celo

Data Processing Agreement

Data Processing Agreement

This Processor Agreement ('Agreement') is an agreement between the user (s) of the Celo Platform ('Controller') and Celo Limited, or any of its subsidiaries ('Processor').

This Agreement forms part of the Contract for Services under the Celo Terms and Conditions of Use.

Whereas
(A) You act as the Data Controller ('Controller') for all 'User Generated Data.'
(B) You act as the Data Subject for 'Celo User Data.'
(C) You wish to subcontract certain Services, which imply the processing of Personal Data, to Celo Limited ("Processor").
(D) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
(E) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:
PARTIES
(1) Celo, or any of its subsidiaries ('Processor')
(2) Healthcare Organization / Healthcare Worker / Healthcare Provider / Authorized User ('Controller')

Celo means all companies in the Celo group of companies including Celo Limited, Celo Health Pty Ltd and Celo Health, Inc. The contact details for these companies is listed at bottom of this document. You can contact us at any of the locations listed in this document.

The Agreement

(A) The Processor has developed a secure communication, collaboration and community platform for healthcare known as "Celo."
(B) The Processor provides Celo as a platform that can be used on an end-user's mobile device or desktop device and software that is provided as a service and runs under the control of the Processor on remote servers.
(C) The Processor provides various additional services such as implementation, training and consulting services in support of its software application.
(D) The Controller wishes to use the Processor's software and services as an individual health provider or in its healthcare organization and the Processor has agreed to provide the software and services.

This Agreement comprises:
- The Agreement
- General Terms and Definitions
- Data Processing Agreement

By using the Celo Platform you are agreeing to this Data Processing Agreement set forth herein. We recommend that you also read the policies and agreements at: https://www.celohealth.com/legal

General Terms and Definitions

Acceptable Use Policy: The policy issued by the Processor from time to time concerning use of the Celo Platform in accordance with good practice and healthcare standards.

Agreement: This Data Processing Agreement.

Authorized Users: Individuals who are authorized to access and use the Celo Platform, as described here:

Authorized Users are users that have set up a Celo account. The Processor also carries out additional checks on its authorized users. These checks include Workplace, Identity and Profession Verification.

In order to ensure secure use of the Celo Platform, The Processor reserves the right to restrict access to the Celo Platform depending on the level of verification of a user.

Each Authorized User is required to comply with the **Celo Acceptable Use Policy, Terms and Conditions of Use and Privacy Policy.**

Celo User Data: The Personal Data belonging to Authorized Users of the Celo Platform.

Celo Platform: The Processor's proprietary software, a secure communication, collaboration and community platform for healthcare .

Controller, Processor, Data Subject, Data concerning health, Personal Data, Personal Data breach, Processing and Appropriate Technical and Organizational measures: as defined in the Data Protection Legislation.

Data Protection Legislation: The Data Protection Act 2018 implementing the General Data Protection Regulation (EU) 2016/679 as amended or updated from time to time, automatically including any updates made to UK legislation.

General Data: The Data that is general in nature, is not User Generated Data or Celo User Data.

Personal Data: Includes User Generated Data and Celo User Data.

Privacy Policy: The Processor's privacy policy is updated from time to time which can be found at **https://www.celohealth.com/legal**.

User-Generated Data: The data inputted into the Celo Platform by the Controller, by Authorized Users, or by the Processor on the Controller's behalf. This includes, but not limited to patient health data.

Virus: Anything or device (including any software, code, file or program) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by rearranging, altering or erasing the program or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

Data Processing Agreement

Personal Data
For the purposes of this Data Processing Agreement, it is acknowledged that Celo is both a data controller and data processor of Celo User Data. Our Celo users are the data subjects.

It is further acknowledged that the Authorized Users of the Celo Platform are the controllers of User Generated Data and Celo is the processor of User Generated Data.

The terms of the Privacy Policy shall apply in relation to Celo's processing of both the Celo User Data and the User Generated Data.

Processing of data including both Celo User Data and the User Generated Data by the Processor is done in full compliance with the Data Protection Legislation.

