18 July 2025

Data Processing Agreement

PREAMBLE

This data processing agreement ("**Data Processing Agreement**") is entered into by and between the Parties (Settly and Client) as indicated in the Order Form and forms an integral part of the Agreement, applying to all agreement(s) under which Settly processes personal data on behalf of Client. All capitalized terms not otherwise defined in this Data Processing Agreement shall have the meaning ascribed to such terms in the Agreement.

Client is deemed to be the controller within the meaning of article 4(7) of the EU General Data Protection Regulation ("**GDPR**") and Settly is deemed to be the processor within the meaning of article 4(8) of the GDPR. Where, in this Data Processing Agreement, reference is made to terms that are defined in the GDPR, such as "**controller**", "**processor**" and "**personal data**", such terms shall have the meanings given to them in the GDPR.

THE PARTIES HAVE AGREED AS FOLLOWS:

1. PROCESSING OBJECTIVES

1.1. Settly undertakes to process personal data on behalf of Client in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, in particular for hosting Client Data on the Application Platform as a Service of Settly, and for all such purposes as may be agreed to subsequently. For the purpose of this agreement Settly shall act as a Processor where client is the Controller of the personal data.

1.2. Within the scope of the Agreement Settly must be able to determine the amount of internal, external and/or anonymous users. For this reason, Settly may process "Authentication Profiles", and their contents insofar necessary for the aforementioned purpose. The impact is kept minimal by not extracting any contents of any database, but only utilizing the necessary information in a hashed form.

1.3. The personal data (to be) processed by Settly under this Data Processing Agreement, and the categories of data subjects to whom the personal data relates, are specified in Appendix 1. The processing of Personal Data shall be limited to the Personal Data that are necessary to deliver the services to the client. The locations of the Processing by the Contractor is limited to those described in the Agreement or Appendix 1.

1.4. Settly shall refrain from making use of the personal data for any other purpose than as mentioned under Section 1.2 or as specified by Client.

1.5. Client shall inform Settly of any processing purposes to the extent not already mentioned in this Data Processing Agreement.

1.6. Settly shall not process any Personal Data for purposes other than that which is strictly necessary for the performance of its obligations under this DPA or the Agreement. The control over the personal data processed pursuant to this Data Processing Agreement and/or other agreements between the Parties rests with Client.

1.7. All personal data processed on behalf of Client shall remain the property of Client and/or the relevant data subjects.

2. PROCESSOR’S OBLIGATIONS

2.1. Settly shall comply with the laws and regulations relating to the protection of personal data in connection with the processing of personal data by Settly, such as the GDPR.

2.2. Settly shall only process the Personal Data strictly in accordance with client's documented instructions given in this Agreement or by any other means during the term of the Agreement. And Settly shall immediately inform client if, in its opinion an instruction infringes the applicable data protection laws.

2.3. At the request of Client, Settly shall furnish Client with all relevant details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement, Client agrees to receiving this information in a reasonable manner such as already existing audit reports, certifications and/or other relevant documents as deemed necessary.

2.4. Settly’ obligations arising under the terms of this Data Processing Agreement also apply to whomsoever processes personal data under Settly’s instructions.

2.5. Settly will provide any reasonably necessary assistance if a data protection impact assessment, or a prior consultation with a supervisory authority, is necessary with respect to the processing of personal data.

3. TRANSMISSION OF PERSONAL DATA

3.1. Client hereby grants Settly permission to process the personal data in countries within the European Economic Area (“**EEA**”). In addition, the Processor may process the personal data in a country outside of the EEA, provided that the country ensures an adequate level of protection of the personal data and complies with other obligations imposed on it under this Data Processing Agreement and the GDPR, including the availability of appropriate (technical and organizational) safeguards, enforceable data subject rights and effective legal remedies.

3.2. A list of the processing locations at the time of entering into this Data Processing Agreement is set out in Appendix 1

4. ALLOCATION OF RESPONSIBILITY

4.1. The authorized processing shall be carried out by Settly within a (semi-)automated environment.

4.2. Settly shall be responsible for the processing of personal data under this Data Processing Agreement, in accordance with the documented instructions of Client.

4.3. Settly is expressly not responsible for other processing of personal data, including but not limited to, the collection of personal data by Client and processing for purposes that are not reported by Client to Settly in writing (i.e. as an amendment to this agreement).

4.4. Client represents and warrants that it has obtained explicit consent and/or another legal basis to process the relevant personal data.

