DATA PROCESSING AGREEMENT
(Revision May 2019)

This Data Processing Agreement ("DPA") forms part of the master agreement between the Client and Guestmeter (the "Agreement") to reflect the parties' agreement in regards to the processing of Personal Data during the provision of the Guestmeter services (the "Services") to the Client and in accordance with the requirements of the EU Regulation 2016/769 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 repealing Directive 95/46/EC (the "GDPR").

In the course of providing the Services, Guestmeter may process Personal Data on behalf of the Client and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

EXECUTION

This DPA consists of two parts: the main body of the DPA, and annexes 1 and 2 regarding the purpose of the processing of personal data on the Guest Satisfaction Surveys ("GSS") service and on the Guest Messaging Hub ("GMH") service.

Guestmeter as a consequence of the provision of Services detailed in the annexes, will be able to access and proceed with the processing of certain data owned by and responsibility of the Client.

By accepting this Agreement, the Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection laws and regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Guestmeter processes Personal Data for which such Authorized Affiliates qualify as the Controller.

Now, therefore, and in order to comply with the personal data protection legislation, and in particular, with the GDPR, the Parties agree to enter into this Agreement pursuant to the following:

TERMS

1. OBJECT

The object of this Agreement is to define the conditions under which the DATA

PROCESSOR shall process the personal data necessary to provide the service contracted by the DATA CONTROLLER in accordance with the provisions of Article 28 GDPR and other data protection legislation.

Said treatment will be carried out on personal data of which the DATA CONTROLLER is the owner in accordance with what is set forth in Annex I (hereinafter, the "Personal Data"), for the provision of the Service, which the DATA PROCESSOR provides to the DATA CONTROLLER.

2. OBLIGATIONS OF THE DATA PROCESSOR

The DATA PROCESSOR shall process the personal data resulting from the provision of the contracted service in accordance with the following obligations:

- It shall limit its activities to those necessary to provide the contracted Service to the DATA CONTROLLER, as set out in this Agreement and its Annexes, these being understood as inseparables parts thereof.

  In particular, it shall at all times process the personal data in the manner set out in the instructions given to it by the DATA CONTROLLER, and as provided for in the applicable personal data protection laws, even with respect to the transfer of personal data to another country or to an international organization, unless it is obliged to do so by virtue of the European Union or Member State Laws applicable to the DATA PROCESSOR, in which case the DATA PROCESSOR shall inform the DATA CONTROLLER of that legal requirement before processing the data.

  If the DATA PROCESSOR considers that any of the instructions contravene the GDPR or any other European Union or Member States data protection legislation it shall inform the DATA CONTROLLER immediately.
- It shall not process any other personal data or apply or use the data for any purpose other than to provide the Service or use the data for its own purposes.
- It shall provide the necessary training in personal data protection to the personnel authorized to process the personal data.
- The DATA PROCESSOR shall keep a written record of all data processing activities it carries out, containing:
  - The name and contact data of the DATA CONTROLLER and the DATA PROCESSOR and, as applicable, of the representatives of the DATA CONTROLLER and the DATA PROCESSOR, and, if necessary, of the data protection officer.
  - The processing categories established by each PROCESSING MANAGER.
  - Transfers of personal data to other countries or international organizations, as the case may be, including the name of the country or international organization and documentation containing the appropriate guarantees.
  - A general description of the technical and organizational security measures in relation to:
    - The pseudonymisation and encryption of personal data, when necessary.

- The capacity to guarantee permanent confidentiality, integrity, availability and resilience of the processing systems and services.
- The capacity to rapidly restore the availability and access to personal data in the event of a physical or technical incident.
- The regular checking, assessment and valuation process regarding the efficacy of the technical and organizational measures to guarantee security during processing.

- It shall keep under control and safeguard the personal data supplied by the DATA CONTROLLER to which it has access during the provision of the Service and shall not disclose, transfer or any other way, communicate the data to any other persons, not even for conservation purposes.
- In the event of having to transfer personal data to another country or to an international organization, by virtue of any Union or Member State Law applicable to it, it shall notify the DATA CONTROLLER of that legal requirement beforehand, except if that Law forbids this due to important reasons of public interest.
- It shall provide support to the DATA CONTROLLER in implementing personal data impact assessments, when necessary.
- It shall support the DATA CONTROLLER in holding consultations with the control authorities, when necessary.
- When necessary, it shall designate a data protection officer and communicate the name and contact data of that person to the DATA CONTROLLER.

