EverReady

LEGAL · EU · UK · UNITED STATES

Data Processing Agreement

Agreement on the processing of personal data by a processor, applicable in the European Union, the United Kingdom and the United States.

Version 3.0 | September 2026 | GDPR · UK GDPR · US State Privacy Laws

BETWEEN

The Controller

COMPANY NAME, a LEGAL FORM with a share capital of AMOUNT, registered with the CITY Trade and Companies Register under number REGISTRATION NO., with its registered office at REGISTERED ADDRESS, represented by NAME, TITLE.

Hereinafter, "the Controller". On the one hand,

The Processor

EverReady, a French simplified joint-stock company (SAS) with a share capital of €1,906.90, registered with the Nanterre Trade and Companies Register under SIRET number 879 848 919, with its registered office at 21 rue Saint Vincent — 92700 Colombes, France, represented by Loïc Deo Van in his capacity as President, defined under Article 4 of the GDPR as "the legal person which processes personal data on behalf of the controller".

Hereinafter, "the Processor" or "EverReady". On the other hand,

Hereinafter referred to collectively as "the Parties" and individually as "a Party".

Recitals

The services set out below entail the processing by the Processor of personal data (hereinafter "Personal Data") in the name and on behalf of the Controller, as described in Article 2 hereof. The Parties have acknowledged their respective capacities as Processor and Controller within the meaning of Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, applicable from 25 May 2018 (hereinafter, "the GDPR").

EverReady's services as Processor

The Processor publishes a B2B SaaS platform natively integrated with Salesforce, comprising the following modules, subscribed to by the Controller under the terms of the Main Agreement:

- **"Connect" module (CRM automation):** automatic updating of business contacts and sales activities in the CRM based on the analysis of users' professional mailboxes, calendars and telephones, including the retrieval of historical data (Flashback);
- **"Notetaker" module (meetings):** capture, recording, transcription and subsequent analysis by artificial intelligence of the video conference meetings attended by users, and delivery of the recordings, transcripts and summaries into the Controller's CRM;
- **"EverReady Agents AI for Salesforce" module (AI agents):** a suite of artificial intelligence agents embedded in the Controller's Salesforce environment, producing, on the basis of CRM data and sales interactions, enrichments, analyses and draft content submitted to users for validation.

Details of each module, of the data processed and of the retention periods are set out in Schedule A.

Anxious to comply with the regulations relating to the protection of Personal Data, including the GDPR, the Parties have agreed as follows. They acknowledge that these provisions cancel and replace any other provisions relating to the protection of personal data previously agreed between them.

ARTICLE 1

Definitions

The Parties agree on the following definitions:

- **"Data Protection Laws"** means all laws and regulations applicable to the processing of Personal Data under this Agreement, including, without limitation: (i) the GDPR, together with French Act No. 78-17 of 6 January 1978 on information technology, data files and civil liberties, Decree No. 2019-536 of 29 May 2019, and Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; (ii) the UK GDPR, the UK Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003; (iii) the US State Privacy Laws; and (iv) the Swiss Federal Act on Data Protection; in each case as amended, updated or replaced from time to time;
- **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
- **"UK GDPR"** means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;
- **"US State Privacy Laws"** means the California Consumer Privacy Act as amended by the California Privacy Rights Act (together, the "CCPA") and any other US state privacy statute applicable to the Controller's use of the Service, including the Virginia Consumer Data Protection

Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act and the Texas Data Privacy and Security Act;

- **"UK Addendum"** means the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office and laid before Parliament on 2 February 2022 under section 119A of the Data Protection Act 2018, as set out in Schedule D;
- **The terms "Controller", "Processor", "Processing", "Personal Data", "Personal Data Breach", "Data Subjects", "Record of Processing Activities", "Data Protection Officer"** have the meanings given to them by the GDPR, whether used in the singular or the plural;
- **"Service"** means all modules of the EverReady platform subscribed to by the Controller under the Main Agreement;
- **"Module"** means any one of the three modules described in the Recitals (Connect, Notetaker, AI Agents), each of which may be activated or deactivated independently by the Controller;
- **"AI Model"** means a language model or generative model used to operate the Notetaker and AI Agents Modules;
- **"Model Provider"** means the publisher of an AI Model (currently including Mistral AI, OpenAI and Meta), it being specified that the Model is executed within the infrastructure described in Article 4;
- **"Output Data"** means the content generated by an AI Model from the Personal Data (structured transcripts, summaries, suggested field values, draft emails, qualification analyses);
- **"EU SCCs"** means the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and "UK SCCs" means the EU SCCs as amended by the UK Addendum; together, the "Standard Contractual Clauses";
- **"Data Exporter" and "Data Importer"** have the meanings given to them in the Standard Contractual Clauses;
- **"Main Agreement"** means the Service subscription agreement entered into between the Parties, to which this Agreement is appended.

ARTICLE 2

Scope and application by jurisdiction

This Agreement applies to all processing of Personal Data carried out by the Processor on behalf of the Controller in connection with the Service, irrespective of the Controller's place of establishment. The provisions set out below apply cumulatively to the extent that the corresponding legislation applies to the processing in question.

2.1 European Union and European Economic Area

Where the processing is subject to the GDPR, this Agreement constitutes the agreement required by Article 28(3) of the GDPR. The Controller acts as controller and the Processor as processor, save as provided in Article 21. Where the Controller itself acts as a processor on behalf of a third-party controller, the Processor acts as a sub-processor and this Agreement applies mutatis mutandis, references to the Controller's instructions being understood as instructions issued by that third-party controller.

2.2 United Kingdom

Where the processing is subject to the UK GDPR, this Agreement constitutes the agreement required by Article 28(3) of the UK GDPR. References to the GDPR shall be read as references to the UK GDPR, references to the European Union and to Member States shall be read as references to the United Kingdom, references to the competent supervisory authority shall be read as references to the Information Commissioner's Office, and references to a data protection impact assessment shall be read as references to the equivalent obligation under the UK GDPR. Transfers subject to Chapter V of the UK GDPR are governed by Article 8.3 and Schedule D.

