Appendix to General Terms and Conditions

Data Processing Agreement

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE OF THE AGREEMENT 1
2. DEFINITIONS 1
3. PROCESSING OF PERSONAL DATA 1
4. INSTRUCTIONS 2
5. SUB-PROCESSORS 2
6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES 2
7. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES 3
8. SECURITY AND CONFIDENTIALITY 3
9. PERSONAL DATA BREACH 3
10. ASSISTANCE TO THE CUSTOMER 4
11. AUDIT 4
12. TERM AND TERMINATION 4
13. MISCELLANEOUS 5
SUB-APPENDIX 1 – SPECIFICATION OF THE PROCESSING 6
SUB-APPENDIX 2 – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES 8
SUB-APPENDIX 3 – PRE-APPROVED SUB-PROCESSORS 9

1. BACKGROUND AND PURPOSE OF THE AGREEMENT

This data processing agreement (the "Agreement") forms an appendix to the general terms and conditions (the "General Terms and Conditions") governing the provision of services (the "Services") between the Supplier and the Customer. The terms "the Supplier", "the Customer" and "the Parties" have the meaning set out in the General Terms and Conditions. The Agreement governs the Supplier's processing of personal data on behalf of the Customer in connection with the Services and has been entered into in order to satisfy the requirements of Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR").

In the event of any conflict between the Agreement and the General Terms and Conditions, the Agreement shall prevail in matters relating to the processing of personal data. Other matters shall be governed by the General Terms and Conditions, which shall also apply to the Agreement.

Further details of the Processing are set out in Sub-Appendix 1 (Specification of the Processing). In the event of any conflict between the Agreement and Sub-Appendix 1, Sub-Appendix 1 shall prevail in matters relating to the nature and scope of the specific Processing.

2. DEFINITIONS

In the Agreement, the following terms shall have the meanings set out below. Other terms used in the Agreement with an initial capital letter shall have the meaning set out in the General Terms and Conditions or in the GDPR.

- "Processing", "Personal Data", "Controller", "Processor", "Personal Data Breach", "Data Subject" and "Third Country" have the meaning set out in Article 4 of the GDPR.
- "Data Protection Legislation" means the GDPR, the Swedish Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation, as well as other applicable laws and binding decisions from the competent supervisory authority concerning the processing of personal data, as in force from time to time.
- "Customer Data" has the meaning set out in the General Terms and Conditions.
- "Sub-processor" means a processor engaged by the Supplier to carry out the Processing, in whole or in part, on behalf of the Customer.

3. PROCESSING OF PERSONAL DATA

The Supplier is the Processor and the Customer is the Controller in respect of the Processing carried out under the Services. The Supplier shall Process Personal Data solely for the purpose of providing the Services and only in accordance with the Customer's documented instructions as set out in this Agreement and Sub-Appendix 1.

The subject matter, nature, duration and purpose of the Processing, as well as the categories of Data Subjects and the categories of Personal Data, are set out in Sub-Appendix 1.

The Customer is responsible for ensuring that there is a legal basis under the Data Protection Legislation for the Processing and that the instructions provided by the Customer to the Supplier comply with the Data Protection Legislation. The Customer is further responsible for safeguarding the rights of Data Subjects, for notifying Personal Data Breaches to the supervisory authority to the extent such obligation rests with the Customer, and for ensuring that persons Processing Personal Data under the Customer's authority do so only in accordance with the given instructions.

The Supplier undertakes to maintain a record of the categories of Processing carried out on behalf of the Customer in accordance with Article 30(2) of the GDPR.

4. INSTRUCTIONS

The Supplier may only Process Personal Data in accordance with the Customer's documented instructions. The Agreement, including the Sub-Appendices, together with the General Terms and Conditions, constitute the Customer's complete instructions at the time of entering into the Agreement. During the term of the Agreement, the Customer may issue further written instructions to the extent required to comply with the Data Protection Legislation.

