Data Processor Agreement

Between

The Data Controller:

Client data and contact information as specified in the Master Agreement,

and

The Data Processor:

PROMISE ApS

With company ID/VAT number: DK43700839,

and the legal owner of ActionPlanner platform and brand.

Version: V2512

Effective from: January 1, 2026

Background

1. The Data Processor provides one or more software services, including the application 'ActionPlanner' to the Data Controller. When using the application, the Data Controller is responsible for the processing of personal data in the application. The Data processor will process personal data on behalf of the Data Controller and according to the Data Controllers instructions. This Data Processor Agreement sets out the rights and obligations that apply to the Data Processor's handling of personal data on behalf of the Data Controller.

   This Agreement has been designed to ensure the Parties' compliance with Article 28, sub-section 3 of ***Regulation 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)***, which sets out specific requirements for the content of Data Processor Agreements.

2. The Data Processor's processing of personal data shall take place for the purposes of fulfilment of the Parties' Master Agreement.

   The Data Processor Agreement and the Master Agreement shall be interdependent and cannot be terminated separately. The Data Processor Agreement may however – without termination of the Master Agreement – be replaced by an alternative valid Data Processor Agreement.

   This Data Processor Agreement shall take priority over any similar provisions contained in other agreements between the Parties, including the Master Agreement.

3. Two appendices are attached to this Data Processor Agreement. The Appendices form an integral part of this Data Processor Agreement.

   Appendix A of the Data Processor Agreement contains details about the processing as well as the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

   Appendix B of the Data Processor Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

4. Applicability to non-EU jurisdictions: The data protection standards set forth in this Data Processor Agreement meet or exceed the requirements of applicable US state privacy laws, including but not limited to the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and similar state-level data protection legislation.

   Where the Data Controller is established outside the European Union, the protections afforded by this Agreement shall apply to all personal data processed on behalf of the Data Controller, regardless of the data subjects' location.

The rights and obligations of the Data Controller

The Data Controller shall be responsible to the outside world (including the data subject) for ensuring that the processing of personal data takes place within the framework of the General Data Protection Regulation and the Danish Data Protection Act.

The Data Controller shall therefore have both the right and obligation to make decisions about the purposes and means of the processing of personal data.

The Data Controller shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised in law.

The obligations of the Data Processor

Instructions

The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller unless processing is required under EU or Member State law to which the Data Processor is subject; in this case, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.

The Data Processor shall immediately inform the Data Controller if instructions in the opinion of the Data Processor contravene the General Data Protection Regulation or data protection provisions contained in other EU or Member State law.

By entering into this agreement, the Data Controller instructs the Data Processor to process personal data in the following ways:

1. In accordance with applicable law
2. To fulfil the Data Processors' obligations according to the 'Master Agreement', 'Software License Agreement' (the subscription terms to the application 'ActionPlanner') and the Data Controllers' normal use of the application 'ActionPlanner'
3. As specified in this agreement

The Data Processor is obligated to offer the Data Controller an application and related services of the highest quality possible. This obligation is fulfilled by registering how The Data Controller and its employees use the application 'ActionPlanner'. In this registration, data is processed in aggregated and/or pseudonymised form, to operate, maintain, secure, and improve the Services. To the extent such processing involves personal data, it is covered by Appendix A.

Confidentiality

The Data Processor shall ensure that only those persons who are currently authorised to do so are able to access the personal data being processed on behalf of the Data Controller. Access to the data shall therefore without delay be denied if such authorisation is removed or expires, e.g. If a person's employment with The Data Processor ends.

The Data Processor shall ensure that persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

The Data Processor shall at the request of the Data Controller be able to demonstrate that the employees concerned are subject to the above confidentiality.

Security of processing

The Data Processor implements appropriate technical and organisational measures in accordance with Article 32 GDPR to ensure a level of security appropriate to the risk.

The Data Processor has implemented the following measures:

- Access control (least privilege) and multi-factor authentication for administrative access.
- Encryption in transit and at rest (where supported by the underlying services).
- Logging/monitoring and regular backups with the ability to restore availability in a timely manner.

Use of sub-processors

The Data Processor shall meet the requirements specified in Article 28(2) and 28(4) of the General Data Protection Regulation in order to engage another processor (Sub-Processor).