2.3 United States

Where the processing is subject to the US State Privacy Laws, Article 20 applies. The Controller is the "business" or "controller" and the Processor is the "service provider", "contractor" or "processor", as those terms are defined in the applicable statute. Where a provision of this Agreement conflicts with a mandatory requirement of an applicable US State Privacy Law, that requirement prevails for the processing concerned.

2.4 Switzerland

Where the processing is subject to the Swiss Federal Act on Data Protection, references to the GDPR shall be read as including that Act, the competent supervisory authority shall be the Federal Data Protection and Information Commissioner, and the protection afforded by this Agreement extends to the data of legal entities to the extent required by that Act.

ARTICLE 3

Description of the processing subject to this Agreement

The processing subject to this Agreement is described in Schedule A hereto. The list of Sub-Processors is set out in Schedule B. The technical and organisational measures implemented by the Processor are set out in Schedule C.

The Schedules form an integral part of this Agreement. They are updated in accordance with Articles 7 and 23.

ARTICLE 4

Obligations of the Processor towards the Controller

The Processor undertakes to:

- Process the data solely for the purpose or purposes subject to this Agreement;
- Process the data in accordance with the documented instructions of the Controller, as supplemented at any time and by any means by the latter. This Agreement, the Main Agreement and the configuration carried out by the Controller in the Service administration console constitute its documented instructions;
- Where the Processor considers that an instruction constitutes a breach of the Data Protection Regulations, immediately inform the Controller, in accordance with the Communication Article hereof;
- In such a case, the Parties agree to meet by any means within a reasonable period, not exceeding thirty (30) calendar days, in order to discuss and jointly find a solution. Should the disagreement persist at the end of such discussions, the Processor may refuse to carry out the disputed instruction;
- Transfer Personal Data to a country outside the European Union or to an international organisation only with the prior consent of the Controller and under the conditions set out in Article 8, unless otherwise required by law;
- Inform the Controller where the Processor is required to transfer data to a third country or to an international organisation under a legal obligation to which it is subject, prior to the processing, unless the relevant law prohibits such information on important grounds of public interest;
- Ensure the confidentiality of the Personal Data processed under this Agreement;
- Ensure that the persons authorised to process the Personal Data under this Agreement:
  - Undertake to respect confidentiality or are subject to an appropriate statutory obligation of confidentiality;
  - Receive the necessary training in the protection of personal data;
- Take into account, in respect of its tools, products, applications and services, the principles of data protection by design and data protection by default as defined in Article 25 of the GDPR, and as clarified by guidance issued by the various competent national and European data protection authorities;
- **Refrain from using the Personal Data, the recordings, the transcripts or the Output Data for the purposes of training, re-training, fine-tuning or evaluating artificial intelligence models, or for any purpose of its own**, with the exception of strictly technical and aggregated data which does not permit any re-identification (volumes, error rates, response times) and solely for the purposes of monitoring and improving the availability of the Service;
- Limit access to the Personal Data to those members of its personnel who need to know it for the performance of the Service, on a least-privilege basis, and log such access;

- Make available to the Controller the export and deletion functionalities enabling it to respond to requests from Data Subjects exercising their rights.

ARTICLE 5

Specific provisions applicable to processing carried out by artificial intelligence

5.1 Execution architecture and the Controller's choice

For the Notetaker and AI Agents Modules, the Controller selects one of the following configurations, such choice constituting a documented instruction within the meaning of Article 4:

- **Configuration A — Native Salesforce models:** AI processing is carried out within the Controller's Salesforce environment, using the artificial intelligence services made available by Salesforce. In this configuration, Salesforce acts as a processor of the Controller under the agreement entered into directly between the Controller and Salesforce, and not as a Sub-Processor of EverReady;
- **Configuration B — EverReady AI services:** AI processing is carried out by the Processor using the Amazon Bedrock service, in a European Union region. The Controller selects the AI Model from those offered in the catalogue (currently including Mistral, OpenAI and Meta models). The Personal Data is processed on an ephemeral basis, is not retained by the inference service once processing is complete, and is not transmitted to the Model Providers, who have no access to it;
- **Configuration C — The Controller's own LLM environment:** the Personal Data is transmitted, via API, to the artificial intelligence environment designated and administered by the Controller. In this configuration, the Processor merely executes the instruction to transmit; the Controller remains solely responsible for the choice of that provider, for its compliance, for the lawfulness of the processing it carries out, for the retention periods applied and, where applicable, for framing any resulting transfers outside the European Union.

The Processor shall inform the Controller, in accordance with Article 7, of any change to the catalogue of AI Models offered under Configuration B.

5.2 Scope of access to CRM data

The AI Agents may access objects and fields within the Controller's Salesforce environment, in particular: Account, Opportunity, Contact, Lead, Case, Task and Event, Note, User, as well as custom objects.

The Controller itself configures, object by object and field by field, the read and write access permissions granted to each AI Agent. It is accordingly the Controller's responsibility to grant access only to the data strictly necessary for the purposes pursued, in accordance with the data minimisation principle set out in Article 5(1)(c) of the GDPR, and not to grant access to data falling within Article 9 of the GDPR. The configuration chosen by the Controller is logged and enforceable between the Parties.

Actions performed by the AI Agents in the CRM (creation, modification, re-linking of records) are traced and attributable, so as to enable the Controller to monitor their scope.

5.3 No automated individual decision-making

The Output Data constitutes proposals, enrichments or decision-support material. No decision producing legal effects concerning a Data Subject, or similarly significantly affecting them within the meaning of Article 22 of the GDPR, is taken solely on the basis of automated processing carried out by the Service.

The Controller undertakes to maintain effective human oversight over the use of the Output Data and shall refrain from using the Service, in particular its performance or engagement analyses, for the purposes of individual assessment, scoring or monitoring of its employees, without first having completed the formalities and consultations incumbent upon it (including informing and consulting employee representative bodies).