If the Supplier considers that an instruction infringes the Data Protection Legislation, the Supplier shall without undue delay notify the Customer in writing. The Supplier is entitled to suspend the execution of such instruction until the Customer has confirmed or amended it.

For the handling of instructions or changes that are not required by laws to which all or the majority of the Supplier's customers are subject, the Supplier is entitled to reasonable compensation in accordance with the price list in force from time to time. The Supplier shall notify the Customer of such compensation in advance, and the Customer shall approve the charge before the work commences. If the Customer does not approve the charge, the Supplier may **terminate** the affected Service subject to a reasonable notice period.

5. SUB-PROCESSORS

The Customer hereby gives the Supplier general prior authorisation to engage Sub-processors for the provision of the Services. Pre-approved Sub-processors are listed in Sub-Appendix 3. An up-to-date list of engaged Sub-processors, including information on the location of the Processing, is published at https://caspeco.com/gdpr/.

The Supplier shall notify the Customer in writing at least thirty (30) days before engaging a new Sub-processor or replacing an existing Sub-processor. Such notification shall be given by updating the list on the website referred to above and, if the Customer so requests, by direct written notice or an equivalent subscription service.

The Customer is entitled, within thirty (30) days of the notification, to object in writing to the change on legitimate grounds relating to the protection of Personal Data. If the Supplier is unable to accommodate the Customer's legitimate objection, the Customer is entitled to terminate the affected Service(s) in writing subject to the notice period set out in the General Terms and Conditions. If the Customer neither approves nor objects within the stated period, the Sub-processor shall be deemed approved.

The Supplier shall enter into a written agreement with each Sub-processor imposing on the Sub-processor data protection obligations that are substantially equivalent to those set out in this Agreement, in particular the requirements of Article 28(3) of the GDPR. The Supplier shall be liable to the Customer for the Sub-processor's performance of its obligations in the same manner as for its own undertakings.

6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

As a general rule, Personal Data shall be Processed within the EU/EEA. The Supplier may only transfer Personal Data to, or allow access from, a country outside the EU/EEA if (i) the country is covered by an adequacy decision of the European Commission, (ii) the transfer is made on the basis of the European Commission's Standard Contractual Clauses or binding corporate rules, or (iii) another valid basis for transfer under Chapter V of the GDPR exists.

Where required, the Supplier shall carry out a transfer impact assessment of the level of protection in the recipient country and implement such supplementary technical, organisational and contractual safeguards as are necessary to ensure a level of protection essentially equivalent to that within the EU/EEA. The Supplier is entitled to enter into

Standard Contractual Clauses with Sub-processors on behalf of the Customer.

If the legal basis for an ongoing transfer ceases to apply, the Parties shall without undue delay cooperate to identify an alternative transfer mechanism or supplementary safeguards. If such measures cannot be implemented within a reasonable time, the transfer shall be suspended.

If the Supplier receives a binding request from a public authority in a Third Country to disclose Personal Data, the Supplier shall, unless prohibited by applicable law, without undue delay notify the Customer and take reasonable legal measures to limit the disclosure.

7. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Supplier shall implement appropriate technical and organisational security measures in accordance with Article 32 of the GDPR to ensure a level of security appropriate to the risk associated with the Processing. A general description of the Supplier's security measures is set out in Sub-Appendix 2. The Supplier is entitled to update the security measures from time to time, provided that the level of protection is not materially diminished.

For Services that involve card handling, the Payment Card Industry Data Security Standard (PCI DSS) applies to the extent relevant. The Customer is responsible for keeping itself informed of, and complying with, the rules and procedures applied from time to time by banks and other parties with which the Supplier cooperates in providing the Services.

Within its own system and sphere of control, the Customer is responsible for the handling of login credentials, transaction information and other aspects of data security. The Customer shall promptly notify the Supplier upon suspicion of any breach of data security on the Customer's side.

Documentation of the Supplier's technical and organisational security measures shall be made available without undue delay upon the Customer's written request.

