Data Processing Agreement

Last updated: 6 Jan 2026

SECTION I

Clause 1

Purpose and scope

1. The purpose of Data Processing Agreement (the "DPA") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 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 repealing Directive 95/46/EC (General Data Protection Regulation).
2. The controllers and processors listed in Annex I have agreed to this DPA in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.
3. This DPA applies to processing personal data as specified in Annex I.
4. Annexes I to III are an integral part of this DPA.
5. This DPA is without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.
6. This DPA does not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2

Interpretation

1. Where this DPA uses the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. This DPA shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 3

Hierarchy

In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 4

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of the processing for which the personal data is processed on behalf of the controller, are specified in Annex I.

Clause 5

Obligations of the Parties

5.1. Instructions

1. The processor shall process personal data only on documented instructions from the controller unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
2. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

5.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I unless it receives further instructions from the controller.

5.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex I.

5.4. Security of processing

1. The processor shall at least implement the technical and organizational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risks involved for the data subjects.

2. The processor shall grant members of its personnel access to the personal data undergoing processing only to the extent strictly necessary for implementing, managing, and monitoring the contract. The processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.5. Sensitive data

The processor's services are not designed or intended for sensitive data. The controller shall not submit any sensitive data to the processor's services. If the controller submits sensitive data to the services despite this prohibition, the controller does so at its own risk and the processor shall have no liability whatsoever for such sensitive data.

5.6. Documentation and compliance

1. The Parties shall be able to demonstrate compliance with this DPA.
2. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this DPA.
3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by this DPA at reasonable intervals or if there are indications of non-compliance, provided that such audits shall be conducted during normal business hours, with at least thirty (30) days' prior written notice, and shall not unreasonably interfere with the processor's business operations. The controller shall bear all costs associated with any audit, including the processor's reasonable costs for time and resources expended in connection with such audit. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
4. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice. Audits shall be limited to once per calendar year unless required by a supervisory authority or following a personal data breach. The controller shall ensure that any independent auditor is bound by confidentiality obligations and shall not be a competitor of the processor.
5. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

5.7. Use of sub-processors

1. The processor has the controller's general authorization for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes to that list through the addition or replacement of sub-processors at least 20 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned

sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. If the controller does not object in writing within ten (10) days of receiving such notice, the controller shall be deemed to have approved the sub-processor. Any objection must be based on reasonable grounds relating to data protection.

2. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract that imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to this DPA and to Regulation (EU) 2016/679.
3. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfill its contractual obligations.

5.8. International transfers

1. Any transfer of data to a third country or an international organization by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
2. The controller agrees that where the processor engages a sub-processor in accordance with Section 5.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 6

Assistance to the controller

1. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself unless authorized to do so by the controller. The processor may charge the controller reasonable fees for any assistance provided in responding to data subject requests beyond the first request per data subject per calendar year.
2. The processor shall assist the controller in fulfilling its obligations to respond to the data subject's requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

3. In addition to the processor's obligation to assist the controller pursuant to Section 6(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor. The controller acknowledges that such assistance may be subject to additional fees at the processor's then-current professional services rates.
    - the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    - the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    - the obligation to ensure that personal data is accurate and up to date by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
    - the obligations in Article 32 of Regulation (EU) 2016/679.
4. The Parties shall set out in Annex II the appropriate technical and organizational measures by which the processor is required to assist the controller in the application of this Section, as well as the scope and the extent of the assistance required.

Clause 7

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor. The controller acknowledges that the processor's assistance obligations under this Section 9 are limited to providing information and cooperation reasonably available to the processor, and the processor shall not be liable for any delays or failures in the controller's compliance with its notification obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

7.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

1. in notifying the personal data breach to the competent supervisory authorities/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

2. in obtaining the following information, which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification and must at least include:
    - the nature of the personal data, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    - the likely consequences of the personal data breach;
    - 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, and insofar as it is not possible to provide all this information at the same time, the initial notification shall contain the information then available, and further information shall, as it becomes available, subsequently be provided without undue delay.

1. in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

7.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor has become aware of the breach. Such notification shall contain at least:

1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
2. the details of a contact point where more information concerning the personal data breach can be obtained;
3. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as it is not possible to provide all this information at the same time, the initial notification shall contain the information then available, and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex I all other elements to be provided by the processor when assisting the controller in compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 8

Non-compliance with this DPA and termination

1. Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under this DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this DPA or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with this DPA, for whatever reason.
2. The controller shall be entitled to terminate the contract insofar as it concerns the processing of personal data in accordance with this DPA if:
    - the processing of personal data by the processor has been suspended by the controller pursuant to point (a), and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;
    - the processor is in substantial or persistent breach of this DPA or its obligations under Regulation (EU) 2016/679;
    - the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or to Regulation (EU) 2016/679.
1. The processor shall be entitled to terminate the contract insofar as it concerns the processing of personal data under this DPA where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Section 7.1(b), the controller insists on compliance with the instructions.
2. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so or return all the personal data to the controller and delete existing copies unless Union or Member State law requires the storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA. If the controller does not provide instructions regarding the return or deletion of personal data within thirty (30) days following termination, the processor may delete all personal data without further notice to the controller.

Clause 9

1. The liability of the processor towards the controller under or in connection with this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement. Nothing in this DPA shall be construed to increase the liability of the processor beyond the limits established in the Agreement.