5. SUB-PROCESSORS

5.1. Within the framework of this Data Processing Agreement and the Main Agreement, the Processor may use the services of third parties and/or subcontractors (**“Sub- Processors”**), as contained in Appendix 2. If the Processor wishes to engage new Sub- Processors, the Processor will inform the Controller in advance of the intended changes.

5.2. The Controller can object in writing to the engagement of a new Sub-Processor within fourteen (14) days after the announcement of the intended change, stating reasons. If the Controller does not object within that period, the Controller is deemed to consent to the engagement of a new Sub-Processor.

5.3. If the Controller submits an objection to the engagement of a new Sub-Processor, the Processor may be unable to provide or continue to provide the agreed Services in full. In such a case, the Parties will consult in order to reach an appropriate solution. If the parties are unable to arrive at a solution within thirty (30) days after the announcement of the intended change, the Controller is authorized to terminate the Main Agreement by the date on which the new Sub-Processor will be engaged.

5.4. The Processor will ensure that the engaged Sub-Processor will strictly comply with the same or similar obligations with regard to the processing of personal data as the obligations of the Processor pursuant to this Data Processing Agreement.

6. SECURITY

6.1. Settly shall implement appropriate and sufficient, technical and organisational security measures(no less than the measures described in Appendix 3) prior to and during Processing of any Personal Data to protect the security, confidentiality and integrity of the Personal Data and to protect the Personal Data against any form of accidental, unlawful or unauthorized Processing. In particular, without limitation, Settly shall protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, use or access to Personal Data transmitted, stored or otherwise processed and against any form of unlawful Processing. Settly shall ensure a level of security appropriate to the risks presented by the Processing of Personal Data and the nature of such Personal Data. Such measures shall include, as appropriate:

(i) the ability to ensure the on-going confidentiality, integrity, availability and resilience of Processing systems and services;

(ii) the ability to restore the availability and access to the Personal Data in timely manner in the event of a physical or technical incident;

(iii) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

6.2. Settly will endeavour to ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6.3. Settly operates in accordance with ISO 27001 / ISO 27002, which are deemed to conform to the security requirements considering the current state of the art.

7. PERSONAL DATA BREACHES

7.1. In the event of a personal data breach, within the meaning of the GDPR, Settly will notify Client thereof without undue delay but at least within thirty-six (36) hours upon its discovery by an email to Clients email and any other designated email address.. Settly will use reasonable endeavours to ensure that the provided information is complete, correct and accurate. Client shall then decide whether or not to notify the data subjects and/or the relevant supervisory authorities.

7.2. If required by applicable laws and/or regulations, Settly shall cooperate in notifying the relevant authorities and/or data subjects. Client shall determine whether or not to inform the relevant regulatory authorities and/or the data subjects. Client remains the responsible party for any statutory notification obligations in respect thereof.

7.3. The notification obligation includes, subject to availability at time of reporting, in any event the duty to report the fact that a breach has occurred, and all information required for asssiting Client with its notification obligations, including but not limited to details regarding:

- the (suspected) cause of the breach;
- the contact point where more information can be obtained;
- the approximate number of data subjects and number of personal data records concerned;
- the (currently known and/or anticipated) consequences thereof;

- the (proposed) solution;
- the measures that have already been taken.
- the relevant logs, alerts, indicators of compromise, intelligence and other relevant content that is material to the investigation of the Breach.

Settly shall not make any statement to any third party identifying Client in connection with a Data Breach unless Settly has obtained 's prior written authorization.

8. HANDLING REQUESTS FROM DATA SUBJECTS

8.1. In the event that a data subject submits a request to Settly to exercise his/her rights under applicable privacy laws and regulations, Settly will notify Client within ten days of receiving of such request and Client will be responsible for handling the request. Settly may notify the data subjects of the fact that their requests have been forwarded and will be handled by Client. Where necessary, Settly shall reasonably assist Client in implementing appropriate technical and organisational measures. Settly shall cooperate with Client, at its own expense, to enable Client to respond and comply with reasonable request to (i) the exercise of rights of individuals (such as their right of access, right to rectification, right to object to the Processing of their Personal Data, right to erasure, right to restriction of Processing of their Personal Data and their right to data portability) and (ii) any other correspondence, enquiry or complaint received from an individual, regulatory or any other third party (pursuant to Applicable Data Protection Laws) in respect of Personal Data processed by Settly under this DPA.