3. SECURITY OF THE PERSONAL DATA

The DATA PROCESSOR shall implement the security measures and mechanisms set out in Article 32 GDPR to:

- Guarantee the permanent confidentiality, integrity, availability and resilience of the processing systems and services.
- Rapidly restore availability and access to personal data in the event of a physical or technical incident.
- Regularly check, evaluate and assess the technical and organizational methods implemented to guarantee security in processing.
- Pseudonymisation and encryption of personal data, as required.

In this regard, the DATA PROCESSOR, proposes the technical and organizational measures indicated as follows, in view of the risk analysis which has been carried out:

Control		Responsible Parties	
		DATA PROCESSOR	DATA CONTROLLER
1.0	ASSET MANAGEMENT		
1.1	Acceptable use of equipment		

Control		Responsible Parties	
		DATA PROCESSOR	DATA CONTROLLER
1.1.1	The guidelines provided in writing by the DATA CONTROLLER regarding devices provided by the DATA CONTROLLER that can be used to access confidential Data of the DATA CONTROLLER shall be complied with.	X	
1.2	**Information Classification**		
1.2.1	For each job description, the DATA CONTROLLER shall communicate to REVIEW RANK the types of confidential Data of the DATA CONTROLLER that REVIEW RANK must process. The DATA CONTROLLER will inform REVIEW RANK when providing Confidential data, which must be clearly and appropriately marked.		X
2.0	**Security of Human Resources**		
2.1	**Training**		
2.1.1	All REVIEW RANK personnel assigned to the project must receive the standard training in data protection, as well as the training provided by the DATA CONTROLLER.	X	
2.1.2	All personnel of the DATA CONTROLLER assigned to the project must receive the training specified in the Procedures.		X
3.0	**Physical and environmental security**		
3.1	**Physical security**		
3.1.1	The physical security controls required by the security regulations will be adopted in each center where confidential data of REVIEW RANK is being processed.	X	X
3.1.2	All personnel must be registered and carry identification cards.	X	X
4.0	**Management of communications and operations**		
4.1	**Network security management**		
4.1.1	Access control lists will be maintained for network devices.	X	X
4.1.2	Network traffic will pass through monitored and protected firewalls using intrusion prevention/detection systems that keep track of traffic in them.	X	X
4.1.3	Access to network devices for administration tasks will be protected with at least 128-bit encryption.	X	X
4.1.4	Antispoofing will be activated.	X	X
4.1.5	Authentication passwords in networks, applications and servers must have the level of complexity required by each Party.	X	X
4.1.6	If possible, the DATA CONTROLLER will disable access to e-mails external to the DATA CONTROLLER from devices provided by the DATA CONTROLLER accessing Confidential Data of the DATA CONTROLLER.		X
4.1.7	The transport layer security (TLS) will be activated between the email domains of the DATA CONTROLLER and REVIEW PRO.	X	X
4.2	**Virtual private networks ("VPN"). If it is necessary to remotely access the REVIEW RANK network to process confidential Data of the DATA CONTROLLER and it has been agreed to create a VPN between centers, both Parties will install VPN servers with the following or similar characteristics:**		
4.2.1	Connections will be protected with at least 128-bit encryption.	X	X