8. SECURITY AND CONFIDENTIALITY

The Supplier shall ensure that persons authorised to Process Personal Data under the Agreement have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Supplier shall further ensure that access to Personal Data is limited to those persons who need such access in order to perform their duties.

The Supplier may not, without the Customer's consent or a basis in law or a binding decision of a public authority, disclose Personal Data to any third party. If the Supplier is required to disclose Personal Data on the basis of law or a decision of a public authority, the Customer shall, unless prohibited, be notified before the disclosure is made.

9. PERSONAL DATA BREACH

The Supplier shall, without undue delay and at the latest within seventy-two (72) hours of becoming aware of a Personal Data Breach, notify the Customer in writing. To the extent the information is available, the notification shall contain:

(a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned;

(b) the name and contact details of the Supplier's data protection officer or other point of contact from whom further information can be obtained;

(c) a description of the likely consequences of the Personal Data Breach; and

(d) a description of the measures the Supplier has taken or proposes to take to address the Personal Data Breach and, where appropriate, to mitigate its adverse effects.

Where it is not possible to provide all of the information set out above at the same time, the information may be provided in phases without undue further delay. The Supplier shall document all Personal Data Breaches and, upon the Customer's written request, make the documentation available.

The Supplier shall promptly take appropriate remedial measures to prevent or mitigate the potential adverse effects of the Personal Data Breach and, where necessary, cooperate with the Customer and the competent supervisory authority.

10. ASSISTANCE TO THE CUSTOMER

Taking into account the nature of the Processing and the information available to the Supplier, the Supplier shall reasonably assist the Customer in fulfilling its obligations under Articles 32–36 of the GDPR regarding the security of Processing, notification of Personal Data Breaches, data protection impact assessments and prior consultation with the supervisory authority.

The Supplier shall further, taking into account the nature of the Processing, assist the Customer by appropriate technical and organisational measures in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR (information, rectification, erasure, restriction, data portability and objection). If a Data Subject contacts the Supplier directly, the Supplier shall without undue delay forward the request to the Customer.

Assistance under this clause shall be provided without undue delay. The Supplier is entitled to reasonable compensation in accordance with the price list in force from time to time for assistance that goes beyond what follows directly from the Supplier's own obligations under the Data Protection Legislation. The point of contact at the Supplier for the Customer's requests for assistance is the Supplier's data protection officer, or another function designated by the Supplier.

11. AUDIT

The Supplier shall make available to the Customer the information reasonably required to demonstrate compliance with the obligations under Article 28 of the GDPR, and allow for and contribute to audits and inspections conducted by the Customer or by an independent auditor who is not a competitor of the Supplier. The Supplier may fulfil this obligation by providing a current independent audit report (such as SOC2 Type II or ISO/IEC 27001) once per calendar year upon the Customer's written request and subject to appropriate confidentiality. On-site inspections may be conducted on at least thirty (30) days' prior notice if the audit report is insufficient or if there is a well-founded suspicion of a material deficiency; the Customer shall bear the cost unless a material deficiency is established.

12. TERM AND TERMINATION

The Agreement applies for as long as the Supplier Processes Personal Data on behalf of the Customer under the Services. The Agreement shall automatically terminate when the Supplier's Processing of Personal Data on behalf of the Customer has ceased and any erasure or return as set out below has been carried out.

Upon completion of the Processing, upon termination of the Service or the General Terms and Conditions, or upon the Customer's written request, the Supplier shall, at the Customer's choice, either erase or return all Personal Data to the Customer. Unless the Customer specifies otherwise, the Supplier shall erase the Personal Data.

The Supplier is entitled to store Customer Data containing Personal Data for a period of up to three (3) months following the termination of the Service in order to allow the Customer to extract data, unless the Customer requests immediate erasure in writing. The Supplier is further entitled to continue storing Personal Data to the extent required under Union law or the national law of a Member State, but only

for such period and to such extent as the storage is necessary for the relevant purpose.

