GCO and CDA Privacy and Cookies Policy

Contents

1. Our Role and Responsibilities 1
2. Your Role and Responsibilities 1
3. When and How We Collect Data 1
4. Why We Use Your Data 3
5. Legal Basis Explained 4
6. Sharing Your Personal Data 5
7. Transferring Your Personal Data 5
8. Cookies and Similar Technologies 6
9. Storing and Deleting Your Data 7
10. How We Secure Your Personal Data 7
11. Children's Data 7
12. Your Data Protection Rights and Choices 8
13. How to Exercise Your Rights 9
14. Changes to this Policy 10
15. Contact Us 10

1. Our Role and Responsibilities

Ascensia Diabetes Care Holdings AG ("Ascensia," "we," or "us") acts as the "controller" of your personal data that you provide through the Contour Diabetes App ("CDA") and / or glucocontro.online ("GCO") (together the "Apps"). This means that we determine how and why your personal data is collected, used and stored.

2. Your Role and Responsibilities

If you are a user of one or both of these Apps, whether as a patient, caregiver, or healthcare professional, this Privacy and Cookies Policy ("Policy") applies to you. Please read the Policy. It contains important information about what personal data we collect, why we collect it and what we do with it. Some sections, where indicated, apply only to patients or healthcare professionals, or only to the CDA or GCO.
For residents of Washington and other US States with consumer health privacy laws, please also see our separate Consumer Health Privacy Policy.

3. When and How We Collect Data

Some data is provided directly by you and some data is automatically collected. We collect data after you have reviewed this Policy and when you use the Apps (for example, on the initial CDA screen if you provide a date of birth, and choose to provide a name, we do not store this data at this point). Once you complete your registration for an account, your personal data will then be backed up to the cloud. Creating an account with either of the Apps will ensure that the meter you (or your dependents or your patient) pair with the App can synchronize information and settings, such as target ranges, with the Apps.

Please read the table below to understand the types of data we collect and where this data comes from.

	Types of Data We Collect
<u>Data you provide</u> We do not collect these types of data unless you provide them to us	**Contact and Personal Details** For example, your name, email address, gender, and date of birth. We also collect your phone number if you want to use this as extra security for log-in. For healthcare professionals we will additionally collect office location and company name
	Location Data The country where you live. Where you agree and have turned on location services during the registration process for the Apps, we will collect information about your precise or approximate location from information derived from your mobile device. We use this information to improve our products and services, including to identify the distribution of meters
	Authentication and account registration details This includes passwords and preferred language, and biometric data (considered sensitive data in some countries), such as fingerprint or faceprint, if you choose to enable this feature on your device, or need to use the parental consent process so your child can access the Apps.
	Sensitive Data For patients, information about how you manage your diabetes, for example your diabetes type, medications, insulin, food consumption and exercise regime, your hospital address and hospital attendance dates, healthcare professional reports, blood glucose readings, A1c data, and information about your meter, such as meter model number, serial number and settings
	Third Party Apps and Mobile Device Data For patients, depending on your mobile device operating system, you may be asked if you want to give access to certain system services on your device, such as camera, photos and contact list. Access to these system services allows certain optional features of the CDA to function properly, and does not result in Ascensia having access to, collecting or storing any information relating to such system services. In addition, access to any third party apps you choose to connect to the CDA, such as the Apple Health app (if you would like to share health-related data with Apple Health, and it is available in your country) You can change access approvals at any time through the settings on your mobile device or the CDA's settings
	Customer Services If you contact us for support, we will keep a record of that contact. You may provide us with personal data by completing forms by e-mail as part of an order for products or services, where you have enquiries or requests or when you report a problem with the Apps and similar situations where you choose to give us your data

Automatically Collected Data In some cases, we automatically collect data once you begin using the Apps, for example via cookies and similar technologies	**Technical Data** Including the type of mobile device you use, a unique device identifier (such as a universal unique identifier (UUID), MAC address of the device's wireless network interface, or the mobile phone number used by the device), your mobile operating system and software version number, the type of mobile browser you use, the country and language code and time zone setting. The UUID is a number which is generated for each App installation on your mobile device or browser (as applicable), allowing Ascensia to synchronize data to enable end-to-end display of information in the Apps on all devices, if you log in from multiple devices. If a user deletes the Apps or clears the browser history (as applicable), the UUID is no longer usable

If you provide us with personal data related to anyone other than yourself (such as a healthcare professional, patient or family member), you are responsible for complying with all data protection and privacy laws before sharing that information with Ascensia (including obtaining their permission, if required).

