Kwick
Expense

DATA PROCESSING AGREEMENT

This Data Processing Agreement is entered into by Customer and Kwick Expense AB ("Kwick"), each a "**Party**" and together the "**Parties**".

1. Background

Customer and Kwick have entered into an agreement (the "**Agreement**") regarding an expense management service in the form of a mobile app and web-admin (the "**Service**") pursuant to which Customer is provided access and use of the Service. In providing the Service, Kwick will engage on behalf of Customer, in the processing of Personal Data submitted to and stored within the Service by Customer or third parties with whom Customer transacts using the Service. To ensure the secure, correct, and lawful processing of the Personal Data, the Parties have agreed on the terms and conditions as set forth in this Data Processing Agreement ("**DPA**").

To the extent that any terms of the Agreement conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data), the terms of this DPA shall take precedence.

2. Definitions

Definitions used in the Agreement shall apply in this Data Processing Agreement, unless specified otherwise herein. Capitalised terms in this DPA shall have the meanings given to them below. Unless otherwise stated herein, or clearly follows from the context in which it appears, the term "including" shall mean "including without limitation".

Non-capitalised terms and expressions used in this DPA, e.g. 'data subject', 'controller', 'personal data', 'processing', 'processor', 'third country' etc., shall be construed in accordance with the meaning given to them in the GDPR.

"**Applicable Data Protection Legislation**" shall mean, the privacy and personal data legislation, including but not limited to the 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 ("**GDPR"**), applicable to Kwick in connection with Kwick's processing of personal data as a processor to provide the Service(s) to Customer;

"**EU SCCs**" shall mean the standard contractual clauses for the transfer of personal data to controllers and processors established in third countries, adopted by the European Commission from time to time, the adopted version of which in force at the date of signature of this DPA is that set out in the Annex to the European Commission's Implementing Decision 2021/914 of 4 June 2021, and as may be amended or replaced from time to time;

"**Instruction**" shall mean the documented instruction defining subject matter, duration of processing performed by Kwick under this DPA, including the nature and purpose of processing, the type of personal data, and categories of data subjects as described in **Annex A** of this DPA, or as amended during the term of this DPA;

"**Processor Group**" shall mean Kwick and any entity which controls, is controlled by, or is under common control with, Kwick;

"**Sub-processor**" shall mean any third-party data processor engaged by Kwick, including entities from the Processor Group, who receives Personal Data from Kwick for processing on behalf of Customer and in accordance with Customer's instructions (as communicated by Kwick) and the terms of its written subcontract.

3. Roles and ownership of Customer Data

The Customer shall be regarded as a controller of all personal data processed on behalf of the Customer in accordance with its Instructions. Kwick shall be considered a processor of the personal data processed on behalf of the Customer. Kwick may only process the Customer's personal data for the purpose and to the extent it is necessary for the fulfilment of Kwick's obligations under this DPA or the Agreement.

Without prejudice to processing of personal data that is carried out in accordance with this DPA, in the event that Kwick infringes the Applicable Data Protection Legislation by determining the purposes and means of processing (e.g. by processing the personal data in violation of the Instruction), Kwick will be regarded as the controller in respect of that processing. It should be noted that Kwick, under the aforementioned circumstances, will be fully liable as the controller for such processing under the Applicable Data Protection Legislation including in relation to any sanctions under the said provisions.

As between the Parties, all Customer Data processed under the terms of this DPA and the Agreement shall remain the property of Customer, irrespective if the Customer is considered to be a controller of the personal data.

