HiJiffy Privacy Policy

Data Processing

In this section references to, "**Controller**" is a reference to the counterparty accepting "HiJiffy Privacy Policy" when registering in the website http://console.hijiffy.com/register, and "**Data Processor**" is a reference to a data processor, Horizon Behaviour Lda, engaged by the Controller to process personal data on its behalf, that has accepted these terms. Unless otherwise defined, other terms used in this Annex shall be given the meaning allocated to them in the European Union General Data Protection Regulation 2016/679 ("**GDPR**").

The table below sets out information on the scope of the processing of personal data by the Data Processor, which the Controller may from time to amend by written notice to the Data Processor if there are any updates or changes to the scope of processing.

Subject matter of processing	End-users that contact the Controller either through Facebook Messenger or the Data Processor's widget in the Controller's website.
Duration of processing	3 years
Nature of processing, e.g. means of processing	The Data Processor services will start operate when some end-user contacts the Controller through Facebook Messenger and/or the widget in the website. The goal is to provide answers to users' frequently asked questions in an immediate way and handoff to a human agent when necessary.
Purpose of processing	The purpose of data processing by Horizon Behaviour Lda. is to improve the user experience of users contacting Hotel Reservation Service Robert Ragge GmbH through Facebook Messenger (https://m.me/hrs), to answer users' queries in an automated way and providing a new channel for users to make reservations at Hotel Reservation Service Robert Ragge GmbH. The Data Processor does not verify the personal data supplied by the end-users; end-users shall be liable for the authenticity and compliance of such data.
Categories of data subjects	End-users that contact the Controller either through Facebook Messenger or the Data Processor's widget in the Controller's website.
Type of personal data (including special categories of personal data)	By contacting the Controller through the Data Processor services end-users users consent to the gathering, storage and use of their below data - which may be provided at their own discretion - for the purposes provided in this policy: • Name • Gender • Messages sent by the user • Facebook profile photo • Email address • Phone number • Logging of all interactions in the conversation • Details of reservations (hotel, check-in and check-out dates, number of adults, children and infants)

The Data Processor shall:

Instructions

1. Only process personal data in compliance with the GDPR, and shall not cause itself or the Controller to be in breach of the GDPR.

2. Process personal data:
   (a) strictly in accordance with and to the extent required for, the purposes of which the Data Processor is engaged by the Controller, including as set out in the table above; or
   (b) pursuant to the Controller's written instructions.

3. Promptly notify the Controller:
   (a) regarding events which impede the Data Processor's current or future ability to process personal data in accordance with these terms;
   (b) if the Data Processor becomes aware of any legal requirement for the Data Processor to process or disclose personal data to a third party or regulatory authority (save to the extent such notification is expressly prohibited by such laws), and cooperate with the Controller regarding action the Controller may reasonably take to challenge such requirements and, in any event, process and disclose no more personal data than is reasonably necessary to meet such requirements; and
   (c) immediately inform the Controller if the Data Processor considers (or has reason to believe that) any instruction from the Controller to be in violation of the GDPR.

4. Only process personal data in the **European Economic Area**, or such other country or territory as may be approved by the Controller in writing, and where the Data Processor seeks approval for the processing or holding of personal data outside of such countries or territories, the Data Processor shall provide a standard of protection to personal data that is comparable to the protection afforded under the GDPR. Any approval may also be subject to such other conditions as the Controller deems necessary to protect personal data or comply with the GDPR.

Confidentiality

5. Keep all personal data private and confidential, and not transfer or disclose personal data to any third party unless permitted under these terms or authorised by the controller in writing.

6. Only permit and ensure that its employees access personal data on a need to know basis, where they need to access personal data for the purposes set out in these terms, and provided that confidentiality obligations have been imposed on such employees to maintain and keep confidential the personal data.

Security

7. Protect personal data in the Data Processor's control or possession by making appropriate security arrangements (technical and organisational, described in the section "Annex 1 - General security measures") to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of personal data, or other similar risks.

Engaging Other Processors

8. Not engage any other processor (including the data processor's related entities) with respect to the Data Processor's processing of personal data ("**Other Processor**") unless:

   (a) the prior written consent of the Controller has been obtained;
   (b) the Data Processor has carried out adequate due diligence to ensure that the Other Processor is capable of providing a level of protection for personal data in accordance with these terms; and
   (c) there is a written agreement with the Other Processor containing obligations on the Other Processor which are equivalent to, and no less onerous than, those set out in these terms.

9. Remain fully liable to the Controller for all actions and omissions by such Other Processor.

Data Subject Rights

10. Provide all reasonable assistance to enable the Controller to fulfil its obligation to respond to requests by data subjects for the exercise of the rights available to them under the GDPR.

