Ditto Privacy Policy Mobile App

Summary

- **Your privacy first**: Your medical data stays encrypted on your device
- **Secure processing**: Only when you request AI functionality, for a conversation summary or explained document, your data leaves the Ditto app to be processed on our secure servers within the EU. No individual at Ditto accesses your data and we delete it directly after processing.
- **Your data is yours alone**: We never train our AI on your data.
- **No tracking**: We don't do cross-app tracking or share your data with third parties
- **Minimal collection**: We only collect the minimum data needed to provide our service, e.g. technical logging and anonymous app analytics

As soon as you download and use our Ditto Care mobile application ("Ditto app") or contact us, we receive information about you. In this privacy statement, we explain what we do with that information. We always handle your information with care and store it securely. If you have any questions or want to know what information we have on you, please contact us. We may amend this privacy statement if necessary. We recommend that you regularly review this privacy statement so that you are aware of these changes. This privacy statement was last modified on 10 April 2025.

Glossary of Terms

In clear, understandable language

- **Anonymized Data**: Information that has had all identifying details removed so no one can tell it's about you. It's like removing your name and address from a survey before sharing the results.
- **Data Controller**: The company (Ditto Care B.V.) that decides why and how your information is used. We're responsible for keeping your data safe.
- **Encryption**: A way of scrambling your information so only authorized people with the right "key" can read it. It's like putting your data in a locked safe.
- **GDPR**: A set of rules created in Europe to protect people's personal information and give you control over your data.
- **Personal Data**: Any information about you - like your name, email, phone number, or anything else that could identify you.
- **Processing**: Anything we do with information, such as collecting, storing, or using it.
- **SDK (Software Development Kit)**: Pre-made building blocks that help us create our app without starting from scratch.
- **Special Category Data**: Extra sensitive information that gets special protection, like health information or medical records.

Contents

1. When do you apply this privacy statement?

This privacy statement applies to all personal data that we process in connection with the Ditto app and to all domains related to us. This concerns the personal data of everyone who has ever had contact with us or used our mobile application, such as app users, customers, and business contacts. Personal data is all data that can be traced back to you as an individual, such as your name, telephone number, IP address, device identifiers, or health information. If you want to know more about personal data, please visit the website of the relevant Data Protection Authority in your country.

The Ditto app is currently only available in the Netherlands.

2. Who uses your data?

Ditto Care B.V. is responsible for the Ditto app and therefore the responsible organisation (data controller) for the use of your personal data as described in this privacy statement. The full details are:

Ditto Care B.V. Hofplein 19 3032AC Rotterdam The Netherlands KvK: 94952736

3. Whose data do we use?

We process the personal data of everyone who has had contact with us or used our Ditto app. These include app users, private customers, business customers, and contact persons of our partners.

4. How do we get your data?

We receive the data directly from you as soon as you:

- download and install the Ditto app
- create an account within the app
- input medical or health data into the app
- use any features or functionalities of the app
- grant permissions to the app (such as camera, location, etc.)
- contact our customer support

5. What data of you do we use?

We carefully distinguish between data we need to process to deliver our services and data we never have access to:

Data we process to deliver our services

Basic Identity Data:

- name
- e-mail address
- telephone number

Account Data:

- app preferences and settings

Medical and Health Data:

- medical documents that you request to have summarized or explained
- conversation recordings that you request to have summarized

Data we process only anonymously

Device Data:

- device type and model (anonymized)
- operating system version (anonymized)
- unique device identifiers (anonymized)

Usage Data:

- app features used (anonymized)
- time, frequency, and duration of app use (anonymized)
- app performance data (anonymized for technical excellence)

Data we can never access

Credentials:

- login credentials (encrypted and never leave your device)
- biometrics data used to lock the Ditto app

Medical and Health Data:

- any medical data that you add to the Ditto app that you don't have processed

Special note on Medical Data: All medical and health data is stored in encrypted form exclusively on your local device. We are never able to access or inspect this data. The only exception is when you explicitly initiate AI processing functionality (by pressing the record button or explaining a document), at which point the specific data you chose to process is temporarily processed on our secure servers. This processing includes transcription of conversations, summarization of transcripts, and simple summarization of uploaded medical documents. We never train our AI models on your medical data. After processing is completed, this data is completely deleted from our systems, with only technical and anonymous logging files retained.