The Data Controller hereby grants the Data Processor general written authorisation to engage and replace sub-processors in accordance with Appendix B.

The Data Processor shall provide prior notice of material changes and give the Data Controller the opportunity to object on reasonable and documented data-protection grounds, as set out in Appendix B.

Transfer of data to third countries or international organisations

1. The Data Processor shall solely be permitted to process personal data on documented instructions from the Data Controller, including as regards transfer (assignment, disclosure and internal use) of personal data to third countries or international organisations, unless processing is required under EU or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest, cf. Article 28, sub-section 3, para a.
2. Without the instructions or approval of the Data Controller, the Data Processor therefore cannot within the framework of this Data Processor Agreement:

   - disclose personal data to a data controller in a third country or in an international organisation
   - assign the processing of personal data to a sub-processor in a third country
   - have the data processed in another of the Data Processor's divisions which is located in a third country

   The Data Controller's documented instructions and approval for third-country transfers include the transfers necessary to engage the approved sub-processors listed in Appendix B, subject to the safeguards stated therein (e.g., SCCs and supplementary measures where required).

Assistance to the Data Controller

1. The Data Processor, taking into account the nature of the processing, shall, as far as possible, assist the Data Controller with appropriate technical and organisational measures, in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights pursuant to Chapter 3 of the General Data Protection Regulation.

   This entails that the Data Processor should as far as possible assist the Data Controller in the Data Controller's compliance with:

   - notification obligation when collecting personal data from the data subject
   - notification obligation if personal data have not been obtained from the data subject
   - right of access by the data subject
   - the right to rectification
   - the right to erasure ('the right to be forgotten')
   - the right to restrict processing

- notification obligation regarding rectification or erasure of personal data or restriction of processing
- the right to data portability
- the right to object
- the right to object to the result of automated individual decision-making, including profiling

2. The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32-36 of the General Data Protection Regulation taking into account the nature of the processing and the data made available to the Data Processor, cf. Article 28, sub-section 3, para f.

   This entails that the Data Processor should, taking into account the nature of the processing, as far as possible assist the Data Controller in the Data Controller's compliance with:

   - the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing
   - the obligation to report personal data breaches to the supervisory authority (Danish Data Protection Agency) without undue delay and, if possible, within 72 hours of the Data Controller discovering such breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
   - the obligation – without undue delay - to communicate the personal data breach to the data subject when such breach is likely to result in a high risk to the rights and freedoms of natural persons
   - the obligation to carry out a data protection impact assessment if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons
   - the obligation to consult with the supervisory authority (Danish Data Protection Agency) prior to processing if a data protection impact assessment shows that the processing will lead to high risk in the lack of measures taken by the Data Controller to limit risk

   The Parties' possible regulation/agreement on remuneration etc. for the Data Processor's assistance to the Data Controller shall be specified in the Parties' Master Agreement.

Notification of personal data breach

1. On discovery of personal data breach at the Data Processor's facilities or a sub-processor's facilities, the Data Processor shall without undue delay notify the Data Controller.

   The Data Processor's notification to the Data Controller shall take place without undue delay after the Data Processor has discovered the breach, to enable the Data Controller to comply with applicable reporting obligations.

2. The Data Processor shall – taking into account the nature of the processing and the data available – assist the Data Controller in the reporting of the breach to the supervisory authority.

   This may mean that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33, sub-section 3, of the General Data Protection Regulation, shall be stated in the Data Controller's report to the supervisory authority:

- The nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records
- Probable consequences of a personal data breach
- Measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage

Erasure and return of data

1. Standard deletion timeline
   Upon termination or expiration of the Master Agreement and following any grace period for license renewal as specified in the Software License Agreement, the Data Processor will delete personal data within 30 days unless EU or Member State law requires retention.

2. Accelerated deletion upon request
   The Data Controller may at any time request immediate deletion of all personal data by submitting a written request to the Data Processor. Upon receipt of such request, the Data Processor shall:

   a) Provide the Data Controller with an opportunity to export their data within 14 days of the request, and

   b) Complete deletion of personal data within 30 days of the request, or within 14 days after data export (whichever is later).