9. NON-DISCLOSURE AND CONFIDENTIALITY

9.1. All personal data received by Settly from Client within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties.

9.2. Settly shall treat Personal Data with strict confidence and take all appropriate steps to ensure that disclosure of or access to Personal Data is restricted to its employees, consultants or agents that strictly require such Personal Data to perform the tasks allotted to them by Settly in the performance of Settly's obligations under the Agreement (the "Authorized Persons") and excluding all access to Personal Data which are not strictly necessary for the Authorized Persons to perform its part of the Services. Settly shall ensure that the Authorized Persons who will Process Personal Data:

(i) are aware of and shall comply with the provisions of this DPA;

(ii) are under a duty of confidentiality with respect to the Personal Data no less restrictive than the duties set forth herein prior to any access to the Personal Data. Settly shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement;

(iii) have received appropriate training in relation to the Applicable Data Protection Laws;

(iv) are subject to user authentication and log-on processes when accessing the Personal Data; and

(v) shall only process the Personal Data as necessary for the purposes specified in Appendix 1 and in accordance with Client's instructions.

9.3. This duty of confidentiality will not apply in the event that Client (i) has expressly authorised the provision of such information to third parties, (ii) where the provision of the information to third parties is reasonably necessary taking into account the nature of the instructions and the implementation of this Data Processing Agreement, or (iii) if there is a statutory obligation to provide the information to a third party.

10. AUDIT

10.1. In order to confirm compliance with all points in this Data Processing Agreement and with applicable data protection laws, Client shall be entitled to have audits carried out by an independent third party who is bound to confidentiality.

10.2. The audit will only take place after Client has requested and assessed similar audit reports made available by Settly and provided reasonable arguments that justify an audit initiated by Client. Such an audit is justified when the audit reports provided by Settly give no or insufficient information regarding Settly's compliance with this Data Processing Agreement. The audit initiated by Client will take place no more than once a year and after Client has provided reasonable prior notification (except where such notice would defeat the purpose of the Audit). The Audit shall take place during the regular business hours and under a duty of confidentiality.

10.3. Settly will cooperate in the audit and will make available all reasonably necessary information, including supporting information such as system logs appropriate employees, and any relevant information relating to the processing of the Personal Data, available to client to demonstrate compliance with its obligations laid down in this agreement and Applicable Data Protection Laws.

10.4. The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented by one of the Parties or jointly by both Parties.

10.5. The costs of the audit will be borne by Client, it being understood that the costs for the engaged independent third party will always be borne by Client. Settly shall reimburse the costs of audit incurred by the Client when the audit findings leads to discovery of Non compliance on the part of Settly

11. DURATION AND TERMINATION

11.1. This Data Processing Agreement is entered for the duration set out in the Agreement.

11.2. This Data Processing Agreement may not be terminated for convenience.

11.3. Upon termination of the Data Processing Agreement, Settly shall, at the request of Client, return the personal data to Client and/or shall destroy such personal data, except to the extent the Data Processing Agreement, Agreement or applicable laws and regulations provide otherwise.

11.4. Amendments to this Data Processing Agreement may only be agreed by the Parties in writing.

11.5. Parties shall provide their full cooperation in amending this Data Processing Agreement in the event of any amended privacy laws and regulations or identified changes in processing activities by either Party.

12. RETURN OR DESTRUCTION OF PERSONAL DATA

12. Upon Client's request anytime during the term of the Agreement, Settly shall promptly delete or return any Personal Data(including Personal Data that is processed by Sub-contractors) in accordance with Client's instructions. As soon as it is no longer required for the performance of the Services and at the latest upon the expiration or termination of the Agreement, Settly shall promptly return or delete(at Client’s sole election) all Personal Data processed by Settly or its Sub-contractors. Settly shall certify to Client that all Personal Data has been returned or destroyed in accordance with the foregoing and Client's instructions

13. INDEMNIFICATION

13.1 Settly acknowledges that the obligations set forth in this DPA are essential and that any violation thereof may seriously harm Client. Notwithstanding any limitation of liability provided in the Agreement(if any), Settly shall have full and sole liability for all damages resulting from a failure on its part to comply with the provisions of this DPA. Should any individual to whom the Personal Data relates, a Data Protection Authority or any other regulatory body lodge a claim for compensation against Client that results from the Settly's breach of its obligations under the Applicable Data Protection Laws (a "Claim"), Settly shall assist and intervene in Client’s defence against such Claim upon Client’s request and shall indemnify and hold harmless Client against all costs and damages resulting from such Claim. Client shall give Settly prompt written notice of any such Claim and shall provide all reasonable cooperation in the defence and settlement of such Claim, at Settly's expense.

14. MISCELLANEOUS

14.1 This Data Processing Agreement forms an integral part of the Agreement. All rights and obligations under the, including the limitations on liability and applicable law as stated in Settly’s General Terms and Conditions, apply mutatis mutandis to this Data Processing Agreement.

