidentiality obligations and is properly instructed to perform its duties in a manner helping to ensure compliance to the terms of this DPA and has been duly instructed to apply the applicable data security and confidentiality standards.

6. PERSONAL DATA BREACH

6.1 In case of a Personal Data Breach, Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach. Processor shall use its best commercial efforts to address the following in the notification:

- (i) Description of the nature of the Personal Data Breach including, where possible, the categories and number of Data Subjects;
- (ii) Name and contact details of Processor's contact where more information can be obtained;
- (iii) Description of the likely consequences of the Personal Data Breach;
- (iv) Description of the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including where appropriate measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

6.2 Processor will promptly take the necessary and appropriate actions to investigate, mitigate and remediate any effects of a Personal Data Breach, and provide assistance to Controller to ensure that Controller can comply with specific obligations under Data Protection Laws it may be subject to in relation to the Personal Data Breach.

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

7. SUB-PROCESSORS

Controller provides Processor hereby with a general authorisation to engage Sub-Processors. Processor will impose the same material data protection obligations on the Sub-Processors as set out in this DPA, in particular in relation to the implementation of appropriate technical and organisational measures. Processor shall notify Controller of any intended changes concerning the engagement or replacement of a Sub-Processor and Controller shall be given thirty (30) days to object, duly motivated and in writing, after receiving such notification. If Processor fails to address such objection, Controller's sole and exclusive remedy is to terminate the Service Agreement and this DPA immediately by providing written notice to Processor. For the avoidance of doubt, in the event Processor uses Sub-Processors, Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this DPA.

8. LIABILITY

HotspotSystem is not liable for damages incurred by the other party which are caused directly by a party's breach of the commitments made in this DPA.

9. TERM AND TERMINATION

9.1 This DPA shall take effect from the Effective Date of the Service Agreement and continue in full force and effect until the termination of the Service Agreement, after which this DPA will automatically simultaneously terminate, with the exception of the clauses which by their nature should continue to remain in full force and effect.

9.2 Processor shall, upon termination or expiration of this DPA, return or delete any Personal Data on Controller's first request. Such request should be filed within 3 months after this DPA has been terminated or expired. Processor shall confirm the return or deletion of Personal Data in writing.

9.3 Processor will not be required to delete Personal Data where retention by Processor is mandatory to comply with applicable legal requirements. Processor will in such case block the Personal Data for further use, ensure the secured storing of such Personal Data and not use such Personal Data for any other purpose than such compliance purposes. In the event deletion of a payment transaction and/or related Personal Data is not practically possible due to technical limitations Controller acknowledges that Processor may choose to use Pseudonymisation measures, rather than delete, certain Personal Data.

.....
Hotspot Operator

.....
Service Provider (HotSpot System Ltd.)

10. MISCELLANEOUS

11.1 This DPA shall be subject to the laws agreed to be applicable to the Service Agreement. In case of any conflict or dispute under or in relation to this DPA, this will be resolved solely before the competent courts as stipulated in the Service Agreement or, if applicable, in accordance with the arbitration rules specified in the Service Agreement.

11.2 No change of or amendment to this DPA shall be valid and binding unless made in writing and agreed upon by both Parties. In case a change in applicable law makes an amendment of this DPA necessary, the Parties will discuss and agree such required change in good faith and in writing.

12. SIGNATORIES

This DPA may be signed in separate counterparts.

	Hotspot Operator (Controller)	Hotspot System Ltd (Processor)
Name of Ceo/Owner (BLOCK LETTERS):		
Singature:		