Control		Responsible Parties	
		DATA PROCESSOR	DATA CONTROLLER
4.2.2	DATA CONTROLLER connections to REVIEW RANK service centers will be established exclusively using REVIEW RANK VPN services.	X	X
4.2.3	Split Tunneling functionality will be disabled.	X	X
4.2.4	Two factor authentications will be required.	X	X
4.3	**Support**		
4.3.1	**For transmission of confidential data of the DATA CONTROLLER.**		
4.3.2	The data will be protected with at least 128-bit encryption, unless local regulations prevent it, or the Parties reach another agreement.	X	X
4.3.3	As far as possible, the use of portable external supports to transmit confidential data of the DATA CONTROLLER shall be avoided. When necessary, data transmitted on recordable or portable external media will be encrypted during transmission, using encryption keys that will be transmitted separately. All Confidential Data transmitted between the Parties will be transported using a secure and encrypted storage device, or a file transfer mechanism accepted by the Data Protection Executives. The data will be protected with at least 128-bit encryption. When possible, emails between companies will be avoided.	X	X
4.3.4	Whenever it is viable from a commercial point of view and agreed by the Data Protection Executives, the DATA CONTROLLER shall adopt measures such as masking or anonymization of confidential Data before facilitating access to REVIEW RANK. The DATA CONTROLLER will identify situations in which open/unencrypted data is used outside of production environments before facilitating access to REVIEW RANK. If production data are used in tests, compensatory controls will be agreed upon and applied.		X
4.4	**Physical transport of data**		
4.4.1	A professional messenger with documented chain of custody will be used for the transportation by third parties of paper copies or mobile media that contain confidential data of the DATA CONTROLLER.	X	X
4.5	**Data deletion**		
4.5.1	The members of the team that leave the project will return or destroy all the confidential Data of the DATA CONTROLLER that are in their possession.	X	
4.5.2	REVIEW RANK will keep in its files copies of records containing Confidential Data from the DATA CONTROLLER for as long as necessary or as part of normal backup processes to ensure that REVIEW RANK fulfills its obligations under the Agreement. REVIEW RANK will inform the DATA CONTROLLER when it keeps such data in its files and will protect or hide the confidential Data of the DATA CONTROLLER in those files by means of masking or by other methods. REVIEW RANK will have no obligation to keep copies of REVIEW RANK databases or other compilations or confidential data repositories in your	X	

	files.		
4.5.3	REVIEW RANK will destroy the paper copies of Confidential Data of the DATA CONTROLLER, using a paper shredder or a secure destruction system, when they are no longer necessary for the provision of the Services.	X	
4.6	**Management of third-party services**		

Control		Responsible Parties	
		DATA PROCESSOR	DATA CONTROLLER
4.6.1	The subcontractors employed to provide the Services must comply with contractual conditions similar to those imposed on the Parties in terms of privacy and security.	X	
4.6.2	The communications and information technologies providers that provide general services to REVIEW RANK, and that have not been contracted specifically for the provision of the Services (such as telecommunications and email providers), must comply with contractual conditions regarding privacy and security that are reasonable from the commercial point of view.	X	
4.7	**Security copies**		
4.7.1	In the event that REVIEW RANK provides storage services for production databases and backups are made on magnetic tapes or other external media, the backup copies will be protected with a minimum 256-bit encryption (unless there are requirements legal rights that contravene this) on behalf of the DATA CONTROLLER.	X	X
5	**Access control**		
5.1	**User access control**		
5.1.1	The DATA CONTROLLER will use means that are commercially viable so that REVIEW PRO can only access the confidential Data of the DATA CONTROLLER that are necessary for REVIEW RANK to fulfill its obligations under the Agreement.		X
5.1.2	Procedures for creation and elimination of user accounts, with the necessary authorizations, will be applied to grant and deny access to all the systems, data and internal applications of the DATA CONTROLLER that are used during the project. A person with the necessary authority (in accordance with the Agreement) will be designated to authorize the creation of new user IDs or to increase the level of access of the existing IDs.	X	X
5.1.3	An access control list containing access data of the persons assigned to the project will be drawn up, detailing the type of access, as well as the date on which the access to the team members was granted or revoked.	X	
5.1.4	The access control list will be reviewed, at least, quarterly or as often as agreed in writing by the Parties, in order to confirm that the levels of access continue to be adequate and that the revocation of access to personnel that has left the project have been processed correctly.	X	
5.1.5	The access of the personnel that has left the project will be revoked in a maximum term of two working days or when the Agreement requires it.	X	X
5.1.6	When necessary, access to project staff and other employees will be allowed according to the principle of minimum privilege, so that each person has access only to the resources and systems needed for their work.	X	X
5.1.7	When necessary, access to project staff and other employees will be allowed according to the principle of minimum privilege, so that each person has access only to the resources and systems needed for their work.	X	X

5.1.8	Each person accessing a system or application will have their own user IDs and passwords. Sharing of both user IDs and passwords will be prohibited.	X	X