   By requesting accelerated deletion, the Data Controller acknowledges that this action is irreversible and waives any grace period for license renewal.

3. Backup retention
   Residual copies in backups will be deleted in accordance with the Data Processor's backup retention cycle, typically within 90 days of deletion from primary systems.

4. Deletion confirmation
   Upon request, the Data Processor shall provide written confirmation that deletion has been completed.

Inspection and audit

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and this Data Processor Agreement, and allow for and contribute to audits, including inspections performed by the Data Controller or another auditor mandated by the Data Controller.

The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller’s and Data Processor’s facilities, or

representatives acting on behalf of such supervisory authorities, with access to the Data Processor’s physical facilities on presentation of appropriate identification.

The Data Controller is entitled to initiate a review of the Data Processor's obligations under the Agreement once a year. The Data Controller must provide a detailed audit plan with a description of the scope, duration and start date at least four weeks prior to the proposed start date. For security reasons, the audit shall be done by a neutral third party after the Data Processor's choice, as it is a processing environment where multiple Data Controllers’ data is processed.

If the proposed scope of the audit follows an ISAE, ISO or similar audit report conducted by a qualified third-party auditor within the previous twelve months and the Data Processor confirms that there have been no material changes in the measures under review, the Data Controller shall accept this review instead of requesting a new review of the measures already covered.
In any case, audits must take place during normal office hours on the relevant facility in accordance with the Data Processors' policies and may not unreasonably interfere with the Data Processor's usual commercial activities.

The Data Controller shall bear all costs associated with the request for review. The assistance from the Data Processor, which exceeds the general service that the Data Processor must provide as a result of applicable data protection legislation, is settled separately.

Commencement and termination

1. This Data Processor Agreement shall become effective on the date of both parties accept of the Master Agreement.
2. Both Parties shall be entitled to require this Data Processor Agreement renegotiated if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.
3. This Data Processor Agreement may be terminated according to the terms and conditions of termination, incl. notice of termination, specified in the Master Agreement.
4. This Data Processor Agreement shall apply as long as the processing is performed. Irrespective of the termination of the Master Agreement and/or this Data Processor Agreement, the Data Processor Agreement shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any sub-processors.

Data Controller and Data Processor contacts/contact points

1. The parties may contact each other using the contact persons/contact point listed in the Master Agreement.
2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A: Information about the processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

that the Data Controller is able to use the application 'ActionPlanner' which is owned and managed by the Data Processor and that the Data Processor can provide the best service to The Data Controller when using the application.

The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

that the Data Processor makes available the application 'ActionPlanner' and hereby stores personal data about the Data Controller's employees that are relevant for the Data Controllers' use of the application and related support activities. The Data Controller adds personal data in the application.

The processing includes the following types of personal data about data subjects:

Account identifiers (name, email) and any voluntary personal data uploaded (profile picture, birthday, phone number, job title and initials), entered, or generated by authorised users in the Services, including initiative, milestone, action and goal items and comments, progress updates, meeting content (agenda topics, comments), attachments, and related metadata (timestamps, user IDs).

Processing includes the following categories of data subject:

- Persons who are employed with the Data Controller
- Persons who are stakeholders with the Data controller, including board members, suppliers, clients, collaborators etc.

The Data Processor's processing of personal data on behalf of the Data Controller may be performed when this Data Processor Agreement commences. Processing has the following duration:

Processing shall not be time-limited and shall be performed until this Data Processor Agreement is terminated or cancelled by one of the Parties. After this Data Processor Agreement is terminated or cancelled, the personal data will be deleted permanently.

The Data Processors processing of personal data takes place on the following locations:

Consulting services: Europe / EU

Client Support: Europe / EU

Web based services: Europe / EU and other locations as per Appendix B.

Appendix B: Terms of the Data Processor's use of sub-processors and list of approved sub-processors

Terms of the Data Processor's use of sub-processors

The Data Processor has the Data Controller's general authorisation to engage sub-processors for the provision of the services. The Data Processor shall inform the Data Controller of any planned changes with regard to the addition or replacement of sub-processors and thereby give the Data Controller the opportunity to object to such changes. Such notification shall be submitted to the Data Controller a minimum of one (1) month prior to the engagement of the sub-processor or the amendment coming into force.