4. Why We Use Your Data

We must have a legal basis, i.e. a justifiable reason to use your data. For more information on what these legal bases mean, see **Legal Basis Explained** below.



Delivery of Services

(1) Permitting patients to send blood sugar reports to their care team, (2) connecting to other third party apps, where available (e.g. Apple Health), (3) presenting information to patients about their blood glucose testing and measurements to understand patterns and trends, (4) allowing participation in interactive features of the Apps, (5) notifying you of changes to our services, (6) issuing safety notices or corrective action, (7) providing you with cloud services relating to the Apps or connected devices.

Legal Bases: Contract | Consent | Legal obligation



Product Improvement

(1) Developing and testing new features of the Apps, devices and consumables, such as test strips (2) fixing issues with the Apps or account services, (3) conducting data analysis and research, including understanding the most effective areas to focus sales activity, and to identify the distribution of the Apps and meter users (4) implementing security tools to keep the Apps safe and secure, (5) better understanding how you interact with the Apps, including their features, as well as ensuring that content is presented in the most effective manner, (6) performance, impact and experience.

Legal Bases: Contract | Consent | Legitimate interest | Public interest in the area of public health



Customer Service

(1) Responding to requests for support with the Apps or your account(s), (2) helping fix any issues with the Apps or your account(s), including where we respond to your questions regarding maintenance, troubleshooting, or other performance issues.

Legal Bases: Contract | Consent



Research

(1) Evaluating the performance, impact, and experience of the Apps and account services on users, (2) reviewing our operating and business strategies for research and development, (3) conducting statistical analysis related to diabetes, (4) determining and improving the effectiveness of diabetes management techniques, therapies, treatments and costs, (5) scientific research relating to diabetes, including publishing articles in medical and/or peer-reviewed publications and journals, and presenting at conferences.

Legal Bases: Legitimate interest | Public interest in the area of public health

Marketing

(1) Inviting users to participate in surveys or opinion groups related to the operation and use of the Apps or other promotional activities, including with selected third parties (2) recommending products or services that may be of interest to users, (3) understanding the effectiveness of advertising we may serve and to deliver relevant advertising

You may withdraw your consent to receive marketing messages at any time by contacting us or clicking the unsubscribe link in our messages. If you withdraw your consent, we will continue to contact you for non-marketing related purposes (for example, to send important information about the Apps).

Legal Basis: Consent

5. Legal Basis Explained

Here is what each of the legal bases mentioned above means:

Consent

You have agreed that we can handle your personal data for a specific purpose. For example, you have agreed to receiving marketing emails with product offers.

If you have previously given consent, you can withdraw this consent at any time. For example you can withdraw your consent to our collection of your location information by disabling the use of location services in your device's settings menu.

Contract

Handling your data is necessary for a contract you have with us. For example, to provide you with the Apps and respond to your questions regarding maintenance, troubleshooting, or other performance issues.

Legitimate interests

Handling your data is necessary for the so-called legitimate interests of Ascensia or a third party, and these interests are not outweighed by your rights and interests. Our legitimate interests include:

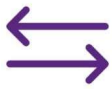
- Developing, improving, and testing new features of the Apps;
- Evaluating the performance, impact, and experience of the Apps; or
- Implementing security tools to keep the Apps safe and secure

Legal Obligation

Handling your data is necessary to comply with the law. For example, issuing safety notices or corrective action related to a medical device that you, your patient, or your dependent uses.

Public interest in the area of public health
Handling your data is necessary for public health reasons. For example, conducting statistical analysis related to diabetes and ensuring high standards of quality and safety of medical devices.

6. Sharing Your Personal Data



We do not rent or sell your personal data to anyone. When necessary, or requested by you, we share your information with:

- For healthcare professionals, you can choose to share your data with your colleagues working in the same clinic or office.
- For patients, third parties you ask us to share your data with to assist you in managing your diabetes:
    - where connections with third-party apps are available in your country and you agree to the sharing of your, for example, meal markers;
    - where you want to share health-related information with a doctor, nurse, medical provider, or other person of your choice.
- Your local Ascensia company or another company within the group of companies of which Ascensia is a member, helping us to provide our products and services to you;
- Distributors of our products if you live in a country where we use a distributor;
- Our service providers involved in the development, provision, troubleshooting, or fixes of the Apps or other services to you;
- Our selected partners where you have chosen to participate in surveys, opinion groups, or other marketing-related initiatives; or
- A prospective seller or buyer, in the event of a sale or purchase of any Ascensia business or asset, so that the buyer can continue to provide you with information and services.

Your data is only shared according to the safeguards in this Policy.