5.4 Accuracy and limitations of the Output Data

The Parties acknowledge that AI Models may produce Output Data that is inaccurate, incomplete or irrelevant. The Processor implements reasonable measures to limit this risk (grounding of responses in source data, display of the underlying source material, user correction capability). The Controller shall put in place the controls necessary to comply with the accuracy principle set out in Article 5(1)(d) of the GDPR, the Output Data remaining editable and deletable within the CRM.

5.5 Regulation (EU) 2024/1689 on artificial intelligence

The Parties shall cooperate in good faith with a view to complying with Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, as it progressively becomes applicable. The Processor shall make available to the Controller the information relating to the AI systems used that is necessary for the Controller to discharge its own transparency and AI literacy obligations.

ARTICLE 6

Specific provisions applicable to the Notetaker Module

6.1 Activation and configuration

The activation of the Notetaker Module, the designation of authorised users, the types of meetings concerned and the rules triggering recording are matters for the Controller alone. The Processor makes available the settings enabling recording to be activated or deactivated by user, by meeting type or on a case-by-case basis.

6.2 Processing chain

Meetings are processed in the following sequence:

- Capture: the video conference is recorded and transcribed by the Sub-Processor Hyperdoc Inc. (Recall.ai), whose hosting and processing take place on its infrastructure located in Frankfurt, Germany, within the European Union;
- Deletion at source: the recordings and transcripts are deleted from Recall.ai's servers immediately after being transferred to the Processor's platform, the Processor having enabled the automatic deletion setting which triggers the erasure of content from Recall.ai's servers as soon as the recording ends;
- Analysis: the recordings and transcripts are transmitted to the Processor's platform hosted with Amazon Web Services in the European Union, and are then processed by artificial intelligence via Amazon Bedrock in accordance with the configuration selected under Article 5.1;
- Storage: the content is retained, at the Controller's choice, (i) in the Processor's Amazon S3 storage located in the European Union, or (ii) in an Amazon S3 storage bucket owned and administered by the Controller;
- Delivery: the recordings, transcripts, timestamps, identities and business email addresses of participants, together with the summaries generated, are synchronised into the Controller's Salesforce environment.

Where the Controller elects to store content in its own Amazon S3 bucket, it assumes control of, and responsibility for, the security, location, retention periods and deletion of the content stored there, the Processor merely writing the content to that location on instruction.

6.3 Information and legal basis — obligations of the Controller

The Controller is solely responsible for the lawfulness of the recording of meetings. Prior to any capture, it is the Controller's responsibility to:

- inform all participants, whether internal or external, of the existence of the recording and transcription, of their purposes, of the recipients, of the retention periods and of the rights available to them;
- obtain, where the applicable law so requires, the prior consent of participants, in particular external participants and participants located in jurisdictions requiring the consent of all parties to a communication;
- guarantee participants an effective ability to object to the recording, to request that it be stopped, or to continue the meeting without capture, without adverse consequence;
- determine and document the legal basis for the processing within the meaning of Article 6 of the GDPR, together with, where applicable, the information and consultation of employee representative bodies.

The Processor makes available the technical means facilitating such information, in particular visible signalling of the recording within the video conference where the meeting platform allows it, and the ability to stop the recording during the meeting.

6.4 Exclusions

The Controller undertakes not to use the Notetaker Module for meetings whose subject matter involves the processing of special categories of data within the meaning of Article 9 of the GDPR (health, political opinions, religious beliefs, trade union membership, sexual orientation, biometric or genetic data), of data relating to criminal convictions and offences within the meaning of Article 10 of the GDPR, or of data covered by a legally protected professional privilege, nor for meetings of employee representative bodies.

Should such data nevertheless be captured incidentally, the Controller assumes responsibility for it and may at any time request the deletion of the corresponding recording and transcript, which the Processor shall carry out without delay.

6.5 Retention periods

Video recordings, transcripts, timestamps, participant identification data and associated summaries are retained in the Processor's storage for a period of six (6) months from the date of the meeting.

The Controller may subscribe, as a paid option, to an extended retention period of up to twenty-four (24) months. The period selected is set out in the Main Agreement or its order form and constitutes a documented instruction of the Controller, who remains responsible for ensuring that it is proportionate to the purposes pursued.

Upon expiry of the applicable period, the content is automatically deleted from the Processor's systems. Content synchronised into the Controller's Salesforce environment, or stored in its own Amazon S3 bucket, remains subject to the retention policies defined by the Controller.

ARTICLE 7

Sub-processing

The Processor may engage another processor (hereinafter, "the Sub-Processor") to carry out specific processing activities. The Controller expressly authorises the engagement of the Sub-Processors listed in Schedule B.

For any intended change concerning the addition or replacement of a Sub-Processor, the Processor shall inform the Controller in advance and in writing. Such information shall clearly state the processing activities subcontracted, the identity and contact details of the Sub-Processor, the location of the processing and the dates of the sub-processing agreement. The Controller has a maximum period of thirty (30) calendar days from receipt of such information to raise reasoned objections. Such sub-processing may only take place if the Controller has not objected within the agreed period.

The Sub-Processor is required to comply with the obligations of this Agreement on behalf of and in accordance with the instructions of the Controller. It is the responsibility of the Processor to ensure that the Sub-Processor provides the same sufficient guarantees as to the implementation of

appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. If the Sub-Processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of that Sub-Processor's obligations.

The Sub-Processors listed in Schedule B themselves engage their own sub-processors, the list of which is published and kept up to date by them. The Processor subscribes to the notification mechanisms operated by those Sub-Processors, reviews the changes notified to it and informs the Controller where such changes affect the location of processing, the security of the data or the existence of a transfer outside the European Union. The objection periods available to the Processor in respect of its own Sub-Processors may be shorter than the thirty (30) day period provided for in this Article; in such a case, the Processor shall inform the Controller without delay and, in the event of a reasoned objection from the Controller, the Parties shall jointly seek an alternative solution in accordance with Article 4.

ARTICLE 8

International transfers of personal data

8.1 Principle

The hosting and processing of Personal Data take place within the European Union, on the infrastructure described in Schedule B. Any transfer of Personal Data to a country outside the European Economic Area, the United Kingdom or Switzerland that does not benefit from an adequacy decision is subject to the prior consent of the Controller and to the implementation of an appropriate transfer mechanism.