Upon the Customer's written request, the Supplier shall certify that erasure or return has been carried out. In addition, the provisions on Customer Data set out in the General Terms and Conditions shall apply.

13. MISCELLANEOUS

Amendments and additions to the Agreement shall be in writing in order to be valid. With respect to limitation of liability, choice of law and dispute resolution, the provisions of the General Terms and Conditions shall apply.

SUB-APPENDIX 1 – SPECIFICATION OF THE PROCESSING

This Sub-Appendix specifies the Processing of Personal Data carried out by the Supplier on behalf of the Customer under the Agreement, in accordance with Article 28(3) of the GDPR.

1.1 SUBJECT MATTER AND PURPOSE

The subject matter of the Processing is the Supplier's provision of the Services to the Customer pursuant to the General Terms and Conditions and the specific service agreements entered into between the Parties. The purpose of the Processing is to enable the delivery, operation, support, maintenance and development of the Services, and to fulfil the Supplier's obligations under contract and law.

1.2 NATURE AND DURATION OF THE PROCESSING

The nature of the Processing comprises the collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure by transmission, alignment or combination, restriction, erasure and destruction of Personal Data to the extent required for the provision of the Services.

The Processing is carried out for as long as the Services are provided to the Customer and during any period following the termination of the Services as set out in clause 12 of the Agreement.

1.3 CATEGORIES OF DATA SUBJECTS

The following categories of Data Subjects may be subject to the Processing:

- The Customer's employees and contractors (e.g. service staff, kitchen and bar staff, managers and owners);
- Individuals at the Customer's suppliers and business partners (e.g. staffing consultants, hired temporary staff, performers, supplier contacts);
- Contact persons and technical users at system integration partners (e.g. accounting and payroll consultants, hotel systems/PMS, payment providers and resellers); and
- The Customer's guests (e.g. table bookers, takeaway orderers, hotel guests and participants in loyalty programmes).
- Recipients of digital receipts (private individuals identified by the Customer's guest or customer at the time of purchase so that the receipt can be transmitted digitally via a third-party service, e.g. Kivra users).

1.4 CATEGORIES OF PERSONAL DATA

The following categories of Personal Data may be subject to the Processing:

- Names of the Customer's employees and guests;
- Contact details (such as telephone number, address and email address) of the Customer's employees and guests;
- Login and user data for employees and administrators (e.g. usernames, encrypted authentication credentials, session data, IP address, device information and logs of logins and system activity);
- Role and authorisation data in the Services (role assignment, authorisation level and access scope);
- Personal identity numbers of employees*;
- Date of birth and legal gender of employees;
- Employees' job titles and occupations with the Customer;
- Employees' salary and payment data, such as employment contracts, absence

reporting, account numbers and salary amounts;

- Employment-related documents uploaded to the Services (employment contracts, payslips, certificates, qualifications and other HR documents; information in such documents may in individual cases constitute data concerning health under Article 9 of the GDPR);
- Free-text fields that the Customer chooses to register;
- Photographs of the Customer's employees (for identification in scheduling and staff views);
- Time and attendance data for employees (clock-in/clock-out events, scheduled and actual hours worked, breaks);
- Absence data for employees (absence periods and type of absence; information about the type of absence may in some cases constitute data concerning health under Article 9 of the GDPR);
- Staff register data under Chapter 39, Sections 11–12 of the Swedish Tax Procedure Act (names and times for all persons working at the business premises, irrespective of their employment relationship);
- Sales, tips and performance data linked to individual employees (e.g. sales per waiter, tip distribution and individual turnover statistics);
- Booking data for the Customer's guests (contact details, party size and free-text information provided by the guest, e.g. allergies or other dietary preferences; information on allergies may constitute data concerning health under Article 9 of the GDPR);
- Loyalty and guest profile data (membership, purchase history, point balances and preferences) for guests participating in loyalty programmes or similar;
- Consent and communication preferences (recorded consents, opt-in/opt-out status and choice of communication channels);
- For hotel-related Services: guest linking data between the restaurant and the hotel PMS (room number, stay period and linkage to the hotel guest profile for charging purposes);
- Payment and transaction data and, for Services that involve card handling, such card data as is processed in a PCI DSS-certified environment and which is not visible to the Supplier in plain text;
- Contact and identification data for recipients of digital receipts (personal identity number*, mobile number or email address), as well as the content and metadata of the digital receipt; and
- Other categories of Personal Data that the Customer registers in, or otherwise adds to, the Services.