Control		Responsible Parties	
		DATA PROCESSOR	DATA CONTROLLER
5.1.9	Two factors authentication will be required to access the internal network environment of the DATA CONTROLLER from centers outside the DATA CONTROLLER/REVIEW RANK. In general, an internal network environment will be the network environment that a person can access from the offices or data centers of the DATA CONTROLLER.	X	X
5.1.10	To the extent possible, the access methods used by the DATA DONTROLLER will control the download, printing, copying and other forms of extraction of confidential data from the DATA CONTROLLER (for example, Citrix/VDI/firewall in applications layer).		X
5.2	**Password administration**		
5.2.1	The electronic communication of passwords will be protected with encryption of 128 bits minimum.	X	X
5.2.2	The initial user passwords must be changed at the first access. Sharing of user IDs and passwords will be prohibited.	X	X
6.1	**Encryption**		
6.1.1	Transmissions of confidential data between the Parties will be protected with at least 128-bit encryption.	X	X
6.1.2	Mobile phones and tablets will be protected by PIN, the number of emails that can be stored on the device will be limited and remote deletion will be enabled.	X	
6.1.3	Hard disks will be protected with at least 256-bit encryption in all work stations used for the provision of Services (work stations of the Treatment Manager, rented, owned by the Client or subcontractors).	X	X
7	**Management of information security incidents**		
7.1	**Communication of security incidents**		
7.1.1	Any actual or potential security incident that causes or may cause the loss, misuse or unauthorized acquisition of confidential data (such as theft or loss of a laptop) should be reported immediately to a REVIEW PRO center.	X	
7.1.2	Other requirements for notification of security incidents under the Agreement will be identified and said requirements will be communicated to the project staff.	X	X
8	**Compliance**		
8.1	**Compliance with legal requirements**		
8.1.1	The confidential data of the DATA CONTROLLER will not be used for any purpose that exceeds the services contracted or that is not required by the applicable legislation.	X	
8.1.2	For each job description, the commercial, operational and technical requirements derived from the data privacy laws that must be met by the DATA CONTROLLER must be identified in the design and / or definition of business process requirements.		X
8.1.3	The controls required by the data privacy laws that apply to REVIEW RANK as a service provider will be met.	X	

4. AUDIT

For the purposes of checking the level of compliance by the DATA PROCESSOR with the terms set forth in the applicable legislation and in this Agreement, the DATA CONTROLLER may request the performing of audits, alone or through an independent auditor authorised by the DATA PROCESSOR. The DATA CONTROLLER shall notify the DATA PROCESSOR through any channel of its wish to perform such audits at least thirty (30)working days before the planned audit date.

In this regard, The DATA CONTROLLER may ask the DATA PROCESSOR for the necessary information to evaluate its level of compliance, and, in particular, evidence of compliance with the provisions of the legislation applicable to the Agreement and with the terms of the present Agreement.

The DATA PROCESSOR shall cooperate diligently and facilitate access to and the obtaining of the necessary information in response to the needs of the DATA CONTROLLER. The evidence and documentation obtained during the audit shall be stored in a repository owned by the DATA PROCESSOR to guarantee the non-disclosure and security of the information, in keeping with the present state of technology.

By way of example, and without limit, at the request of the DATA CONTROLLER, the DATA PROCESSOR shall provide the following information/documentation:

- The duly-updated certificates set out in Article 42 of the General Data Protection Regulation, in the event of obtaining such certificates as set out in ANNEX 1 of this Agreement, and submission of the audit reports it is obliged to present in accordance with said certificates.
- In the event that the DATA PROCESSOR has declared its adhesion to Codes of Conduct, the data related to its adhesion.
- Certificates and standards held by the DATA PROCESSOR in relation to information security.
- Internal or external audit reports prepared by the DATA PROCESSOR regarding data protection and/or information security.
- Protocols, policies, manuals and procedures regulating the data processing activities of the DATA PROCESSOR.
- A list specifying the controls and indicators implemented in the information systems used by the DATA PROCESSOR.

If, as a consequence of the audit, the DATA CONTROLLER detects any breach, pursuant to current law and the terms of the present Agreement, it may, at its sole discretion and depending on the gravity of the breach:

- Request the DATA PROCESSOR to remedy the detected breach immediately by preparing a correction plan which shall be implemented within a certain time not exceeding one month, and the DATA PROCESSOR shall provide the DATA CONTROLLER with evidence accrediting the resolution thereof.
- Proceed to the early termination of the Service as set out in Annex I. In this case, the DATA PROCESSOR shall return to the DATA CONTROLLER the proportional part of the amounts received for all services not effectively provided.