We may disclose your personal data where required to respond to authorized requests from government authorities or where required by law. We may also disclose your personal data when necessary to enforce or apply our Apps' Terms, or this Policy.

7. Transferring Your Personal Data



Your personal data in your account will be stored on servers located in one of our regional facilities, which may include data hosted with one of our service providers. If you are a resident of a country with data localization laws, your personal data will be stored on servers located within your country. We otherwise endeavor to store your personal data within the region where you reside. This means, for example, that data of European users is stored in France, and Germany, data of users in Asia is stored in Australia, and data of US users is stored in the US. There are limited circumstances where your data may move outside those regional facilities:

- Where we produce statistics from user data for reports, using tools provided by partners, for example in the US. Individuals cannot be identified from these reports.
- To develop the Apps, and to administer and provide you with support and technical services for your account.

Since we operate around the world, some of our colleagues, and the partners we work with, will be outside the country where you live (or in which we provide the services), for example in India. If a data protection authority does not consider a country to have adequate levels of protection for personal data, we will implement appropriate safeguards, to protect your personal data if it is transferred. In most cases, the measures will include appropriate data transfer agreements with recipients of the information (such as Standard Contractual Clauses, and the equivalent contracts in the UK, Switzerland, China and elsewhere). Where applicable we will also perform a transfer impact assessment, and then take any further steps required, such as additional security measures. For more information about how your data is stored and transferred please contact our Data Protection Officer: dp_office@phchd.com or by mail at Ascensia Diabetes Care Holdings AG, Peter Merian-Strasse 90, 4052 Basel, Switzerland.

8. Cookies and Similar Technologies



Ascensia does not use cookies in the CDA. Instead, we use iOS and Android Software Development Kits ("SDKs"), which receive data (non-health related) generated through CDA usage to remember things about you so that we can provide you with a better experience. We receive this information only in a form that does not personally identify users. We use the following main SDKs in certain countries:

- Microsoft Azure SDK – collects statistical data relating to:

1) Number of times users visit a particular screen; and
2) Number of times users click on items on a particular screen.

This data cannot be tracked back to an IP address or segregated to a specific user. It allows us to improve the CDA for all users, for example by changing screens that cause many users to pause in the journey, which might suggest confusion with language or design of the CDA.

- Google Firebase Analytics – for notification messages.

GCO uses an analytics tool to track user behavior on the website, recording how users interact with the website, and non-personal data about them, such as device type (desktop, mobile, tablet), browser (Chrome, Firefox, Safari, etc.), screen resolution, and country.

GCO also uses cookies. Cookies are small data files stored on your browser or device. We make certain websites accessible via GCO and use cookies to collect information about your interactions with these websites:

- **Strictly necessary cookies:** Required for example to enable you to log into secure areas of the web-based App, to move around the website and to use its features;
- **Functionality cookies:** These cookies recognize you when you return to our web-based App. This enables us to personalize content for you, for example by remembering your preferred language; and
- **Analytical/performance cookies:** Allows us to recognize and count the number of visitors, and to see how visitors move around certain web pages made accessible via GCO. This helps us to improve the way GCO works, for example, by ensuring that users easily find what they want.

Some of these are persistent cookies that may be used if you log on to restricted areas to remember who you are. Others are session cookies that may be used for anonymous identification of a website visit for technical purposes only. Session cookies are stored only temporarily during the browsing sessions and are deleted once the browser is closed.

We do not respond to browser "Do Not Track" signals.

9. Storing and Deleting Your Data



If you would like to delete your account, you may do so by using the "Delete Account" option in the Apps or contacting us.

If you delete your account, we will keep aggregated and de-identified information. We may also need to keep certain personal data as required by law. Where we are not otherwise subject to a legal requirement to keep records, we will keep:

- Aggregated and de-identified information for **five years** for audit purposes;
- All other data in your account for **two years** from the date it is uploaded to enable you to access and export such data, if required, in connection with an insurance claim.

Once your account and any associated personal data have been deleted, you will no longer have access to the account and deletion of your account may be irreversible. You may not therefore be able to reactivate your account to export data, and your personal data will be deleted. To avoid any issues, you may want to download and save any required information before deleting your account or requesting that we delete your account.

If you have chosen to share your account information with your healthcare provider and you delete your account, those people will no longer be able to synchronize with your account information, including information about your blood glucose readings. Any historical data shared with your healthcare provider will likely need to be retained as medical records, in line with local laws.

We can delete accounts that remain inactive for an extended period of time. If we choose to exercise this right, we will tell you in advance so that you can ensure your account stays available for your use.