6. What do we use your data for?

We only use your personal data for the specific purposes for which we are legally permitted:

Provision of Services: To provide you with the functionality of the Ditto app, including the secure storage of your medical data on your device. The Ditto app functions primarily as a productivity tool that helps you log relevant information and get summaries from your data. We do not provide medical advice.

Processing with Explicit Consent: When you specifically request AI processing of your medical data (by pressing the record button or explaining a document), we temporarily process this data on our secure servers based on your explicit consent. This processing is solely for the purpose of transcribing conversations, summarizing transcripts, and providing simple summaries of uploaded documents. You'll be notified of this behavior the first time you use this feature.

We never train our AI models on your medical data. We may run anonymous security and safety checks to ensure your AI output is reliable and safe, but the contents of the medical data are not stored—only technical performance data may be anonymously stored to ensure our AI models remain reliable.

Basic Functionality Without Account: You can use the app's basic functionality without an account. This includes manually logging appointments with attached photos and documents, and making audio recordings without server-side processing. For technical reasons, an account is needed to leverage AI functionalities.

Technical Functionality: To ensure the app functions properly, including troubleshooting, data analysis, testing, and system maintenance.

Security and Compliance: To verify your identity, prevent fraud, and ensure compliance with our legal obligations regarding medical data protection.

Service Improvement: To analyze usage patterns in anonymized, aggregated form to improve our app's functionality and user experience.

Communication: To respond to your inquiries, provide customer support, and send you important notices about the app or your account.

We will not use your data for purposes other than those stated above without obtaining your prior consent.

7. How long do we keep your data?

We keep your personal data for as long as:

- required by applicable law
- necessary for the purpose for which we use your data
- you maintain an active account with us

For account data, we store it for as long as you maintain an active account, plus a period of 30 days after account deletion to facilitate potential account restoration if requested.

For medical data that you process using our AI functionality, this data is only temporarily stored on our servers during the processing operation and is automatically deleted once the processing is completed and delivered to your device. If you are offline when processing completes, we will retain the data for up to 24 hours to allow delivery upon reconnection, after which it is permanently deleted regardless of delivery status.

For technical and usage data, we store technical logging for a maximum of 13 months to facilitate app improvements and troubleshooting.

If you want to know more about how long we store specific data about you, please contact us.

8. Our Commitment to Data Confidentiality

We maintain strict confidentiality of your personal data:

No Data Sharing: We do not sell, rent, or share your personal data with any third parties for their marketing or commercial purposes.

Limited Temporary Processing Only: When you explicitly initiate AI processing of your medical data, this data is temporarily processed on our secure servers operated by Ditto Care B.V. This is not sharing—we remain the sole data controller throughout this process. AI processing is performed primarily within the secure Azure Cloud in European data centers. After processing is completed, the data is promptly deleted from our systems.

User-Controlled Exports: The app itself does not directly integrate with healthcare providers. If you wish to share data with your healthcare provider, you can export summaries yourself from the app. Once you export data, it will be handled by your chosen communication platforms (such as SMS, WhatsApp, or email) and subject to their privacy policies.

Limited Service Providers: We use a minimal number of carefully selected service providers (such as Microsoft Azure for cloud hosting) who are contractually bound to process data only as explicitly instructed by us, in compliance with strict security measures and data protection laws.

Legal Obligations: In extremely rare circumstances, we may be legally required to disclose certain information in response to a court order or other valid legal request.

9. Where do we store and process your data?

We process and store your data exclusively within the European Economic Area (EEA):

- Your medical data is only stored in encrypted form on your local device.
- When you initiate AI processing, your data is temporarily processed on our servers located in European data centers.
- Our infrastructure is built on the Microsoft Azure Platform using European data centers only.
- Any peripheral services we use are also located within the EEA.

This ensures that your data is always protected under EU data protection standards (GDPR).

10. How safe is your data with us?

Data security is our top priority, especially for sensitive medical information:

Local Encryption: All medical data on your device is encrypted using the native encryption functionality provided by iOS (for Apple devices) and Android. We do not manage this encryption or have access to your encryption keys.

Biometric Authentication: The app supports biometric authentication (such as Face ID on iPhones) using the device's native implementation. We never have access to any biometric data, as this is handled entirely by your device's operating system.