Schedules A and B contain the information required by Annex I and Annex III of the EU SCCs and by Annex 1A and Annex 1B of the UK Addendum. Schedule C contains the information required by Annex II of the EU SCCs and of the UK Addendum.

8.2 Transfers subject to Chapter V of the GDPR

Where a transfer subject to Chapter V of the GDPR takes place, the EU SCCs are deemed entered into and incorporated into this Agreement by reference, completed as follows:

- Module Two (controller to processor) applies where the Controller is a controller and the Processor processes Personal Data on its behalf as a processor;
- Module Three (processor to sub-processor) applies where the Controller is a processor and the Processor processes Personal Data on its behalf as a sub-processor, including in respect of transfers by the Processor to the Sub-Processors listed in Schedule B;
- Module Four (processor to controller) applies where the Controller is established outside the European Economic Area and receives Personal Data from the Processor;

- The optional docking clause in Clause 7 does not apply; in Clause 9, Option 2 (general written authorisation) applies, with the notice period set out in Article 7; the optional language in Clause 11 does not apply; the square brackets in Clause 13 are removed;
- In Clause 17 (Option 1), the EU SCCs are governed by French law, and under Clause 18(b) disputes are resolved before the courts of Paris, France;
- By entering into this Agreement, the Parties are deemed to have signed the EU SCCs, including their Annexes.

8.3 Transfers subject to Chapter V of the UK GDPR

Where a transfer subject to Chapter V of the UK GDPR takes place, including where the Controller is established in the United Kingdom and Personal Data is transferred to the Processor in France, the UK SCCs apply. The EU SCCs referred to in Article 8.2 are incorporated as amended and completed by the UK Addendum set out in Schedule D. The Information Commissioner's Office is the competent supervisory authority, and the UK Addendum is governed by the laws of England and Wales.

8.4 Transfers from Switzerland

Where a transfer is subject to the Swiss Federal Act on Data Protection, the EU SCCs apply with the following modifications: references to the GDPR include that Act; the Federal Data Protection and Information Commissioner has authority over transfers governed by that Act; and data subjects in Switzerland may enforce their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

8.5 Recall.ai and the Notetaker Module

The Processor draws the Controller's attention to the following. Hyperdoc Inc. (Recall.ai), which carries out the capture, recording and transcription of video conferences under the Notetaker Module, is a company incorporated under the laws of the United States with its registered office at 2261 Market Street #4339, San Francisco, CA 94114, United States.

The Processor has subscribed to and implemented the European localisation option for that service: hosting and processing of the data take place exclusively on the infrastructure located in Frankfurt, Germany, within the European Union. The Processor has further enabled the automatic deletion setting which erases content from Recall.ai's servers as soon as the recording ends.

In the event that remote access to the data from the United States were to become necessary for technical support or maintenance purposes, or were to result from the application of extraterritorial legislation to which that company is subject, such access would constitute a transfer within the meaning of Chapter V of the GDPR and of the UK GDPR. That transfer is governed by the Standard Contractual Clauses, module three (processor to sub-processor), entered into between the Processor and Hyperdoc Inc., and supplemented by the following additional measures:

- Encryption of data in transit and at rest, segregation of environments, restriction and logging of access;
- Undertaking by the data importer not to make any voluntary disclosure of Personal Data to any administrative or judicial authority;
- Undertaking by the data importer, in the event of a request from an authority, to redirect that authority to the Controller, to inform the Processor within a reasonable time unless legally prohibited, and to cooperate so as to allow the available remedies to be exercised;
- Joint review, in the event of a request from an authority, of whether all or part of the transfers should be suspended;
- Periodic reassessment of whether the level of protection afforded by the law of the data importer's country remains sufficient.

A Transfer Impact Assessment is available to the Controller upon request.

8.6 Transfers directed by the Controller

Where the Controller opts for Configuration C referred to in Article 5.1, or elects to store content in its own storage bucket located outside the European Economic Area, the resulting transfers are made on its documented instruction and fall within its sole responsibility, including as regards the implementation of an appropriate transfer mechanism.

8.7 Continued validity

If any transfer mechanism referred to in this Article ceases to be valid, or if a supervisory authority requires transfers made under it to be suspended, the Parties shall cooperate in good faith to put in place an alternative mechanism compliant with the applicable Data Protection Laws, without undue delay.

ARTICLE 9

Right to information of data subjects

Unless otherwise agreed by the Parties, it is the responsibility of the Controller to provide information to the Data Subjects concerned by the processing operations at the time the data is collected, including with regard to the recording and transcription of meetings under the conditions set out in Article 6.3 and to the use of automated processing by artificial intelligence.

Where the collection of Personal Data is carried out by the Processor, the Parties agree that it is the Processor's responsibility, at the time of collection, to provide the Data Subjects with the information relating to the data processing it carries out. The wording and format of that information must be agreed with the Controller prior to collection.

ARTICLE 10

Exercise of data subjects' rights

To the extent possible, the Processor shall assist the Controller in fulfilling its obligation to respond to requests from Data Subjects exercising their rights: the right of access, rectification, erasure and objection, the right to restriction of processing, the right to data portability, and the right not to be subject to an automated individual decision (including profiling).

The Processor makes available to the Controller the functionalities enabling it to access, export, rectify and delete recordings, transcripts, summaries and Output Data. Where an erasure request is executed, deletion is propagated to the copies held in the Processor's systems; the Controller remains responsible for reflecting it in its Salesforce environment and, where applicable, in its own storage.

Where Data Subjects submit requests to exercise their rights to the Processor, the Processor shall forward such requests to the Controller upon receipt, in accordance with the Communication Article hereof.

ARTICLE 11

Notification of personal data breaches

The Processor shall notify the Controller of any personal data breach within a maximum period of forty-eight (48) hours after becoming aware of it, in accordance with the Communication Article hereof. Such notification shall be accompanied by all relevant documentation so as to enable the Controller, where necessary, to notify the breach to the competent supervisory authority. The notification shall contain at least:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer or other contact point from whom further information may be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and to the extent that, it is not possible to provide all of this information at the same time, the information may be provided in phases without undue further delay.