4. Undertakings of the Parties

Kwick undertakes to:

a) Only process personal data in accordance with Applicable Data Protection Legislation and the Customer's Instructions, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Applicable Data Protection Legislation; in such a case, Kwick shall inform the Customer of that legal requirement before processing the personal data, unless such information is prohibited by the Applicable Data Protection Legislation on important grounds of public interest;

b) Ensure that only such employees (of Kwick or its sub-processors) which must have access to the personal data in order to meet Kwick's obligations under this DPA shall have access to the personal data processed on behalf of the Customer, and that such employees have received appropriate training and instructions regarding processing of personal data as well as committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) Taking into account the nature of the processing, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with GDPR Article 32 (and as a minimum the security measures further described in the Instruction) and assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in the Applicable Data Protection Legislation. In the event that Kwick receives a data subject request directly from a data subject, it shall, unless prohibited by law, direct the data subject to Customer (to the extent Kwick is able to associate the data subject with Customer);

d) Assist the Customer in ensuring compliance with the obligations pursuant to GDPR, Articles 32 to 36 (e.g., assisting the Customer in case of data breach, when conducting a data protection impact assessments and prior consultations) considering the nature of the processing and the information available to Kwick;

e) Make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the Customer or another third party mandated by it, in accordance with Section 6; and

f) Otherwise comply with the Applicable Data Protection Legislation in its daily business.

If the Customer gives new or changed instructions during the contract period and such instructions result in additional costs for Kwick, the Customer shall reimburse Kwick for each such cost.

The Customer undertakes as controller to abide by its obligations under Applicable Data Protection Legislation.

The Customer undertakes not to intentionally give instructions that would constitute an infringement of Applicable Data Protection Legislation. Kwick shall immediately inform the Customer, if, in its opinion, a Customer instruction infringes the Applicable Data Protection Legislation. In such event, Kwick is entitled to refuse processing of personal data that it believes to be in violation of any law or regulation.

5. Use of Sub-processors

The Customer hereby confirms its general written authorisation for Kwick's use of the Sub-Processors listed at https://kwick.io/sub-processors in accordance with Article 28 of the GDPR and equivalent requirements in other Applicable Data Protection Legislation to assist Kwick in providing the Service and processing personal data, provided that such Sub-processors:

i) agree to act only on Kwick's instructions when processing the personal data, which instructions shall be consistent with Customer's processing instructions to Kwick;
ii) agree to protect the personal data to a standard consistent with the requirements of this DPA, including implementing and maintaining appropriate technical and organisational measures to protect the personal data they process consistent with the security standards described in **Annex B** to this DPA, as applicable.

Kwick shall remain liable to Customer for the subcontracted processing services of any of its Sub-processors under this DPA. Kwick shall also remain the Customers sole point of contact.

Should Kwick decide to engage a Sub-processor, it shall notify the Customer thirty (30) days in advance through the User Account or via e-mail to the Customers appointed contact. The Customer may object to any proposed Sub-processor on reasonable grounds within ten (10) days following the notification. In such event, the Parties shall negotiate in good faith a solution to Customer's objection. If the Parties cannot reach resolution within twenty (20) days of Kwick's receipt of

Customer's objection, Kwick will either (a) instruct the Sub-processor to not process Customer's personal data, in which event this DPA shall continue unaffected, or (b) allow Customer to terminate this DPA and any related services agreement with Kwick immediately and provide it with a pro rata reimbursement of any sums paid in advance for Services to be provided, but not yet received by Customer as of the effective date of termination.

6. Audit

The Customer shall have the right to perform audits of Kwick's processing of the Customer's personal data (including such processing as may be carried out by Kwick's Sub-processors, if any) in order to verify Kwick's, and any Sub-processor's, compliance with this DPA. The right to perform audits and inspections shall also include a right to receive relevant information upon request and without the Customer staff being physically present at Kwicks' site.

Customer may upon request conduct an audit of Kwick under Applicable Data Protection Legislation. Notice shall be given with at least thirty (30) days' advance in writing to privacy@kwick.io. Such audit shall be conducted no more than once during any twelve-month period and shall be conducted during normal business hours with reasonable duration, and not to interfere with Kwick's operations.