Backup Options: Data recovery is only possible through your device's native backup functionality (such as Apple iCloud or Google Drive). As we don't store your data on our servers, we cannot recover your data if you lose your device and haven't created a backup.

Secure Infrastructure: Our infrastructure is built on the Microsoft Azure Platform according to Microsoft security standards, one of the best secured cloud platforms available.

Encryption Standards: We use AES-256 encryption for data at rest and TLS 1.3/HTTPS for data in transit.

Access Controls: We implement strict access controls based on the principles of Least Privilege and Need-to-Know, with Role-Based Access Control (RBAC) governing all data access.

Two-Factor Authentication: Two-factor authentication is enforced for any human access to data and software systems from Ditto.

Regular Security Testing: We conduct regular vulnerability scanning including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and manual penetration testing.

Continuous Monitoring: We maintain continuous monitoring, performance metrics, access logging, and alerting to detect and respond to incidents.

Staff Vetting: All directors, employees, and subcontractors are required to obtain and present a Certificate of Conduct (Verklaring Omtrent Gedrag).

Certification: Ditto Care is in the process of acquiring NEN/ISO certification to further validate our security practices.

If you have specific questions about how we secure your data, please contact us.

11. What are your rights?

Under EU data protection law (GDPR), you have the following rights:

Right to information: We must explain in an understandable and clear manner what we do with your data and what control you have over it. That is why we explain in detail in this privacy statement what data we collect from you and how we handle your data.

Right to access: You may always ask us to view the data we hold about you.

Right to correction: You may ask us to have your data corrected if it is incorrect or incomplete.

Right to object: You may object to the processing of your data if you do not agree with the way we handle your personal data.

Right to data portability: You may ask us to send you the digital data we have about you. Currently, the Ditto app allows you to save recordings to your local device and export generated summaries and explanations. We are committed to data portability and are actively developing a more comprehensive mechanism to export your complete Ditto medical library. We expect to release this enhanced functionality within 2025. In the meantime, our support team can assist with manual data export requests if needed.

Right to restriction: You may ask to limit the use of your data. This means that in certain cases we may only store your data but not use it.

Right to be forgotten: You may ask us to delete all data we have about you. We will then delete all data that can be traced back to you. In some cases we cannot or may not yet delete your data if we have a legal obligation to retain it.

Data Deletion Process: You have complete control over your data and can delete your account with all associated data directly from within the app at any time. Simply go to Settings > Account > Delete Account and follow the on-screen instructions.

When you delete your account:

- All account information is permanently removed from our systems within 30 days
- Since your medical data is stored only on your device (and optionally in your personal iCloud backups), deleting the app from your phone will remove this data entirely
- Any temporary processing data on our servers is immediately deleted
- No personally identifiable information remains in our possession

Please note that if you've enabled iCloud backups on your device, Apple's backup services may retain your app data according to their policies. You can manage these backups through your device settings.

We complete the account deletion process within 30 days of your request, and typically much sooner.

Right to submit a complaint: You may submit a complaint about the way in which we handle your data. If you have a complaint, we will be happy to resolve it for you. To do so, please contact us. You may also submit your complaint to your national Data Protection Authority. Of course we hope that it does not come to that, but if it's necessary you can also go to court. In that case, the court in the place of business of Ditto Care B.V. is the one which will handle your complaint.

How do I submit a request or complaint? You can submit your request or complaint to us by sending an email to privacy@ditto.care. We process every request or complaint within 30 days. If you submit multiple applications or complaints or if you submit a complex request or complaint, this may take more time. In that case, we will contact you within 60 days at the latest. We may ask you to identify yourself. In that case, we will ask you to submit certain information to ensure that you are the correct person whose personal data is involved.

12. Which rules apply to this privacy statement?

Our privacy statement complies with:

- The EU General Data Protection Regulation (GDPR)
- Applicable national data protection laws
- The Dutch General Data Protection Implementation Act (Uitvoeringswet AVG)
- Medical device regulations, where applicable
- Apple App Store guidelines and policies

13. Which tracking technologies do we use?

Unlike websites that use cookies, mobile applications use different technologies to collect and store information:

App Analytics: We use anonymous app analytics to understand how users interact with our app, identify technical issues, and improve the user experience. This does not identify you personally.