Where the breach originates with a Sub-Processor, the forty-eight (48) hour period runs from the moment the Processor becomes aware of the breach. The Processor contractually imposes on its Sub-Processors an obligation to notify without undue delay and takes the necessary steps to obtain, as soon as possible, the information enabling the Controller to meet its own notification obligations.

The Processor undertakes to use all means at its disposal to resolve and/or mitigate the effects of the data breach as quickly as possible.

ARTICLE 12

Assistance from the Processor in the Controller's compliance with its obligations

The Processor shall assist the Controller, and its Data Protection Officer, in carrying out data protection impact assessments and in conducting prior consultation with the competent supervisory authority where the Controller is subject to any or all of those obligations.

The Parties acknowledge that the implementation of the Notetaker Module, in that it entails the systematic recording of communications, and of the AI Agents Module, in that it relies on innovative artificial intelligence processing of data relating to employees and third parties, may require a data protection impact assessment within the meaning of Article 35 of the GDPR. The Processor shall make available to the Controller the technical descriptions necessary for that assessment.

Where applicable, the Controller may delegate the carrying out of an impact assessment to the Processor.

ARTICLE 13

Security measures

The Processor undertakes to implement all technical and organisational security measures necessary for the protection of the Personal Data processed under this Agreement, in accordance with Article 32 of the GDPR. Those measures are described in Schedule C.

The Processor shall inform the Controller of any material change to those measures that would reduce their level.

ARTICLE 14

Fate of the data

Upon completion of the services relating to the processing of this data, the Processor undertakes, at the Controller's choice:

- To destroy all Personal Data; OR
- To return all Personal Data to the Controller; OR
- To return the Personal Data to the processor designated by the Controller.

The Controller shall notify its choice to the Processor by any means, and the Processor shall have thirty (30) calendar days to comply.

Where the Controller has chosen the return of the Personal Data, whether to itself or to another processor, the return must be accompanied by the destruction of all existing copies in the Processor's information systems. Once destroyed, the Processor must provide written evidence of the destruction within the following seven (7) calendar days.

In any event, and save where an extended retention period has been subscribed to under Article 6.5, the Personal Data is deleted from the Processor's systems no later than six (6) months after the end of the Main Agreement or the termination of the Service, subject to any legal retention obligations to which the Processor is subject.

ARTICLE 15

Data Protection Officer

The Parties inform each other that they have appointed a Data Protection Officer:

For the Controller

DPO SURNAME / FIRST NAME

EMAIL

IF OUTSOURCED DPO: COMPANY NAME

ADDRESS

If no DPO has been appointed, state "no DPO appointed".

For the Processor: Charles Olivier Tolédano — gdpr@everready.ai

ARTICLE 16

Communication

Unless expressly provided otherwise, all communications in connection with the Processing of Personal Data shall be made by email.

Each Party designates a point of contact for the other Party. All communications must be addressed to that person.

For the Controller, the point of contact is

NAME

EMAIL ADDRESS

For the Processor: Charles Olivier Tolédano — olivier@everready.ai

ARTICLE 17

Record of categories of processing activities

The Processor declares that it maintains in writing a record of all categories of processing activities carried out on behalf of the Controller, containing:

- The name and contact details of the Controller on whose behalf it acts, of any Sub-Processors and, where applicable, of the data protection officer;
- The categories of processing carried out on behalf of the Controller;
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
- Where possible, a general description of the technical and organisational security measures.

The Processor shall make available to the Controller the part of the record that concerns it. The Controller may request a copy at any time, in accordance with the Audit Article hereof.

ARTICLE 18

Documentation

The Processor shall make available to the Controller all documentation necessary to demonstrate compliance with all of its obligations and to allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by it.

ARTICLE 19

Audit

The Controller may carry out on-site or desk audits under the following conditions.

The Controller shall send any request for the provision of documentation to the Processor by email with delivery and read receipts. Unless otherwise indicated by the Controller, the documentation shall be provided in an easily readable digital format, by secure email.

The Processor undertakes to make the requested documentation available to the Controller as soon as possible, and in any event within a period not exceeding thirty (30) calendar days.

The Parties agree that the Controller may, no more than once per year, carry out an audit of the Processor's Personal Data processing practices and information systems at the Processor's premises, or have such an audit carried out by a duly authorised third-party auditor bound by confidentiality obligations.

The audit may only take place subject to prior notice, given by any means to the Processor, at least five (5) business days before the audit date. The audit may only take place during the Processor's business hours and under conditions designed not to disrupt its activities.

The Processor may satisfy all or part of an audit request by providing its valid ISO/IEC 27001 certificate, the associated scope of certification and, where applicable, the summary report of its penetration tests, provided that these documents address the matters covered by the request.

At the end of the audit, the Controller may draw up, or have a third-party auditor draw up, an audit report listing the points of non-compliance with this Agreement and with the Data Protection Regulations identified during the audit. The Processor undertakes to implement all appropriate measures to remedy the points of non-compliance within three hundred and sixty-five (365) days following receipt of the report, without passing on the financial cost to the Controller.

ARTICLE 20

US State Privacy Laws

20.1 Roles

This Article applies where and to the extent that the processing of Personal Data under this Agreement is subject to the US State Privacy Laws. In that case, the Controller is the "business" or "controller" and the Processor is the "service provider", "contractor" or "processor". Personal Data includes "personal information" as defined in Section 1798.140 of the CCPA.

20.2 Restrictions on the Processor

The Processor shall not:

- sell or share Personal Data, as those terms are defined in the CCPA;
- retain, use or disclose Personal Data for any purpose other than the specific business purpose of performing the Service under the Main Agreement, or as otherwise permitted by the US State Privacy Laws;
- retain, use or disclose Personal Data outside the direct business relationship between the Parties;
- combine Personal Data received from or on behalf of the Controller with personal information received from or on behalf of any other person, or collected from its own interactions with a consumer, except as permitted by the US State Privacy Laws.