5. NOTIFICATION OF DATA SECURITY BREACHES

The DATA PROCESSOR shall inform the DATA CONTROLLER without undue hesitation and in any case, within 48 hours, of any security breaches with respect to the personal data in its charge which comes to its notice, including relevant information for documenting and reporting the incident.

The DATA PROCESSOR shall provide at least the following information, if it has it:

a) A description of the nature of the personal data security breach, including, if possible, the categories and approximate number of affected interested parties and the categories and approximate number of affected personal data records.

b) The name and contact data of the data protection supervisor or another contact point where more information can be obtained.

c) A description of the possible consequences of the personal data security breach.

d) A description of the measures taken or proposed to remedy the personal data security breach, including, as necessary, measures taken to mitigate any negative effects.

If it is not possible to provide the information simultaneously, and if not provided simultaneously, the information shall be furnished gradually without undue delay, and in all cases, within 24 hours.

6. CONFIDENTIALITY OBLIGATION

The obligation of secrecy and confidentiality arising from this Agreement shall be binding on the DATA PROCESSOR during the Agreement term and shall, depending on the type of information in question, be extended for the maximum terms provided for in the applicable legislation.

The DATA PROCESSOR warrants that the persons authorized to process personal data expressly agree in writing to respect the confidentiality and to comply with the respective security measures which the DATA CONTROLLER shall issue in due time.

Authorized person refers to any person who, apart from the legal nature of their relationship with the DATA PROCESSOR, may have to the data to be processed, by any means.

The DATA PROCESSOR shall make available to the DATA CONTROLLER documentation accrediting compliance with the obligation established in the preceding sections.

7. INFORMATION OBLIGATION

It is the responsibility of the DATA CONTROLLER to facilitate the right of information at the time of the data collection, notwithstanding that the DATA PROCESSOR facilitates through its tool a standard clause in order be used by the DATA CONTROLLER under his responsibility.

8. OBLIGATION TO RETURN OR DESTROY THE DATA

Once the provision of the service object of the Agreement has been completed, the DATA PROCESSOR undertakes to destroy any information that contains personal data and that has been transmitted by the DATA CONTROLLER to the DATA PROCESSOR for the provision of the Service. For this purpose, it will apply the appropriate physical and logical measures to guarantee that the data incorporated to the different supports are irretrievable.

Once destroyed, the DATA PROCESSOR shall issue a certificate of destruction to the DATA CONTROLLER where the information, physical media and documentation destroyed will be related.

However, as foreseen in the previous paragraph, the DATA PROCESSOR may keep the data and information processed, duly blocked, in the event that liabilities could arise from their relationship with the DATA CONTROLLER.

After the expiration of the limitation period for the actions that led to the retention of data, the DATA PROCESSOR shall proceed with its destruction as described in the previous paragraphs.

9. SUBCONTRACTS

The DATA PROCESSOR is only authorized to subcontract the provision of services entailing the processing's object to this Agreement, and with the companies identified through the following link https://www.guestmeter.com/legal/#privacy

To subcontract with other companies, the DATA PROCESSOR must communicate it to the DATA CONTROLLER by writing, clearly and unambiguously identifying the subcontractor company and their contact information. Said subcontracting may be carried out in case the DATA CONTROLLER does not manifest its opposition within a period of thirty (30) calendar days.

The subcontractor, who also has the status of DATA PROCESSOR, is equally bound to comply with the obligations established in this document for the DATA PROCESSOR and the instructions issued by the DATA CONTROLLER. It is up to the initial DATA PROCESSOR to regulate the new relationship in accordance with article 28 of the RGPD, so that the new manager is subject to the same conditions (instructions, obligations, security measures, ...) and with the same formal requirements as him, regarding the adequate processing of personal data and the guarantee of the rights of the people affected.

In the case of non-compliance by the sub-manager, the initial DATA PROCESSOR will remain fully liable to the DATA CONTROLLER regarding the fulfillment of the obligations.

10. RIGHTS OF INTERESTED PARTIES

The DATA PROCESSOR shall assist the DATA CONTROLLER in responding to the exercise of interested parties' rights, within three calendar days from the receipt, so that the DATA CONTROLLER may duly resolve said request.