APPENDIX 1: SPECIFICATION PERSONAL DATA AND DATA SUBJECTS

CATEGORIES OF PERSONAL DATA

Within the framework of the Agreement and on behalf of Client, Settly will process the following categories personal data:

- Please see the details below.

CATEGORIES OF DATA SUBJECTS

The categories of data subjects to whom the personal data relate are:

- Employees of the Client

Client represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate.

The data subjects are employees of the controller. Information will be kept in Settly's database as long as the service requires and in accordance with Settly's Privacy Policy. Deletion (and/or anonymization) of the data can be done on request.

Mandatory information: Full name, email, start date of the employment contract.

Extra information will be processed based on the services that we provide to the employee, which could include:
Gender, family information (children, partner), relationship status, profile picture, country of residence, household, phone number, nationality, date of birth, place of birth, date of birth, residential address, resident permit, employment contract, municipality registration date, flight number, and any other information necessary to provide relocation services.

The categories of the sensitive data will be based on the services provided to the employee. All sensitive data will only be disclosed to the Settly employees assigned to the case and all interactions are logged into Settly's systems.

APPENDIX 2: SUB-PROCESSORS

- Digital Ocean (EU Jurisdiction)Description of the processing: All web servers are provided by DigitalOcean. This includes the full application and information databases. The servers are created under the EU area (using the AMS3 cluster).
- Amazon SES (Amazon Data Services Ireland Limited)Description of the processing: We use Amazon SES to deliver transactional emails related to the use of our web application (eg. reminders, alerts, notifications). First name and email are used on the emails but no other personal data is transferred directly through these emails. Links to activate an account and password reminder requests are sent via these emails. The emails are sent using the Europe (Frankfurt/eu-central-1) cluster.
- Apideck (EU): Apideck provides integration connectors that enable secure communication between our platform and third-party HRIS and ATS systems. Apideck is ISO 27001 and SOC 2 certified. The data transmitted through Apideck is limited to what is permitted via integration-specific permissions and typically includes employee first name, last name, and email address for the purpose of initiating connections. Apideck does not store or persist any personal data; it functions solely as a pass-through connector to facilitate real-time API communication between systems.
- Google Firebase (Google Ireland Limited)Description of the processing: We use Firebase to send push notifications to the user's mobile devices. These notifications may include the first name and the message sent. After the notifications are sent, they are not stored on Firebase.
- Google Suite (Google Ireland Limited)Description of the processing: We use GSuite to email (externally), store and share high level customer data and employee data (eg. name, arrival date, services, start-work date) internally for reporting purposes.
- OpenAI (US): OpenAI's API is used internally to enhance employee productivity by generating response suggestions for incoming client communications. The data sent to the API may include client message content such as names and inquiries. API data may be retained for up to 30 days, after which it will be deleted. OpenAI adheres to all applicable data privacy regulations and signed a DPA with us.
- Pusher (EU Cluster):Description of the processing: We use Pusher to send web-socket notifications from within our web applications. These notifications may include the first name and the message sent. After the notifications are sent, they are not stored on Pusher. The cluster of data is processed within the EU.
- Formstack (US):Description of the processing: We use Formstack to securely request personal data from the employees to conduct visa and tax services. Formstack complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework.
- Zivver (EU) Description of the processing: All sensitive personal information will be shared using Zivver secure email solutions.

- WeFact (EU) Description of the processing: We use WeFact for invoicing. The integration receives name, employee number and service description to generate the invoices sent to our clients.
- Addition to the above subprocessors, Settly B.V. service providers may also be sub processors based on the personal data, main providers, based in the countries that Client requires services to be offered

APPENDIX 3: Settly Technical and Organizational Security Measures

Measures of pseudonymisation and encryption of personal data and Measures for the protection of data during transmission

- All connections to the servers are encrypted using OpenSSL, TLS 1.2, and using a certificate provided by DigiCert, the Mozilla Intermediate cipher suite is used for reference.
- Sessions are stored on cookies encrypted by the backend framework, no principal session data is stored in the user's browser.
- All access to database servers is limited by IP address (from application servers only).
- Access to all servers is protected by SSH keys with password protected authentication.
- Firewalls are in place for all servers.
- All passwords and direct messages are encrypted at rest (provided by 3PSP, using AES-256).