The Processor certifies that it understands and will comply with the restrictions set out in this Article. The Processor shall notify the Controller without undue delay if it determines that it can no longer meet its obligations under the US State Privacy Laws.

20.3 Assistance and consumer rights

The Processor shall provide reasonable assistance to enable the Controller to respond to verifiable consumer requests to know, access, delete, correct, opt out of sale or sharing, or limit the use of sensitive personal information, and shall implement any deletion or correction instruction the Controller transmits to it. Where the Processor receives such a request directly, it shall direct the requester to the Controller and inform the Controller.

The Processor shall assist the Controller with the security of processing, with the notification of security breaches and, where applicable, with data protection assessments required by the US State Privacy Laws, taking into account the nature of the processing and the information available to it.

20.4 Sub-contractors and oversight

The Processor shall impose on each Sub-Processor, by written contract, obligations equivalent to those set out in this Article. The Controller has the right, upon reasonable notice, to take reasonable and appropriate steps to verify that the Processor uses Personal Data in a manner consistent with the Controller's obligations under the US State Privacy Laws, and to stop and remediate any unauthorised use. The audit mechanisms described in Article 19 are deemed to satisfy this right.

20.5 Sensitive personal information and de-identified data

The Controller shall not transmit, and shall not configure the Service so as to cause the collection of, sensitive personal information within the meaning of the US State Privacy Laws, consistently with Article 6.4. Where the Processor holds de-identified or aggregated data, it shall maintain it in de-identified form, shall not attempt to re-identify it, and shall contractually impose the same obligation on any recipient.

ARTICLE 21

Data processed by the Processor as a separate controller

The Parties acknowledge that the Processor processes the following categories of data as an independent controller, and not as a joint controller:

- **Account data:** the identity and business contact details of the persons authorised by the Controller to administer the account, billing data and data necessary for the management of the contractual relationship;
- **Technical usage data:** activity logs, performance and availability data, and aggregated Service usage metrics.

This processing is carried out solely for the purposes of managing the contractual relationship, billing, complying with the Processor's legal and accounting obligations, security, prevention of fraud and abuse, and maintaining the Service in operational condition. It is governed by the Processor's

privacy policy.

Technical usage data does not include the content of emails, meetings, transcripts or recordings, and is not used to train artificial intelligence models, in accordance with Article 4.

The Processor informs the Controller that certain of its Sub-Processors, including Hyperdoc Inc. (Recall.ai), likewise process their own account data and technical usage data as independent controllers, under the conditions set out in their privacy policies.

ARTICLE 22

Term

This Agreement takes effect on the date of signature of the Main Agreement, or on the date of its own signature if later, and remains applicable throughout the term of the Main Agreement. The obligations of confidentiality and security, and those relating to the fate of the data, survive its termination until the Personal Data has been fully returned or destroyed.

ARTICLE 23

Order of precedence and amendment

In the event of any conflict between the provisions of this Agreement and those of the Main Agreement, this Agreement shall prevail in all matters concerning the protection of Personal Data.

Schedules A, B and C may be updated by the Processor to reflect changes to the Service, to the Sub-Processors or to the security measures, subject to prior notice to the Controller in accordance with Article 7 and provided that the level of protection is not thereby reduced.

In the event of any conflict or inconsistency between the following documents, the order of precedence shall be: (1) the applicable Standard Contractual Clauses, including the UK Addendum where applicable; (2) this Agreement; (3) the Main Agreement. Articles 2.2, 2.3, 2.4, 8.3, 8.4 and 20, together with Schedule D, apply only to the extent that the corresponding legislation applies to the processing concerned, and do not otherwise limit the protections afforded under the GDPR.

Any other amendment to this Agreement shall be the subject of a written amendment signed by both Parties.

EXECUTION

Signatures

For the Controller

NAME

TITLE

SIGNATURE

For the Processor — EverReady SAS

Loïc Deo Van, President

SIGNATURE

SCHEDULE A

Description of the Processing

1. Nature of the processing operations

1.1 Connect Module (CRM automation)

The Processor hosts users' Personal Data in order to authenticate them, give them access to the Service and send them notifications.

The Processor analyses the emails, meetings and calls exchanged between users and their prospects and customers in order to automatically update business contacts and sales activities in the CRM, including for the period prior to subscription (historical retrieval).

1.2 Notetaker Module (meetings)

Capture, recording and transcription of the video conference meetings attended by users; analysis of the transcripts by artificial intelligence for the purposes of producing summaries, key points and structured content; storage of the content and synchronisation into the Controller's CRM, in accordance with the processing chain described in Article 6.2.

1.3 EverReady Agents AI for Salesforce Module (AI agents)

Reading, analysis and, depending on the configuration set by the Controller, writing of data in the objects of the Controller's Salesforce environment, by artificial intelligence agents executed in accordance with one of the configurations set out in Article 5.1. The agents currently offered are as follows:

Opportunity Autofill

- **Field Autofill Agent** — keeps Salesforce fields up to date automatically, from the conversations reps already have.
- **Contact Roles Agent** — attaches contacts to the right opportunity with the correct role, no manual tagging.
- **Activity Relink Agent** — finds past activities and reattaches them to the opportunity they belong to.

Deal Analysis

- **MEDDPICC® Execution Agent** — fills and updates MEDDPICC® from every interaction, flags qualification gaps.
- **Deal Summary Agent** — turns any opportunity into a clear, readable summary in seconds.
- **Deal Timeline Agent** — visually reconstructs the full history of exchanges and engagement.

Next Move

- **Meeting Prep Agent** — preps reps ahead of every call with the key points and questions.
- **Follow-Up Email Agent** — drafts the follow-up email with agreed next steps, ready to send.
- **Contact Finder Agent** — surfaces new prospects with verified professional contact details.