11. OBLIGATIONS OF THE DATA CONTROLLER

The DATA CONTROLLER has the following obligations:

- It shall deliver the data to be processed subject to the terms of this Agreement to the DATA PROCESSOR.
- It shall analyze the risks that could arise from the processing service assignment and on the basis of that analysis, inform the DATA PROCESSOR of the technical and organizational means to be implemented in order to provide the assigned processing service.
- If necessary, it shall make an assessment of the personal data impact of the processing operations to be carried out by the DATA PROCESSOR.
- It shall make all the necessary preliminary consultations.
- Before and during the whole processing operation, it shall ensure that the DATA PROCESSOR complies with the GDPR.
- It shall supervise the processing, including the conducting of inspections and audits.

12. RESPONSIBILITIES

The DATA PROCESSOR agrees to fulfil the obligations established in this Agreement and in the applicable legislation, in connection with this processing service assignment.

Pursuant to the terms of Article 28.10 GDPR and other applicable data protection legislation, if the DATA PROCESSOR breaches the terms of the GDPR in determining the purposes and means of the processing, it shall be held responsible for the processing, with respect to such processing.

13. PROTECTION OF THE PERSONAL DATA OF THE PARTIES' REPRESENTATIVES

The personal data of the Parties' representatives shall be processed, respectively, by the entities identified on the first page, which shall act independently, as the parties responsible for the processing thereof. Such data shall be processed in accordance with the rights and obligations set out in this Agreement, without taking automated decisions that could affect these representatives. Therefore, the legal basis of the processing is to fulfil that contractual relationship, with this purpose being strictly necessary to execute this Agreement.

The data shall be kept during the term of the contractual relationship established herein and shall be processed only by the parties and by those third parties who are legally or contractually obliged to communicate them (as is the case of third party service providers who have been entrusted with any service related to the management or execution of the Agreement).

The Parties' representatives may, pursuant to the terms set forth by current law, exercise their rights of access, rectification and erasure of data, and establish restrictions on the processing of their personal data, object to the same or request the portability

of their data by writing to each of the Parties at the addresses specified on the first page of this document. In the event they are not satisfied with the service received from the Parties after previously exercising any of the above rights, they may submit a complaint to the Spanish Data Protection Agency or any other competent authority.

The Parties' representatives may contact the data protection officer of REVIEW RANK, S.A. by sending an email to: privacy@guestmeter.com

14. ENTRY INTO FORCE

This Agreement shall enter into force on the date of its signature and shall remain in force until the termination of the service provision relationship by the DATA PROCESSOR in favor of the DATA CONTROLLER and provided that the obligations set forth in the in this Agreement have been meet, independently of any other obligation of legal nature that is applicable to the parties after the termination of said relationship.

In witness whereof, the Parties sign this Agreement as proof of their intent to be bound, in duplicate copy, as of the date and place first above written.

ANNEX I PURPOSE OF THE PROCESSING – (GSS)

1. **The main activities of the DATA PROCESSOR are:**

   The collecting of Guest Satisfaction Survey

2. **The services provided by the DATA PROCESSOR are thefollowing:**

   - Sending an email to Client guests inviting them to fill in thesurvey
   - Hosting of the survey form
   - Hosting of the survey response

3. **Contract /purchase order date subscribed between the DATA CONTROLLER and the DATA PROCESSOR giving rise to this Agreement:**

   The initial date of this DPA corresponds to the same as as that of the main contract.

4. **Duration of the contract:**

   The term of this Contract corresponds to the same as that of the main contract.

5. **Personal data subject to processing:**

OBJECT	Treatment of personal data of the guests of the hotels for the sending of satisfaction surveys.
PROCESSING TO BE CARRIED OUT	☐ Collection ☒ Registration ☐ Structuring ☐ Modification ☒ Conservation ☐ Extraction ☒ Consultation ☐ Communication by transmission ☐ Diffussion ☒ Interconnection ☐ Checking ☐ Limitation ☐ Suppression ☐ Destruction ☒ Conservation ☐ Communication