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical):

- High-availability service architecture. [Managed by DigitalOcean] It is possible to recover and restart the services from a backup:
  - Full server provision and DNS propagation: 5:45 hrs
  - Database and assets restore only: 1:30 hrs
- Full server backups are made on a weekly basis. [Managed by DigitalOcean]
- Database servers are backed up daily. [Managed by DigitalOcean]

Note: All physical measures to ensure the availability of the servers are taken by DigitalOcean.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

- PenTesting is conducted on our web and mobile applications by a third party on a yearly basis, following all international information security standards (the provider lists SOC2, PCI DSS, HIPAA, ISC2, ISECOM, EC/COUNCIL, OWASP, ISO 27001 Annex A ISO 27002 as standards followed when conducting tests on Settly's applications).
  - Last pentest date: July 2023.

Measures for user identification and authorisation

- Authentication on Settly's applications is made using email and password.

    - For client accounts (controller’s relocating employees and controller’s HR employees) Settly requires passwords that are 8 characters long and contain at least a number, an uppercase letter and a lowercase letter following FIPS-140 recommendations.
    - For internal Settly employee accounts, the password requirements are 8 characters in length (although in practice at least 30 characters are used) and to contain at least a number, a special char (!@#$&*), an uppercase letter and a lowercase letter.
- Two-factor authentication is implemented and mandatory for internal Settly employee accounts with access to information.
- Two-factor authentication for controller’s HR employees is optional by default and can be made mandatory by an admin. We also offer SSO with Okta.
- Two-factor authentication is optional to activate for controller’s relocation employees
- Throttling of login attempts is based on IP addresses.

Measures for the protection of data during storage

- Each type of account has their own authorisation levels and roles:
    - Employees: Access to only their own information and communications with the Settly team. For group chats it is only possible to read the first name of the members and the messages that are sent.
    - Controller: Access to information of the employees initiated by the controller only and to initiate new employees. It can be segmented per city where the service is provided.
    - Settly Employees:
        - Operations: Multiple roles and levels of access based on the user cases they are in charge of. This can be segmented by companies, cities, products, and single users.
        - Admin: Multiple roles of access based on type of data to access.
- Roles and permissions are reviewed on a weekly basis.
- Every action on the platform (including information opening) by each type of account is logged on the database. The access logs can be traced back to each user independently with IP and User Agent information.

Measures for ensuring physical security of locations at which personal data are processed:
The measures taken by Settly’s sub-processor for servers and databases (DigitalOcean) are:

- DigitalOcean data centers are located in nondescript buildings that are physically constructed, managed, and monitored 24 hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates.
- CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities. All data centers used by DigitalOcean are certified to ISO27001 and have a SOC2 (type 2) statement available. Digital Ocean SOC2 attestation is verified on an annual basis.

(Taken from their DPA: Legal - Data Processing Agreement)

Measures for ensuring events logging

- As stated above, actions on the platform (including information opening) by each type of account are logged on the database. The access logs can be traced back to each user independently with IP and User Agent information.

Measures for ensuring system configuration, including default configuration

- All changes on the system are reviewed and approved by the Product Owner and Engineering Manager.
- Deployment of new releases of code on the systems are tested and accepted by the Product Owner and Engineering Manager.

Measures for internal IT and IT security governance and management

- All access to sub processor platforms is stored on a password management system on which only relevant employees have access to the keys and logins.
- SSH Keys are reviewed on a regular basis
- All access to sub processor platforms is protected by two-factor authentication.

Measures for certification/assurance of processes and products

Settly is currently ISO27001 certified.

Measures for ensuring data minimisation

Given the nature of the services rendered by Settly, clients can - up to a certain level - determine the amount of processed information themselves.

Measures for ensuring data quality and Measures for allowing data portability and ensuring erasure

All data can be extracted in industry-standard formats (csv and/or database dumps).

Measures for ensuring limited data retention

Application of data retention policies as stated on Settly's Privacy Policy.

Measures for ensuring accountability

All employees have a confidential agreement as part of their employment contract and are familiar with our data protection laws. We also emphasize this during our data security sessions.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Based on risk profile (type of data processed) we require our vendors to have a minimum set of organizational and technical controls in place as mandated by ISO27001 and SOC2 (where applicable).

Description of the specific technical and organizational measures to be taken by the processor to be able to provide assistance to the controller.

All data processed by Settly is - by Settly - linkable to individuals. Therefore we can automatically generate exports of all data "belonging to a certain individual". Any request for information shall be handled as a regular support activity.

Settly has a formalized internal information security management system that contains:
a) a formalized information security policy,

b) a - by management - mandated process to verify existence, operation and correctness of this management system and
c) has been certified against ISO27001.