2. Purposes of the processing operations

- Automatically update contacts and sales activities in the CRM;
- Provide dashboards tracking the updates performed;
- Send notifications to users regarding the updates performed;
- Record, transcribe and summarise sales meetings in order to retain a record of them and deliver their content into the CRM;
- Structure and enrich opportunity data (fields, contact roles, activity linkage, MEDDPICC® qualification);
- Produce analyses, summaries, meeting preparation material and draft messages intended to be reviewed and validated by users;
- Identify relevant business contacts and their professional contact details;
- Authenticate users, administer their access rights and ensure the security and traceability of the Service.

3. Categories of Personal Data

3.1 Data relating to Service users, stored on the Processor's servers

- Identification: surname, first name, business email address, business telephone number;
- System access, Service usage, permissions and roles;
- Technical connection and activity logs.

3.2 Connect Module — data processed in real time, without storage on the Processor's servers

Data relating to users' sales activities with their prospects and customers:

- From business emails: subject, message, business signature (first name, surname, business landline and mobile telephone numbers, business postal address, business email address, job title), recipients, sender, attachment, timestamp;
- From the business calendar: event, subject, participants, timestamp;
- From CRM company accounts: company name, domain name, telephone, email;
- From CRM contacts: surname, first name, telephone, email, job title;
- From CRM leads: company or contact name, telephone, email;

- From the business mobile telephone: call history, numbers, outgoing / incoming calls, duration, timestamp, during business hours only; conversations are not recorded.

Only technical data (identifiers and dates) relating to items created or modified in the CRM by EverReady is stored.

3.3 Notetaker Module — data recorded and retained

- Audio and video recording of the meeting, including the image and voice of participants who enable their camera or microphone, together with any content shared on screen;
- Full textual transcript of the exchanges, with speaker attribution;
- Participant identity: surname, first name, business email address, organisation, and status as organiser or invitee;
- Meeting metadata: title, description, video conference identifier and platform, date, start and end times, timestamps and duration of speaking turns;
- Output Data generated by artificial intelligence: summaries, key points, next steps, qualification elements, draft messages.

Recordings and transcripts are retained in the Processor's Amazon S3 storage or in the Controller's own storage, at the Controller's choice, and are synchronised into its Salesforce environment.

3.4 AI Agents Module — accessible data

Within the limits of the configuration set by the Controller, the AI Agents access the standard and custom objects and fields of its Salesforce environment, in particular: Account, Opportunity, Contact, Lead, Case, Task, Event, Note and User, as well as the emails, calendar events and meeting content synchronised by the Connect and Notetaker Modules.

The data thus accessible includes business identification and contact data, the content of business exchanges, data relating to the activity and engagement of counterparties, and data relating to the activity of the Controller's users.

The Contact Finder Agent additionally processes business contact data obtained from external sources: surname, first name, job title, employer, business email address, business telephone number and public professional profile.

4. Categories of Data Subjects

- Employees: users of the Service within the Controller's organisation;
- Prospects, customers and partners: natural persons who are business counterparties of the users, present in the CRM, in the exchanges analysed or participating in recorded meetings;
- Third parties: any natural person mentioned in an email, a calendar event or a recorded meeting, or whose business contact details are identified by the Contact Finder Module.

No special category of data within the meaning of Article 9 of the GDPR is processed intentionally, in accordance with Article 6.4.

5. Retention periods

- Data relating to Service users: retained for the term of the Main Agreement and deleted no later than six (6) months after its end or the termination of the Service;
- Connect Module: the data analysed is not stored; only technical data (identifiers and dates) relating to items created or modified in the CRM is retained for the term of the Main Agreement;
- Notetaker Module: recordings, transcripts, timestamps, participant identification data and summaries retained for six (6) months from the date of the meeting by default; extended to up to twenty-four (24) months where the corresponding option is subscribed to;
- Data processed by Recall.ai: deleted as soon as the recording ends, immediately after transfer to the Processor's platform;
- Output Data of the AI Agents: retained in the Controller's Salesforce environment, in accordance with the retention policies it defines;
- Technical and security logs: twelve (12) months.

Where content is stored in the Controller's own Amazon S3 bucket or synchronised into its Salesforce environment, the applicable retention periods are those it defines itself.

6. Location of processing

- Hosting of the platform, storage and artificial intelligence processing: Amazon Web Services, European Union regions (Ireland, Frankfurt, Paris);
- Capture, recording and transcription of video conferences: Recall.ai, infrastructure located in Frankfurt, Germany;
- Authentication and notifications: Google Firebase, Dublin, Ireland.

SCHEDULE B

List of Sub-Processors

The Controller authorises the engagement of the following Sub-Processors. This Schedule contains the information required by Annex III of the EU SCCs and by Annex 1B of the UK Addendum.

1. Amazon Web Services

Name	Amazon Web Services
Legal entity	Amazon Web Services EMEA SARL
Registered office	38 avenue John F. Kennedy, L-1855 Luxembourg
Location of processing	European Union — Ireland, Germany (Frankfurt), France (Paris)
Data centre address	4033 Citywest Avenue, Cooldown Commons, County Dublin, Ireland; AWS data centres in the eu-west-1, eu-central-1 and eu-west-3 regions
Transfer outside the EU	No
Privacy policy	https://aws.amazon.com/legal/
Scope of services	Hosting of the EverReady.ai technical platform and of all data; storage of recordings and transcripts (Amazon S3); execution of artificial intelligence processing (Amazon Bedrock)
Relationship with EverReady.ai	Service provision on behalf of EverReady.ai

2. Hyperdoc Inc. (Recall.ai)

Name	Recall.ai
Legal entity	Hyperdoc Inc.
Registered office	2261 Market Street #4339, San Francisco, CA 94114, United States
Location of processing	Frankfurt, Germany (European Union) — European localisation option subscribed to and implemented by EverReady
Data centre address	Infrastructure hosted in Frankfurt, Germany
Transfer outside the EU	No. Hosting and processing take place in Frankfurt, Germany. Remote access from the United States for support purposes is governed by the Standard Contractual Clauses (module three, Irish law) and the additional measures described in Article 8
Privacy policy	https://www.recall.ai/privacy
Its own sub-processor list	https://security.recall.ai/subprocessors
Scope of services	Capture, recording and transcription of video conference meetings under the Notetaker Module
Retention	Automatic deletion of content from Recall.ai's servers as soon as the recording ends, a setting enabled by EverReady
Independent processing	Processes its own account data and technical usage data as an independent controller, under the conditions set out in Article 21
Relationship with EverReady.ai	Service provision on behalf of EverReady.ai