The Data Controller shall notify the Data Processor of any objection within fourteen (14) days of receipt of the notification. The Data Controller may only object on reasonable and documented data-protection grounds.

The Data Processor shall ensure that each sub-processor is subject to the same data protection obligations as those set out in this Data Processor Agreement, by way of a contract or other legal act under EU or Member State law, providing sufficient guarantees that appropriate technical and organisational measures are implemented in accordance with the General Data Protection Regulation.

Upon request, the Data Processor shall make available to the Data Controller a copy of the relevant sub-processor agreement and any subsequent amendments, excluding commercial terms that do not affect the data protection obligations.

Scope of applicability
The sub-processors listed below may be engaged depending on the specific services, features, or functionalities used by the Data Controller. Not all listed sub-processors apply to all services or clients.

AI-based processing
AI-based functionality and processing are disabled by default and only activated upon explicit client configuration or upgrade. Client data is not used to train general-purpose AI models.

Approved sub-processors

Name	Purpose	Data categories	Processing location	Safeguards
Microsoft Azure	Hosting, databases, file storage, backups, logging, and AI/LLM infrastructure	User account data, application data, files, metadata, limited personal identifiers	Europe / EU (primary), with potential global transfers	Microsoft DPA, SCCs, ISO 27001, SOC 2
Microsoft 365	Email, calendar, contact, document, and collaboration services	Names, email addresses, calendar data, documents, meeting metadata	Europe / EU	Microsoft DPA, SCCs, ISO 27001, SOC 2
Cloudflare	Content Delivery Network (CDN), DNS resolution, and network security	IP addresses, request metadata	Global (edge network)	Cloudflare DPA, SCCs
Twilio SendGrid	Transactional email delivery	Email addresses, email content, delivery metadata	Europe / EU and/or Global (depending on configuration)	SendGrid DPA, SCCs

Name	Purpose	Data categories	Processing location	Safeguards
Pipedrive	CRM, sales pipeline management, and customer/prospect communication	Names, email addresses, business contact details, communication notes	Europe / EU	Pipedrive DPA, SCCs
ScoreApp	Lead capture, assessments, and marketing funnel interactions	Names, email addresses, assessment responses	UK / Europe	ScoreApp DPA, GDPR compliance
Kit (formerly ConvertKit)	Marketing communications and lead nurturing	Names, email addresses, engagement metadata	USA	Kit DPA, SCCs
Calendly	Meeting scheduling and availability coordination	Names, email addresses, meeting metadata	USA	Calendly DPA, SCCs
Zenegy	Payroll processing, accounting, invoicing, and financial reporting	Employee names, payroll data, customer names, billing and invoice data	Europe / EU	Zenegy DPA, GDPR compliance
E-conomic	Financial management and invoicing (legacy system retained for statutory data-retention obligations)	Customer names, billing and invoice data	Europe / EU	Visma DPA, GDPR compliance
SignNow	Electronic signing of contracts and documents	Names, email addresses, signed documents, signature metadata	USA	SignNow DPA, SCCs
VELOSO Consulting	Training, onboarding, coaching, and implementation support	Names, email addresses, role information, workshop materials	Europe / EU	Data Processor Agreement (DPA), confidentiality obligations

Transfer mechanisms and safeguards

For sub-processors located outside the European Economic Area, or where personal data may be transferred outside the EEA in the course of providing services, the Data Processor ensures that appropriate safeguards are in place in accordance with Chapter V of the GDPR. The primary transfer mechanism is the sub-processor's Data Processing Agreement, which incorporates the European Commission's Standard Contractual Clauses (SCCs) adopted pursuant to Commission Implementing Decision (EU) 2021/914. The Data Processor does not separately execute individual SCC agreements with each sub-processor; rather, the SCCs are incorporated by reference into the sub-processor's standard contractual terms, which the Data Processor has accepted. Additional safeguards may include the sub-processor's certifications (such as ISO 27001 or SOC 2 Type II), technical measures (such as encryption), and organisational measures (such as access controls and confidentiality obligations).

The Data Processor may engage sub-processors for substantially similar processing activities in accordance with this Appendix B.