Device Identifiers: We may collect unique device identifiers to ensure secure authentication and basic functionality. We do not use these identifiers for cross-app tracking, advertising, or profiling purposes. You can reset these identifiers in your device settings at any time.

Local Storage: We store your medical data and app preferences locally on your device in encrypted form to provide app functionality even when offline.

Push Notifications: With your permission, we may send push notifications to inform you about new app releases, remind you of upcoming events you've entered in the app, and notify you when AI processing of your data is complete. These notifications use only data you've already provided within the app. Push notifications are optional and can be disabled in your device settings.

Third-Party SDKs: Our app includes the following third-party software development kits (SDKs):

1. **Auth0 (v2.10.0)**
    - Accesses user authentication data
    - Processes login credentials
    - Stores authentication tokens
    - May collect email addresses and user identifiers
2. **Firebase Analytics & Crashlytics (v11.10.0)**
    - Collects app usage data and crash reports
    - May include device information (model, OS version)
    - Tracks user interactions within the app

    - Note: We use the privacy-friendly "WithoutAdIdSupport" version for Analytics to enhance your privacy

These SDKs are contractually bound to process data only as explicitly instructed by us and in compliance with applicable data protection laws.

You control your data: You can manage app permissions through your device settings. You can also delete all local data by uninstalling the app, though this will permanently delete any medical data you have stored locally.

14. What do we do with data of minors?

Special Protections for Minors: We recognize that medical information of minors requires special protection:

- Our app is not designed for or targeted at users under the age of 16.
- If you are under 16, you must have permission from a parent or legal guardian to use the Ditto app.
- Parents/guardians of minors are responsible for supervising their child's use of the app and managing the consent for processing their data.
- We implement age verification measures as required by applicable law.
- If we become aware that we have collected personal data from a minor without parental consent, we will take steps to delete that information.

15. Offline Functionality

The Ditto app is designed with offline access as a priority:

- All your medical data is stored locally on your device in encrypted form
- You can view, organize, and manage your entire medical library without an internet connection
- You can reference previously generated summaries and explanations while offline
- You can add new medical documents, photos, and manual notes while offline

An internet connection is only required for:

- Initial account creation and authentication
- AI processing of new data for summaries or explanations
- Receiving app updates and non-critical notifications

This offline-first approach ensures your medical information remains accessible even in areas with limited connectivity, such as hospitals or medical facilities with network restrictions.

16. Other

App Monetization: The Ditto app is free to use for all users. No paid subscription is needed.

Medical Device Classification: The Ditto app is positioned as a productivity tool that helps you log relevant information and get summaries from the data you insert. It does not qualify as a medical device under EU MDR. We don't provide medical advice and always include disclaimers on all output that any information should be carefully checked.

Geographic Availability: Currently, the Ditto app is focused on availability in the Netherlands.

Data Breach Protocol: In the unlikely event of a data breach affecting your personal data, we will comply with all applicable notification requirements under EU data protection law. As we store minimal user data on our servers and medical data is primarily stored only on your device, the risk of significant data breaches is reduced.

Azure OpenAI Service Privacy: When we process your data using AI capabilities, we utilize Microsoft's Azure OpenAI Service with the following privacy protections:

- **No Training on Your Data**: The AI models are stateless – your data is never used to train, retrain, or improve the base models.
- **Regional Data Processing**: All data is processed within European data centers and never leaves the European Economic Area.
- **Content Filtering**: Real-time content filters assess inputs and outputs without storing your data.
- **Abuse Monitoring**: Automated systems monitor for misuse without human review unless specifically flagged. If review is needed:
    - Data remains encrypted and accessible only to authorized Microsoft employees
    - Data is stored separately in the same region as our deployment
    - Data is retained for no more than 30 days
    - For European deployments, reviewers are also located within the EEA

For more information about these privacy protections, you can visit Microsoft's official Azure OpenAI documentation.

17. Do you have a question about this privacy policy?

If you have any questions about our privacy policy or how we handle your data, please contact us at:

Email: privacy@ditto.care Address: Ditto Care B.V., Hofplein 19, 3032AC Rotterdam, The Netherlands

We are happy to help explain any aspects of our privacy practices.