Data Breach

11. Where any event occurs that results, or may result in, any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed ("**Data Breach**"):

    (a) immediately notify the Controller after becoming aware of the Data Breach, providing Controller with details relating to the Data Breach, and regular updates on such details as the Data Processor becomes aware of it or as requested by the Controller; and
    (b) provide such reasonable assistance as may be required by the Controller in relation to the Data Breach, including assistance required to notify any regulatory authority of the Data Breach, communicate the Data Breach to affected data subjects, remedy the Data Breach and mitigate the impact of the Data Breach on the Controller and affected data subjects.

Impact Assessments

12. Notify the Controller prior to adopting any new type or method of processing in respect of personal data (including the use of new technology or processes).

13. At the Controller's reasonable request, participate in, and provide all reasonable assistance with, a data protection impact assessment or consultation in respect of the existing and any new type or method of processing proposed in respect of personal data, in accordance with the GDPR.

Retention and Disposal

14. Upon the request of the Controller or when retention of personal data is no longer necessary to serve the purposes for processing, immediately:

    (a) return to the Controller, all personal data;
    (b) delete or anonymise all personal data in its possession; and/or
    (c) instruct all third parties to whom it has disclosed personal data to return, delete or anonymise the personal data,

Regardless of the form in which personal data is in, and/or the media it is contained in, unless legislation imposed upon the Data Processor prevents it from returning or destroying all or part of the personal data. In that case, the Data Processor warrants that it will guarantee the confidentiality of the personal data and will not actively process the personal data transferred anymore.

Audit

15. Maintain complete and accurate records of the ways in which personal data is processed by the Data Processor, and make available all information, access to premises, systems and personnel necessary to demonstrate evidence of the Data Processor's compliance with these terms upon Controller's written request;

16. Permit the Controller, a third-party auditor acting under the Controller's direction, or any competent regulatory authority, to conduct data protection and/or security audits, including inspections, concerning the Data Processor's data protection and security procedures and those of any Other Processor, relating to the processing of personal data and their compliance with these terms.

Liability

17. Be liable for any damage and loss (including any administrative fines) suffered by the Controller due to the Data Processor's failure to comply with these terms.

Annex 1 - General security measures

IT-Security measures

Physical Access Control:
[Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.]

HORIZON BEHAVIOUR LDA. hosts the service within the Amazon's Web Services (AWS) environment in Dublin. These are world-class data centers and HORIZON BEHAVIOUR LDA. makes use of their web/application servers, file servers and databases. The service spans several layers of the AWS in that HORIZON BEHAVIOUR LDA. utilises the Elastic Computing (EC2) for application and web servers, and additionally for other file servers.

Key to all security measures is the physical security of the AWS data centers. The buildings that house the centers have significant physical access control, and incorporate extensive seismic bracing as well as the latest smoke and fire early-detection systems. The sites are monitored constantly, 24x7x365, by digital surveillance systems.

System Access Control:
[Measures to prevent data processing systems from being used without authorization.]

The machines can be accessed for administrative purposes in various ways: SSH, web interfaces, etc. Access to manage the systems uses only encrypted communications channels.

The access must be done with personal login data so that actions can be traced to a single person. Thus the sharing of credentials with other persons is prohibited. Users with access to our infrastructure are required to manage their password securely.

All machines have root logins for emergencies, which can only be used by administrators if the usual user authentication does not work correctly. The use of the root login must be documented.

Data Access Control:
[Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.]

HORIZON BEHAVIOUR LDA. maintains a set of permissions that allow controllers to check data for which they have rights. Permissions are given to individual controllers. All permissions are set explicitly and comprehensible. Access for a group of people is not granted to track each transaction.

Transmission Control:
[Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.]

All personal data passed to HORIZON BEHAVIOUR LDA. infrastructure must use an authenticated and encrypted communication channel.

Input Control:
[Measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.]

The input, modification and deletion of data are logged in our infrastructure. The security of data entry, modification and deletion is part of the software. Log files are automatically generated by the HORIZON BEHAVIOUR LDA. infrastructure with meaningful retention times.

Job Control:
[Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.]

Commissioned data processing must be carried out according to instructions with measures to segregate the responsibilities :

- Unambiguous wording of the contract;

- Access control policy based on need to know and need to use;
- Monitoring;

Availability Control:
[Measures to ensure that personal data are protected from accidental destruction or loss.]

The service Databases are configured to point-in-time recovery, with snapshots of the database servers being taken every day. The Application and file servers are snapshot on a regular schedule.

Separation Control:
[Measures to ensure that data collected for different purposes can be processed separately.]

Data collected for different purposes are processed separately.