Kwick will provide to the Customer's personnel or its hired consultants, its internal or external auditors, inspectors, and regulators reasonable access to the parts of facilities where Kwick is carrying out processing activities, to personnel, and to data and records (including tools and procedures) relating to the processing. The Customer's auditors and other representatives shall comply with Kwick's reasonable work rules, security requirements and standards when conducting site visits. No audit shall involve access to any data relating to any other Kwick customer or to systems or facilities not involved in the processing of personal data for Customer and in no event shall an audit cause Kwick to violate its confidentiality obligations to any third party.

Customer shall be responsible for all costs and expenses relating to an audit conducted under this Section 6, including for any time Kwick expends on such audit at Kwick's then-current professional services rates. Any report generated in connection with such an audit shall be considered Kwick's Confidential Information and shall be promptly provided to Kwick.

Notwithstanding the aforesaid, any supervisory authority shall always have direct and unrestricted access to Kwick's premises, data processing equipment and documentation in order to investigate that Kwick's processing of the personal data is performed in accordance with the Applicable Data Protection Legislation. In the event of a conflict between the audit terms in this Section 6 and the audit terms in the EU SCC, the audits terms in the EU SCC shall control. Nothing in this Section 6 modifies or affects any supervisory authority's rights under the EU SCC.

7. International personal data transfers

Customer acknowledges that Kwick may process personal data in countries that are outside of the EU/EEA. Such transfer shall take place on the basis of (i) that the country has received an adequacy decision from the European Commission, or if not applicable, on the basis of (ii) the EU SCC. If neither (i) nor (ii) is applicable, the Parties agree to work in good faith without undue delay to implement an appropriate transfer mechanism authorised under Applicable Data Protection Legislation.

EU SCCs

Where Kwick processes personal data that is subject to the GDPR in a country that has not received an adequacy decision from the EU Commission, the Parties hereby incorporate the EU SCCs by reference. The Parties are aware of that an export of personal data outside EU/EEA, in addition to conclusion of EU SCC, may require that Kwick must provide supplementary measures that are necessary to bring the level of protection of the personal data in the recipient country to the EU standard of essential equivalence and provide Customer certain guarantees of compliance regarding such export outside EU/EEA.

Where the EU SCCs apply, they will be deemed completed as follows:

i) Module 1 (controller to controller) will apply where Customer is a controller of Customer Data and Kwick is a controller of Customer Data; Module 2 and Module 4 (controller to processor and processor to controller) will apply where Customer is a controller of Customer Data and Kwick is a processor of Customer Data;
ii) in Clause 7, the optional docking clause will not apply;
iii) in Clause 9(a), Option 2 "General Written Authorisation" will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5 of this DPA;
iv) in Clause 10, module 4 will not apply;
v) in Clause 11, the optional will not apply;
vi) in Clause 17, the EU SCCs will be governed by the laws provided in the Agreement;
vii) in Clause 18, disputes shall be resolved before the courts provided in the Agreement;
viii) Annex I.A, I.B and Annex II of the EU ECC shall be deemed completed with the information set out in Annex A and Annex B to this DPA. Annex III of the EU SCC shall be deemed completed with the information set out in https://kwick.io/sub-processors.

Nothing in the interpretations in this Section 7 is intended to conflict with either Party's rights or responsibilities under the EU SCCs and, in the event of any such conflict, the EU SCCs shall prevail.

8. Renumeration

The remuneration for Kwick's undertakings under this Agreement shall, unless otherwise stated in this DPA, be included in the remuneration paid by the Customer under the Agreement. Thus, unless stated herein, Kwick shall not be entitled to additional remuneration based on this DPA.