<table>
<tr><td>PURPOSE OF THE PROCESSING</td><td colspan="2">☒ Customer, accounting, tax and administrative management
☐ E-commerce
☐ Provision of electronic certification services
☐ Provision of electronic communication services
☐ Provision of financial standing and credit services
☐ Economic-financial and insurance services
☐ Advertising and commercial prospection
☐ Electronic communication guides/repertoires
☐ Management of associative, cultural, leisure, sports and social services
☐ Profile analysis
☐ Video surveillance
☐ Private security
☐ Building access security and control
☐ Statistical, historical or scientific purposes
☐ Compliance/non-compliance of monetary obligations
☐ Human resources
☐ Payroll management
☐ Occupational risk prevention
☐ Clinical histories
☐ Sanitary management and control
☐ Epidemiological research and similar activities
☐ Social assistance management
☐ Management of political party, trade union and parish church associate or members
☐ Education</td></tr>
<tr><td rowspan="6">TYPE OF PERSONAL DATA</td><td><u>CATEGORIES</u></td><td><u>EXAMPLES</u></td></tr>
<tr><td>☐ Data related to employment and the organization</td><td>Name and surname, sex, address, email, fixed or mobile telephone number, group company, department, cost centre,
responsibilities, personnel number, functions, presence (yes/no), etc.</td></tr>
<tr><td>☒ Data related to the use of IT tools</td><td>User ID, functions, rights, access numbers,
computer name, IP address, GID, Legic- no., etc.</td></tr>
<tr><td>☐ Employee photo</td><td>Portrait photo posted by employee (intranet, telephone list, social network platform, etc.)</td></tr>
<tr><td>☒ Private contact data and identification data</td><td>Name and surname, sex, address, email, fixed or mobile telephone number,
date/place of birth,
identification numbers,
nationality, etc.</td></tr>
<tr><td>☐ Conntractual data</td><td>Products purchased, financial services, contract date, purchase price,
extras, warranties, etc.</td></tr>
</table>

	☐ Data related to personal and professional circumstances and characteristics	Data related to partner or children, marital status, portrait photo, honorary post, position data, career, employment period, tasks, activities, analysis of file

		entries, entry and exit data, qualifications, measurements / evaluations, etc.	
	☐ Payment and management data	Wage group, payroll accounting, special payments, wage garnishments, attendance times, justifications of absence, etc.	
	☐ Creditworthiness and financial data	Payment habits, balance, commercial agency data, ratings, financial circumstances, bank account, credit card number, etc.	
	☐ Sensitive data	Racial or ethnical origin, political opinions, religious or philosophical beliefs, trade union affiliation, genetic data, biometric data for the sole purpose of identifying individuals, data related to health or to sex life or preferences.	
	☐ Crimes/ offences	Data referring to crimes, offences or suspected crimes or offences.	
PARTIES	**INTERESTED PARTIES**	**DESCRIPTION**	**EXAMPLES**
	☐ Employees	Employees from the respective Group company (in business unit terms)	E.g., employees, trainees, applicants and former employees
	☐ Group employees	Employee from other Group companies (in terms of REVIEW RANK Group members, but not business units)	E.g., REVIEW RANK-USA, ASIA, employees, etc.
	☐ Partner company employees	Employees from a supplier, joint-venture, temporary work agency	E.g., IT services employees, joint venture employees, temporary workers
	☒ Clients	Any person who has a commercial relationship (with the respective business unit)	E.g., Clients.
	☐ Other business partners	Any person (natural or corporate) who has a commercial relationship (with the respective business unit), except	E.g., suppliers, importers or service providers, agents, free-lance workers, etc.

		clients	

	☐ Third parties	Any person who does not have a commercial relationship with the respective Group company (responsible business unit)	E.g., visitors, guests, related parties
	☐ Underage persons	Persons under 13	

ANNEX II PURPOSE OF THE PROCESSING – (MESSAGING HUB)

1. **The main activities of the DATA PROCESSOR are:**

   The connection of several direct messaging services to a central hub to manage the communication with the guests.

2. **The services provided by the DATA PROCESSOR are the following:**

   - Collection of the guest's messages on a central hub
   - Hosting of the messages on our servers

3. **Contract /purchase order date subscribed between the DATA CONTROLLER and the DATA PROCESSOR giving rise to this Agreement:**

   The initial date of this DPA corresponds to the same as that of the main contract.

4. **Duration of the contract:**

   The term of this Contract corresponds to the same as that of the main contract.