3. Google — Firebase

Name	Google
Legal entity	Google Ireland Limited — Firebase
Registered office	Gordon House, Barrow Street, Dublin 4, Ireland
Location of processing	Dublin, Ireland
Data centre address	Dublin, Ireland
Transfer outside the EU	No
Privacy policy	https://firebase.google.com/support/privacy
Scope of services	Provider of an authentication and notification management solution
Relationship with EverReady.ai	Service provision on behalf of EverReady.ai

Clarifications regarding AI Model Providers

Under Configuration B (Article 5.1), the AI Models selected by the Controller — currently including Mistral, OpenAI and Meta models — are executed within the Amazon Bedrock service, in a European Union region. The Personal Data is neither transmitted to, nor accessible by, the Model Providers, is not retained once inference is complete, and is not used to train models. The Model Providers therefore do not act as Sub-Processors of the Processor.

Under Configuration A, Salesforce's artificial intelligence services fall under the agreement entered into directly between the Controller and Salesforce.

Under Configuration C, the artificial intelligence provider designated by the Controller falls under its own contractual arrangements and is not a Sub-Processor of the Processor.

SCHEDULE C

Technical and Organisational Measures

The Processor implements the following measures, in accordance with Article 32 of the GDPR and of the UK GDPR. This Schedule contains the information required by Annex II of the EU SCCs and of the UK Addendum.

1. Security governance

- Information security management system certified to ISO/IEC 27001;
- Information security policy, annual review and documented risk analysis;
- Staff awareness and training in security and data protection; contractual confidentiality undertakings;
- Appointment of a Data Protection Officer; maintenance of a record of processing activities.

2. Access control

- Named-user authentication and multi-factor authentication for access to production environments;
- Permission management on a least-privilege basis, periodic access reviews, revocation upon termination of employment;
- Strict logical segregation of data by customer (isolated multi-tenancy);
- Configuration by the Controller of AI Agent access, object by object and field by field.

3. Data protection

- Encryption of data in transit (TLS 1.2 minimum);
- Encryption of data at rest (AES-256) for databases and Amazon S3 storage;
- Key management via the hosting provider's key management service;
- Minimisation: in-memory processing without storage for the Connect Module; immediate deletion at source after capture for the Notetaker Module;
- No use of customer data to train artificial intelligence models.

4. Operational security

- Logging of access, user actions and AI Agent actions; logs retained for twelve (12) months;
- Monitoring of and alerting on security events;
- Vulnerability management, application of security patches, periodic penetration testing by an independent third party;

- Separation of development, staging and production environments; no production data in non-production environments;
- Code review and security controls embedded in the development lifecycle.

5. Continuity and resilience

- Regular encrypted backups and restoration testing;
- Infrastructure redundancy across multiple availability zones;
- Documented business continuity and disaster recovery plan.

6. Incident management

- Documented procedure for the detection, qualification and handling of security incidents;
- Notification to the Controller within forty-eight (48) hours of becoming aware of a data breach, in accordance with Article 11;
- Post-incident analysis and corrective action plan.

7. Management of Sub-Processors

- Prior assessment of their security and compliance posture;
- Contractual arrangements compliant with Article 28 of the GDPR and, where applicable, Standard Contractual Clauses;
- Periodic review of Sub-Processors and of their processing locations.

SCHEDULE D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner's Office and laid before Parliament on 2 February 2022 under section 119A of the Data Protection Act 2018 (the "Approved Addendum").

This Schedule applies only to transfers of Personal Data subject to Chapter V of the UK GDPR. The Parties agree to be bound by the Approved Addendum, which is incorporated into this Agreement by reference and completed by the tables below. Entering into this Agreement has the same effect as signing the Approved Addendum and the EU SCCs incorporated into it.

Part 1: Tables

Table 1: Parties

- Start date: the effective date of this Agreement.
- Exporter: the Controller, as identified on the first page of this Agreement. Importer: EverReady SAS, as identified on the first page of this Agreement.
- Key contacts: as set out in Article 16 of this Agreement.

Table 2: Selected SCCs, modules and selected clauses

- The version of the Approved EU SCCs to which this UK Addendum is appended is that referred to in Article 1 and completed by Article 8.2 of this Agreement, including the modules and optional clauses selected therein.

Table 3: Appendix information

- Annex 1A (list of parties): as set out in Table 1 above and on the first page of this Agreement;
- Annex 1B (description of the transfer): as set out in Schedule A and Schedule B of this Agreement;
- Annex II (technical and organisational measures): as set out in Schedule C of this Agreement;
- Annex III (list of sub-processors, modules two and three only): as set out in Schedule B of this Agreement.

Table 4: Ending this Addendum when the Approved Addendum changes

Either Party may end this UK Addendum in accordance with Section 19 of the Approved Addendum.

Interpretation

Where the Approved Addendum uses terms defined in the EU SCCs, those terms have the same meaning. This UK Addendum must be interpreted in a manner consistent with UK Data Protection Laws and so as to provide the appropriate safeguards required by Article 46(2)(d) of the UK GDPR.

Where there is any inconsistency or conflict between the Approved Addendum and the EU SCCs, the Approved Addendum prevails, except where the conflicting terms of the EU SCCs provide greater protection for data subjects.

The UK Addendum, including the EU SCCs incorporated into it, is governed by the laws of England and Wales, and any dispute arising from it shall be resolved by the courts of England and Wales. A data subject may also bring proceedings against the Exporter and/or the Importer before the courts of any country in the United Kingdom.

The amendments to the EU SCCs set out in Section 15 of the Approved Addendum apply, including the replacement of references to Regulation (EU) 2016/679 with references to UK Data Protection Laws, the replacement of references to the European Union and its Member States with references to the United Kingdom, and the replacement of the competent supervisory authority with the Information Commissioner.