Data Processing
The Processor (Celo) shall:

- process Personal Data only to the extent and in such manner as is necessary for the performance of the Services and solely for the purposes set out in the Privacy Policy and shall not process the Personal Data for any other purpose unless the Controller is required by the laws of any member state of the European Union to process the Personal Data and in such case, the Processor shall promptly notify the Controller of this before performing the processing required by such laws unless such laws prohibit the Processor from notifying the Controller;
- only process Data in accordance with the Controller's instructions.

Retention and Deletion of Personal Data

- The Celo platform has the option to delete or export user data on or from its devices and accounts. Your systems will, following a delete action on the Celo platform, delete all user data that is still stored on your systems, except for any retention or backup periods that you apply. User data sent to other users of the Celo Platform are under the control of those users and are not part of any actions as described above.
- Celo establishes all retention periods in our data retention schedule and ensures that retention periods are observed by deleting the respective data. For Celo Enterprise customers, custom data retention schedules can be specified according to their requests.
- After the Processor Agreement ends, you should take all necessary actions to delete all necessary user data from the Celo Platform, and ensure that all necessary associated data processed by Celo and its subprocessors should be destroyed except if further storage of the data is required for example to comply with relevant healthcare data retention laws.
- To learn more about our data retention schedule, please contact us.

Security Measures
The Processor shall take all appropriate technical and organizational measures against the unauthorized or unlawful processing of Personal Data.

The Controller will monitor and update, as necessary, the measures it takes in order to ensure the security of Personal Data.

Please see the Security page on our website to learn more.

Employees
The Processor shall ensure:

a) that it takes reasonable steps to ensure the reliability of any of the Processor's employees who have access to the Personal Data;
b) that access to the Personal Data is limited to only those employees who need access to meet the Processor's obligations under this agreement;
c) that access is restricted, in the case of any access by any employee, to such part or parts that are strictly necessary for the performance of that employee's duties;
d) that all of its employees involved with the Services are obliged to keep the Personal Data confidential and have received comprehensive training on the Data Protection Legislation and related good practice.

Subprocessors
The Processor may only authorize a third party (sub-processor) to process the Personal Data:
a) subject to the Controller's prior consent (which shall not be unreasonably withheld) where the Processor has supplied the Controller with full details of such sub-processor; and
b) provided that provisions relating to data processing and data protection in the sub- processor's contract are on terms which are substantially the same as those set out in this Data Processing Agreement.

The Controller hereby authorizes the processing of Personal Data by the following Sub-Processors:

Subprocessor	Microsoft Azure
Information	Celo uses Microsoft Azure as our Cloud provider.
Where is data stored?	Data is stored as per our Celo Cloud Policy. This document is available to download at: https://www.celohealth.com/legal
What data is processed?	• Celo user data • Celo user generated data • Celo operational data
More info	All Celo data is transparently encrypted to ensure safety; user generated data is encrypted additionally on top of the transparent encryption. For more information see: https://azure.microsoft.com/en-us/support/legal/

Subprocessor	Twilio
Information	Celo uses Twilio for VOIP calling and SMS messaging services. These include: • Programmable Voice • Programmable SMS
Where is data stored?	Twilio is hosted by AWS with data centres located in the following regions: https://www.twilio.com/docs/global-infrastructure/edge-locations#public-edge-locations

What data is processed?	• SMS text message content • Voice call metadata such as call logs and call length
More info	Please Visit: https://www.twilio.com/legal/bcr/processor https://www.twilio.com/legal/security-overview

Subprocessor	SendGrid
Information	Celo uses SendGrid for outgoing emails
Where is data stored?	SendGrid uses Twilio infrastructure and leverages, Twilio data centers, provided by Zayo and Centurylink, and located in the United States.
What data is processed?	Celo outgoing emails may contain Celo user information such as names (first, last, preferred), temporary passwords, and other encrypted tokens to verify user identity and claims.
More info	Please Visit: https://www.twilio.com/legal/security-overview