10. How We Secure Your Personal Data



We take all reasonably necessary steps to safeguard the security, confidentiality and integrity of your personal data, for example, encryption of your password. We also impose contractual restrictions and take other reasonable steps to prevent your personal data being used to train commercial large language models.

We recommend that you use strong password security by using a unique password with a mix of numbers, letters, and symbols. You should not share your password with anyone. Ascensia is not responsible for any lost, stolen or compromised passwords or for any access to your account from unauthorised users, where caused by you. If you believe your account has been compromised, please contact us immediately.

Remember, no transmission of information is 100% secure. Any information transmitted is at your own risk, and this includes if you choose to connect to a third party app. Any personal data you share with a third party will be governed by that third party's privacy policy and terms and conditions.

11. Children's Data

Prior to collecting data from children, we ask for consent from the child's parent or guardian.

The age that a person is considered a child varies in different countries. Because of this, we ask users to provide their location prior to completing the registration process.

If you are located in the United States and have questions about Ascensia and the Children's Online Privacy Protection Act or similar laws, you may also contact our US company directly at Ascensia Diabetes Care US Inc., 5 Wood Hollow Rd, Parsippany, NJ 07054 USA or via privacy.us@ascensia.com.

12. Your Data Protection Rights and Choices

As a user of the Apps, you can exercise certain rights and choices regarding Ascensia's collection, use, and sharing of your personal data. Please see below for information on how to exercise these rights.

Firstly, you can choose how you use the Apps. For example, as a patient: i) you can choose not to provide us with your personal data. This means some features may not be accessible, for example, users who choose not to give the CDA access to their phone's camera will be unable to upload meal photos in the CDA; and ii) once you have created an account you can choose to use the CDA offline, without a connection to the cloud. This means you cannot see your historical readings or patterns in the CDA, but rather what is available on your blood glucose meter.

Not all these rights are available in every country but if you want to know if the rights below apply to you, please contact dp_office@phchd.com:

Rights

Right of access / right to know

You have the right to access the personal data belonging to you that we hold.

Right to rectification

You have the right to change or modify the personal data you provide us when you believe the data is inaccurate or outdated.

Right to erasure

You can ask us to delete any personal data we hold about you, if it is no longer necessary for us to hold that data.

Right to data portability

You have the right to receive the personal data we hold about you, in a commonly used format, to send the data to another controller or use it for your own purposes.

Right to restriction

You have the right to limit the way that we use your data if you have a particular reason for wanting the restriction. If you request restrictions, we will temporarily stop handling the restricted data. We will inform you before lifting this restriction and resuming use.

Right to object

You have the right, at any stage, to object to our handling of your personal data.

Right to avoid automated decision-making

You have the right not to be subject to a decision based solely on automated processing which produces legal effects concerning you.

Right to lodge a complaint

You have the right to lodge a complaint about how we use your personal data with the relevant regulator in your country.

Additional rights for residents of California or specific other US States

Non-discrimination

We will not discriminate against you if you choose to exercise your privacy rights.

Right to limit use and disclosure of sensitive personal data

You can limit our use of your sensitive personal data to that which is necessary to perform the services or provide the goods requested by you.

13. How to Exercise Your Rights

You may be required to verify your identity when you contact us to make a request to exercise your rights, for example by providing evidence that matches information maintained by Ascensia such as verifying name, or mailing address, if maintained in our records. We must verify your identity to ensure that you are the person authorized to make the request for your own personal data, or on behalf of someone.

Our California Privacy Disclosure explains how we collect, use and disclose the personal information of California residents subject to the California Consumer Privacy Act, amended by the California Privacy Rights Act. This Disclosure also applies to residents of other US States with similar privacy laws, as applicable.

If you are a resident of California or specific other US States, with certain legal exceptions and limitations, you may exercise your privacy rights, as explained below.

You may use an authorized agent to exercise your rights on your behalf. You must provide your authorized agent with written permission to exercise your rights on your behalf and we must be able to verify the agent's identity as described above.

Residents of California and other specific US States:

Call (800) 348-8100

Via our webform located on our *website.* If submitting a request via our webform, please indicate which right your request relates to in the "Message" section.

Email: privacy.us@ascensia.com



Residents of Rest of World (where rights apply):

Email dp_office@phchd.com; or

Mail to: Ascensia Diabetes Care Holdings AG, Peter Merian-Strasse 90, P.O. Box 4052, Basel, Switzerland

14. Changes to this Policy

Any future changes to this Policy will be posted on this page and, at our discretion, provided to you by e-mail or via a notification in the App.

15. Contact Us

Please share any questions or requests regarding this Policy by email (dp_office@phchd.com).

Last updated: June 2025