5. **Personal data subject to processing:**

OBJECT	Treatment of personal data of the guests of the hotels for the provision of the Messaging Hub service.
PROCESSING TO BE CARRIED OUT	☒ Collection ☐ Registration ☐ Structuring ☐ Modification ☒ Conservation ☐ Extraction ☒ Consultation ☐ Communication by transmission ☐ Diffussion ☒ Interconnection ☐ Checking ☐ Limitation ☐ Suppression ☐ Destruction ☒ Conservation ☐ Communication

<table>
<tr><td>PURPOSE OF THE PROCESSING</td><td colspan="2">☒ Customer, accounting, tax and administrative management
☐ E-commerce
☐ Provision of electronic certification services
☐ Provision of electronic communication services
☐ Provision of financial standing and credit services
☐ Economic-financial and insurance services
☐ Advertising and commercial prospection
☐ Electronic communication guides/repertoires
☐ Management of associative, cultural, leisure, sports and social services
☐ Profile analysis
☐ Video surveillance
☐ Private security
☐ Building access security and control
☐ Statistical, historical or scientific purposes
☐ Compliance/non-compliance of monetary obligations
☐ Human resources
☐ Payroll management
☐ Occupational risk prevention
☐ Clinical histories
☐ Sanitary management and control
☐ Epidemiological research and similar activities
☐ Social assistance management
☐ Management of political party, trade union and parish church associate or members
☐ Education</td></tr>
<tr><td rowspan="7">TYPE OF PERSONAL DATA</td><td><u>CATEGORIES</u></td><td><u>EXAMPLES</u></td></tr>
<tr><td>☒ Data related to employment and the organization</td><td>Name and surname, sex, address, email, fixed or mobile telephone number, group company, department, cost centre, responsibilities, personnel number,
functions, presence (yes/no), etc.</td></tr>
<tr><td>☒ Data related to the use of IT tools</td><td>User ID, functions, rights, access numbers, computer name, IP address, GID, Legic-
no., etc.</td></tr>
<tr><td>☐ Employee photo</td><td>Portrait photo posted by employee (intranet, telephone list, social network platform, etc.)</td></tr>
<tr><td>☒ Private contact data and identification data</td><td>Name and surname, sex, address, email, fixed or mobile telephone number, date/place of birth, identification
numbers, nationality, etc.</td></tr>
<tr><td>☐ Conntractual data</td><td>Products purchased, financial services, contract date, purchase price, extras, warranties, etc.</td></tr>
<tr><td>☐ Data related to personal and professional circumstances and</td><td>Data related to partner or children, marital status, portrait photo, honorary post, position data, career, employment</td></tr>
</table>

	characteristics	period, tasks, activities, analysis of file

		entries, entry and exit data, qualifications, measurements / evaluations, etc.	
	☐ Payment and management data	Wage group, payroll accounting, special payments, wage garnishments, attendance times, justifications of absence, etc.	
	☐ Creditworthiness and financial data	Payment habits, balance, commercial agency data, ratings, financial circumstances, bank account, credit card number, etc.	
	☐ Sensitive data	Racial or ethnical origin, political opinions, religious or philosophical beliefs, trade union affiliation, genetic data, biometric data for the sole purpose of identifying individuals, data related to health or to sex life or preferences.	
	☐ Crimes/ offences	Data referring to crimes, offences or suspected crimes or offences.	
PARTIES	**INTERESTED PARTIES**	**DESCRIPTION**	**EXAMPLES**
	☒ Employees	Employees from the respective Group company (in business unit terms)	E.g., employees, trainees, applicants and former employees
	☐ Group employees	Employee from other Group companies (in terms of REVIEW RANK Group members, but not business units)	E.g., REVIEW RANK-USA, ASIA, employees, etc.
	☐ Partner company employees	Employees from a supplier, joint-venture, temporary work agency	E.g., IT services employees, joint venture employees, temporary workers
	☒ Clients	Any person who has a commercial relationship (with the respective business unit)	E.g., Clients.
	☐ Other business partners	Any person (natural or corporate) who has a commercial relationship (with the respective business unit), except	E.g., suppliers, importers or service providers, agents, free-lance

		clients	workers, etc.

	☐ Third parties	Any person who does not have a commercial relationship with the respective Group company (responsible business unit)	E.g., visitors, guests, related parties
	☐ Underage persons	Persons under 13	