Subprocessor	AppsFlyer
Information	User acquisition attribution
Where is data stored?	United States See more info here: https://www.appsflyer.com/product/gdpr-ccpa https://www.appsflyer.com/services-privacy-policy/
What data is processed?	No personally identifiable data.
More info	Please Visit: https://www.appsflyer.com/product/gdpr-ccpa https://www.appsflyer.com/services-privacy-policy/

Subprocessor	Google Analytics
Information	Celo uses Google Analytics to better understand the way users interact with our Celo app and website. This is essential to ensure we continue to improve our service to better serve our customers. Data sent to Google only reflects user behaviour and never includes any personally identifiable data.
Where is data stored?	Google Analytics data centres: https://www.google.com/about/datacenters/locations/index.html

What data is processed?	No personally identifiable data.
More info	Please Visit: https://www.google.com/analytics/terms/us.html

Subprocessor	Onfido
Information	Celo uses Onfido as our trusted identity verification provider. By verifying Celo users' identity, we ensure Celo remains a safe and trusted healthcare community.
Where is data stored?	Onfido Data is processed and stored on AWS EU-West-1 (Ireland) then backed up on AWS EU-Central-1 (Germany). Onfido is ISO 27001, SOC Type 2 certified and GDPR compliant.
What data is processed?	• Identity documents, e.g. passport or driver's license • A video and/or photo of yourself
More info	Please visit: https://onfido.com/security/ https://onfido.com/privacy/

Subprocessor	Zoom
Information	Celo uses Zoom Video SDK as our trusted video calling provider. By using the Zoom Video SDK, we ensure Celo remains a safe and trusted healthcare community and provide secure and compliant video calling functionalities to our end users.
Where is data stored?	Zoom Data is processed and stored on respective Zoom regions. Zoom is HIPAA and GDPR compliant.
What data is processed?	• Video call metadata. • A video and/or photo of yourself
More info	Please visit: https://explore.zoom.us/en/trust/privacy/ https://explore.zoom.us/en/trust/security/

Rights of Data Subjects

Processor shall assist the Controller by appropriate technical and organizational measures, as far as reasonably possible, for the fulfillment of Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in articles 12 to 23 GDPR (Rights of the data subject). Parties will discuss in good faith the reasonable allocation of the costs involved.

Any complaint or request from a Data Subject regarding the Processing of User Generated Data is forwarded without delay by Processor to Controller. Controller is responsible for handling the request.

Compliance

The Processor shall:

- promptly comply with any request from the Controller requiring the Processor to amend, transfer or delete the Personal Data
- provide, at the Controller's request, a copy of all Personal Data held by it in the format and on the media reasonably specified by the Controller;
- delete the Controller's Celo User Data on request of the Controller;
- notify the Controller without undue delay if it becomes aware of any unauthorized or unlawful processing, loss of, damage to or destruction of Personal Data;
- maintain complete and accurate records and information to demonstrate its compliance with this Data Processing Agreement;
- maintain the integrity of the Personal Data, without alteration, ensuring that the Personal Data can be separated from any other information created.

Records and Audit

The Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations laid down under this Data Processing Agreement.

The Controller is entitled, on giving at least 5 days' notice to the Processor, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by the Processor. This requirement to give notice will not apply if the Controller believes that the Processor is in breach of any of its obligations under this Data Processing Agreement.

Should you need to contact the DPO of Celo, you can do so by email: dpo@celohealth.com

More Information

To learn more about our service, pricing and data protection and security on the Celo Platform, please visit https://www.celohealth.com/legal/

Our contact details

If you wish to get in touch with Celo, please do so by using any of the following contact details:

Celo New Zealand Head Office
Celo Limited
Level 1, 63 Ponsonby Road, Auckland,
New Zealand, 1011

Celo United States of America
Celo Health, Inc.
2815 Elliott Ave Suite 100
Seattle
WA 98121
United States

Celo United Kingdom
Celo Limited
Grosvenor Gardens 52, Grosvenor Gardens,
Belgravia, London,
United Kingdom, SW1W-0AU

Celo Australia
Celo Health Pty Ltd
3/45 Watt St, Newcastle, NSW,
Australia, 2300

Contact details
support@celohealth.com