ANNEX I

Description of the processing

Categories of data subjects whose personal data is processed:

- Employees of the Customer
- Customers of the Customer

Categories of personal data processed:

- For employees of the Customer: Name, surname, Username, Role, Email, Logs, In-app analytics.
- For customers of the Customer: Name, surname, Email, Phone number, Reservation details, ID Information, Visit purpose, Room number, Checkin time/ checkout time, Group details, Country, Reservation cost, Rates, Notes, Data from PMS data sets.

Nature of the processing:

- As described in the Contract.

Purpose(s) for which the personal data is processed on behalf of the controller:

- Creation of accounts for employees of Customer: role definition, access control lists definition, logs setup and storage, storage of activities.
- Analytics, as defined by the Customer through the use of the Analytics toggle in the App.
- Datasets are imported from PMS systems via APIs provided by the Customer.
- Dematerialization of datasets imported from PMS systems: separation of unnecessary personal data categories, destruction of unnecessary personal data categories.
- Scheduling housekeeping, a live feed of housekeeping.
- Manage linen change, minibar, repair jobs, and amenities.
- Mobile Housekeeping training and housekeeping checklists.
- Communicate tasks & updates to employees.
- Housekeeping dashboard analytics.
- Hotel Maintenance and cost optimization.
- Room service management.
- Definition and implementation of Standard Operating Procedures.
- Task management and to-do lists.
- Guest relations management.
- Lost and found management.
- Guest feedback and analytics.

Duration of the processing:

- As described in the Contract.

ANNEX II

Technical and organizational measures, including technical and organizational measures to ensure the security of the data

Flexkeeping has deployed an IT security policy that addresses the following:

- Data integrity and confidentiality;
- Security of IT equipment;
- Protection against viruses, trojans, malware;
- Security measures regarding databases;
- Back-up of data, recovery measures, provisions for periodic testing of back-ups;
- Security monitoring;
- Security incident management;
- Change Management;
- Classification of data;
- Inventory of equipment and software;
- Physical security;
- Disaster recovery;
- Business Continuity.

Flexkeeping:

- Has signed a Data Processing Annex with all employees and an internal policy for the processing of personal data as an annex to the Internal Regulations.
- Ensures the continuous training of all persons involved in the processing of personal data.
- Has implemented firewall technologies to limit security risks.
- Do not use production data in test, development, and pre-production environments.
- Ensures the secure transmission of Personal Data inside or outside the internal network using encryption technologies so that it is not intelligible.
- Has installed antivirus programs and intrusion detection systems on computer systems that are updated regularly.
- Continuously reviews the software and hardware used to detect and resolve vulnerabilities and defects.
- Part of the Internal Data Processing Policy ensures that only those employees who need to carry out the processing of Personal Data are authorized to do so. The authorization for access to the information systems containing Personal Data will be granted according to the principles of "need to know" and "minimum privileges."
- Through its user access policy, ensures that only identified and logged-in authorized users can access the systems that manage personal data. Each authorized user has only one username.

- Continuously reviews the access rights of Authorized Users to personal data and system components containing Personal Data. Access rights will be deactivated if they are not used for at least six months, except for those that have been authorized exclusively for management and technical support. Access rights will also be disabled if the Authorized User is disqualified or dis-authorized to access computer systems or to process Personal Data.

Flexkeeping has established through the IT Security Policy explicit requirements for strong passwords:

- passwords should not be disclosed to others, including management and system administrators;
- user-generated passwords cannot be distributed through any channel (using oral, written, or electronic distribution, etc.);
- passwords must be changed if there are indications that the passwords or system may have been compromised – in this case, a security incident must be reported;
- strong passwords should be selected as follows:
    - use of at least twelve characters;
    - use of at least one numeric character;
    - use of at least one uppercase and at least one lowercase alphabetical character;
    - using at least one special character;
    - a password must not be a dictionary word, from a dialect or jargon from any language, or any of these words written back;
    - passwords should not be based on personal data (e.g., date of birth, address, name of a family member, etc.);
    - The last three passwords cannot be re-used;
- passwords must be changed every three months;
- the password must be changed at the first logon to a system;
- passwords should not be stored in an automated login system (e.g., macro or browser);
- passwords used for private purposes should not be used for business purposes.

Flexkeeping:

- Monitors access to production environments containing personal data to record the link between access and individual users and access to personal data.
- Stores all physical environments containing Personal Data on-site in a room with restricted physical access to Authorized Users.
- Ensures the secure destruction of personal data through secure erasure procedures to make all Personal Data unrecoverable.
- Ensures the transfer of paper documents containing Personal Data in sealed envelopes and personally handed over to the Authorized User.
- Ensures the training and education of Authorized Users regarding the correct rules of conduct to be adopted for the protection of Character Data.

- Has equipped its premises for the processing of Personal Data with intrusion detection systems (cameras) that are operational 24/7.

The building in which FLEXKEEPING operates has detection/protection systems against fire, lightning, and water damage. These systems work 24/7. Flexkeeping has implemented secure code development policies and best practices using Secure Development Lifecycle (SDL) principles. Flexkeeping has implemented a procedure for analyzing and reporting security breaches.

ANNEX III

List of sub-processors

- Amazon Web Services EMEA Sàrl
    - Description of the processing: Hosting and backup.
- Atlassian, Inc.
    - Description of the processing: project and task management.
    - The transfer mechanism of personal data is the adequacy decision taken by the European Commission in regard to the EU-US Data Privacy Framework.
- Freshdesk, Inc.
    - Description of the processing: customer support.
    - The transfer mechanism of personal data is the adequacy decision taken by the European Commission in regard to the EU-US Data Privacy Framework.
- Creatriks d.o.o.
    - Description of the processing: platform provision, support and incident management.
- Flexkeeping Australia Pty Ltd
    - Description of the processing: support and incident management