9. Security breach management and notification

If Kwick becomes aware of any unlawful access to any Customer Data stored on Kwick's equipment or in Kwick's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data ("**Security Breach**"), Kwick will promptly, and no later than 72 hours from awareness: (a) notify Customer of the Security Breach; (b) investigate the Security Breach and provide Customer with information about the Security Breach; and (c) in co-operation with Customer take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

Customer agrees that;

i) An unsuccessful Security Breach attempt will not be subject to this Section 9. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer Data or to any of Kwick's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

ii) Kwick's obligation to report or respond to a Security Breach under this Section 9 is not and will not be construed as an acknowledgement by Kwick of any fault or liability with respect to the Security Breach.

Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's technical or administrative contacts by any means Kwick selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information to Kwick at all times.

10. Return and destruction of Customer Data

Customer may export or download its Customer Data before termination of Customer's access to the Service. Upon Customer's written request, Kwick will make available to Customer the ability to export or download its Customer Data after termination of the Agreement or a User account subject to the terms set forth in the Agreement. Upon termination or cancellation, Kwick will delete the Customer's Customer Data from Kwick's servers within 3 months of the termination of the Agreement or the cancellation of a User Account.

11. Limitation of liability

Each Party shall indemnify and hold the other Party harmless in the event of damages that is attributable to the first-mentioned Party processing, or given Instruction, of personal data in breach of the DPA or Applicable Data Protection Legislation.

Customer acknowledges and agrees that Kwick's total liability for all claims from Customer arising out of or related to this DPA shall apply in aggregate for all claims under this DPA. The aggregate liability of Kwick in respect of the indemnity set out in this Clause 11 shall in no event exceed an amount equivalent to 100 % of the fees paid by the Customer for the Services in the 12 months prior to the event giving rise to the claim.

Notwithstanding the liability set out in this Clause 11, neither Party shall be liable for any indirect or consequential damages of the other Party, such as (but not limited to) loss of revenue, loss of profit, loss of opportunity, loss of goodwill. For the avoidance of doubt, administrative fines are imposed on the Party in breach of its obligations and, in consequence, neither party will bear the other Party's administrative fines.

This section shall not be construed as limiting the liability of either Party with respect to claims brought by data subjects, where article 82 GDPR shall apply, or under the EU SCCs' Clause 12.

12. Term and termination

This DPA constitutes an appendix to the Agreement and becomes effective in connection therewith, as stated in *Appendix 1 – Terms and Conditions for Kwick Expense*. Unless terminated earlier (i) due to a material breach of the terms of this DPA, or (ii) in accordance with Section 5, this DPA shall remain in force until the termination or expiration of the Agreement, whereupon it shall terminate automatically without further notice.

13. Miscellaneous

Neither Party may assign its rights or obligations under this DPA without the prior written consent of the other Party.

Section 13 of the Agreement shall apply to any dispute, controversy or claim arising out of or in connection with this DPA, or the breach, termination, or invalidity thereof.