* Personal identity numbers constitute particularly privacy-sensitive data under Chapter 3, Section 10 of the Swedish Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation.

The Processing is not intended to encompass special categories of Personal Data under Article 9 of the GDPR or data relating to criminal convictions and offences under Article 10 of the GDPR. However, certain data registered by the Customer or the Customer's guests in the Services (such as type of absence, information about allergies in the free-text field of a booking, or content in uploaded HR documents such as medical certificates) may in individual cases constitute data concerning health under Article 9 of the GDPR. The Customer is responsible for ensuring that there is a legal basis under Article 9(2) of the GDPR for such registration and for informing the Data Subjects in accordance with Articles 13–14 of the GDPR.

1.5 LOCATION OF THE PROCESSING

As a general rule, Personal Data is Processed within the EU/EEA. The Supplier operates in Sweden, Norway, Belgium and France, and Personal Data may be Processed in any of these countries. Any transfer of Personal Data to countries outside the EU/EEA shall take place only in accordance with clause 6 of the Agreement and Sub-Appendix 3.

SUB-APPENDIX 2 – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Sub-Appendix describes the technical and organisational security measures implemented by the Supplier in accordance with Article 32 of the GDPR to ensure a level of security appropriate to the risk associated with the Processing.

2.1 MEASURES FOR CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

- Encrypted transmission of Personal Data between the Supplier and the Customer;
- Pseudonymisation or encryption of data when processing for statistical and marketing purposes for external use;
- Access controls ensuring that only persons who require access for their duties have access to Personal Data;
- Multi-factor authentication for logins to the Supplier's systems from external networks;
- Incremental daily backups and full weekly backups;
- Application of the Payment Card Industry Data Security Standard (PCI DSS), to the extent relevant, for Services that involve card handling.

2.2 ORGANISATIONAL MEASURES

- Contractual confidentiality obligations for all of the Supplier's employees;
- Established procedures for incident management, continuity planning and regular security evaluation;
- Training of personnel in data protection and information security.

2.3 UPDATES

A more detailed description of the Supplier's security measures is available at https://caspeco.com/gdpr/. The Supplier is entitled to update the security measures from time to time, provided that the level of protection is not materially diminished.

SUB-APPENDIX 3 – PRE-APPROVED SUB-PROCESSORS

This Sub-Appendix lists the Sub-processors that the Customer pre-approves in accordance with clause 5 of the Agreement.

3.1 CURRENT LIST

An up-to-date list of engaged Sub-processors is published at https://caspeco.com/gdpr/. For each Sub-processor, the list contains information on (i) the Sub-processor's company name and registered office, (ii) the service provided by the Sub-processor, (iii) the country or countries in which the Processing takes place, and, for Sub-processors located in a Third Country, (iv) the legal basis for the transfer.

By entering into the Agreement, the Customer approves the Sub-processors listed on the website referred to above at the time of entering into the Agreement. The addition or replacement of a Sub-processor shall take place in accordance with the procedure set out in clause 5 of the Agreement.

3.2 SUB-PROCESSORS IN THIRD COUNTRIES

For Sub-processors that Process Personal Data in a Third Country, the website also states the legal basis for the transfer (such as an adequacy decision or Standard Contractual Clauses) and the supplementary safeguards applied in accordance with clause 6 of the Agreement.