Kwick Expense

Annex A – Instruction

Contact details	Title: COO E-mail: privacy@kwick.io
Nature and purpose of the processing, including processing activities	Kwick will process personal data in the course of providing Service(s) under the Agreement, which may include operation of a cloud-based customer services platform, including support and guidance, updates, and improvements to the agreed services, generate statistics and, if applicable, for the fulfilment of Customers' and Kwick's legal obligations and undertakings as stated in the Agreement or the DPA. Kwick may also process personal data in order to detect and prevent misuse for the safety of the Service, the User, or the Customer, and in order to ensure technical functionality and security. The personal data processed will be subject to the following basic processing activities: - Transferring, receiving, organising, storage and administering Customer Data, including Transaction Information and Enriched Information provided by Customer, User or a third-party; - Aggregation and anonymisation of Customer Data, including Transaction Information and Enriched Information; - Disclosure and transfer to the Customer, User or other third-party as instructed by Customer through transmission, reading and production as well as storage of Customer Data, including Transaction Information and Enriched Information; - Disclosure to the Customer by transfer of personal data and aggregated data - Transfer to Kwick or its affiliates for processing which Kwick or its affiliates are the controller or otherwise acts as processor for a third-party controller.
Data subjects	Personal data processed during the Service may include the following categories of data subjects: - Employees (including contractors and temporary employees); - Users - Employees of Customers' service providers; - Employees of Customers' merchants; and - any natural person(s) authorized by Customer to use the Service(s).
Categories of personal data	Personal data processed during the Service may include the following categories of personal data: - Personal information (such as name, personal identification number); - Contact information (such as phone number, e-mail address, address, place of employment); - Financial information (such as credit card information, financial transactions, purchase history); - Content (such as photos, images or PDF, digital receipts, delivery notes, invoices, and environmental reports – all which may include sensitive data); - Device information (IP-number, etc); - Aggregated Customer- or User generated data (such as duration of session, number of transactions, password resets) or Non-aggregated Customer- or User generated data (such as the content and context in support cases, chat conversations, security incident logs etc.); and - Communications (such as telephone recordings, voicemail).
Special categories of personal data	Sensitive Data may, from time to time, be included in processing via the Service(s) where Customer or its Users choose to include sensitive data within the Service(s) (for example within the Enriched Information). Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's Users to transmit or process any sensitive data via the Service(s).
Duration of processing	Personal data included in the Customer data will be processed for the duration of the Agreement and DPA on a continuous basis and will be deleted within three (3) months after termination of the Agreement or DPA, or cancellation of an individual User Account. Personal data processed for the fulfilment of Customers' and Kwick's legal obligations will be retained for the duration as required by applicable law.

Kwick
Expense

Annex B – Security standards

Description of the technical and organisational security measures implemented by Kwick:

1. Access Rights
   - Access rights to IT systems and data, and access to buildings and rooms, are only granted to the level of access needed to perform their activities (need-to-know principle).
   - Access rights are granted according to defined role-based permission profiles. The access rights granted are reviewed regularly. Rights that are no longer required are removed immediately.
   - Separation of data is ensured for customer data based on software system management, e.g., through data storage in separate folders.
   - Customer data is pseudonymized to the extent possible.

2. Physical Access Control
   - The company has implemented security measures to ensure restricted access to the building and office. Our building and offices are locked and not open to the public.
   - Our products are operated on hosted servers in data centers that are monitored and staffed 24/7.
   - Data centers are climate-controlled and fireproof, data center electrical power systems are designed to be fully redundant and maintainable without impact to operations.
   - Hosted environments with AWS follow AWS compliance with GDPR, https://aws.amazon.com/compliance/gdpr-center.

3. Communications Security
   - Setup for securing data traffic and communication connections, as well as for monitoring and logging activities in networks, have been established. Firewalls and intrusion detection and prevention systems in place.
   - Measures also include the use of applications, whenever suitable, to facilitate cybersecurity as well as the network and application security.
   - The environment is protected against DDos attacks.
   - Regularly scan for malicious code in the network.
   - All communication to and from users is encrypted with TLS.

4. Backup and Logs
   - All data is stored in three different locations in Sweden.
   - Sensitive data stored at rest is encrypted.
   - Data is backed up once per day.
   - Log retention in Kwick is 24 months.
   - Uploaded files are passed to a virus and malware-scanner before further processing.

5. Measures for staff include to handle malware, viruses, phishing include training, maintaining good cyber hygiene as well as protecting sensitive data and back up.

6. Security audits may be performed by independent third-party auditors whenever new changes are deployed. Internal auditing may include data privacy requirements, such as:
   - Employees to maintain data secrecy, training and education.
   - Data processing procedures.
   - Procedures in case of data breaches.
   - We have also appointed a role (unofficial data protection officer) which entails the same function as a data protection officer (DPO), and we carry out internal auditing of procedures as well as regular review of technical advancements.

7. Disaster Recovery
   Our business continuity management include:
   - Embedding information security continuity into our business continuity management arrangements.
   - Ensuring availability of information processing facilities.

   We verify our established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations, i.e. ambition to re-establish operations after unforeseen events.