

[For our English privacy policy, click here.](#)

Samenvatting

- **Jouw privacy voorop:** Je medische gegevens blijven versleuteld op jouw apparaat
- **Veilige verwerking:** Alleen wanneer je AI-functionaliteit aanvraagt, voor een gespreksoverzicht of een uitgelegd document, verlaten je gegevens de Ditto-app om verwerkt te worden op onze beveiligde servers binnen de EU. Geen enkele medewerker van Ditto heeft toegang tot jouw gegevens en we verwijderen ze direct na verwerking.
- **Jouw gegevens zijn van jou alleen:** We trainen onze AI nooit op jouw gegevens.
- **Privacyvriendelijke analytics:** We gebruiken Mixpanel en Adjust voor app-verbetering met jouw toestemming. Alle analytische gegevens blijven in de EU en je kunt je op elk moment afmelden.
- **Geen tracking:** We doen niet aan cross-app tracking en delen jouw gegevens niet met derden voor advertentiedoeleinden.
- **Minimale verzameling:** We verzamelen alleen de minimaal benodigde gegevens om onze dienst te leveren, bijv. technische logging en analytics waarvoor je toestemming hebt gegeven.

Zodra je onze Ditto Care mobiele applicatie ("Ditto-app") downloadt en gebruikt, of contact met ons opneemt, ontvangen we informatie over jou. In dit privacybeleid leggen we uit wat we met die informatie doen. We behandelen jouw informatie altijd zorgvuldig en bewaren deze veilig. Als je vragen hebt of wilt weten welke informatie we over jou hebben, neem dan contact met ons op. We kunnen dit privacybeleid indien nodig aanpassen. We raden je aan om dit privacybeleid regelmatig te bekijken zodat je op de hoogte bent van deze wijzigingen. Dit privacybeleid is voor het laatst gewijzigd op 29 oktober 2025.

Verklarende woordenlijst

In duidelijke, begrijpelijke taal

- **Geanonimiseerde gegevens:** Informatie waaruit alle identificerende details zijn verwijderd, zodat niemand kan zien dat het over jou gaat. Het is alsof je naam en adres van een enquête worden verwijderd voordat de resultaten worden gedeeld.
- **Verwerkingsverantwoordelijke:** Het bedrijf (Ditto Care B.V.) dat beslist waarom en hoe jouw informatie wordt gebruikt. Wij zijn verantwoordelijk voor het veilig houden van jouw gegevens.
- **Versleuteling:** Een manier om jouw informatie te versleutelen zodat alleen geautoriseerde personen met de juiste "sleutel" deze kunnen lezen. Het is alsof je jouw gegevens in een afgesloten kluis doet.
- **AVG:** Een reeks regels die in Europa zijn opgesteld om de persoonlijke informatie van mensen te beschermen en jou controle over jouw gegevens te geven.
- **Persoonsgegevens:** Alle informatie over jou - zoals je naam, e-mailadres, telefoonnummer, of iets anders waarmee je geïdentificeerd kunt worden.
- **Verwerking:** Alles wat we met informatie doen, zoals verzamelen, opslaan of gebruiken.
- **SDK (Software Development Kit):** Vooraf gemaakte bouwstenen die ons helpen onze app te maken zonder vanaf nul te beginnen.
- **Bijzondere categorieën van persoonsgegevens:** Extra gevoelige informatie die speciale bescherming krijgt, zoals gezondheidsinformatie of medische dossiers.

Inhoudsopgave

1. Wanneer is dit privacybeleid van toepassing?
2. Wie gebruikt jouw gegevens?
3. Van wie gebruiken we gegevens?
4. Hoe verkrijgen we jouw gegevens?
5. Welke gegevens van jou gebruiken we?
6. Waarvoor gebruiken we jouw gegevens?
7. Hoe lang bewaren we jouw gegevens?
8. Met wie delen we jouw gegevens?
9. Waar bewaren we jouw gegevens?
10. Hoe veilig zijn jouw gegevens bij ons?
11. Wat zijn jouw rechten?
12. Welke regelgeving is van toepassing op dit privacybeleid?
13. Welke tracking-technologieën gebruiken we?
14. Wat doen we met gegevens van minderjarigen?
15. Offline functionaliteit

- 16. Overige informatie
- 17. Heb je een vraag over dit privacybeleid?

1. Wanneer is dit privacybeleid van toepassing?

Dit privacybeleid is van toepassing op alle persoonsgegevens die we verwerken in verband met de Ditto-app en op alle domeinen die aan ons gerelateerd zijn. Dit betreft de persoonsgegevens van iedereen die ooit contact met ons heeft gehad of onze mobiele applicatie heeft gebruikt, zoals app-gebruikers, klanten en zakelijke contacten. Persoonsgegevens zijn alle gegevens die naar jou als individu te herleiden zijn, zoals je naam, telefoonnummer, IP-adres, apparaat-ID's of gezondheidsinformatie. Als je meer wilt weten over persoonsgegevens, bezoek dan de website van de relevante gegevensbeschermingsautoriteit in jouw land.

2. Wie gebruikt jouw gegevens?

Ditto Care B.V. is verantwoordelijk voor de Ditto-app en daarmee de verantwoordelijke organisatie (verwerkingsverantwoordelijke) voor het gebruik van jouw persoonsgegevens zoals beschreven in dit privacybeleid. De volledige gegevens zijn:

Ditto Care B.V., Aert van Nesstraat 45, 3012CA Rotterdam, Nederland KvK: 94952736

3. Van wie gebruiken we gegevens?

We verwerken de persoonsgegevens van iedereen die contact met ons heeft gehad of onze Ditto-app heeft gebruikt. Dit zijn onder andere app-gebruikers, particuliere klanten, zakelijke klanten en contactpersonen van onze partners.

4. Hoe verkrijgen we jouw gegevens?

We ontvangen de gegevens rechtstreeks van jou zodra je:

- de Ditto-app downloadt en installeert
- een account aanmaakt binnen de app
- medische of gezondheidsgegevens invoert in de app
- functies of functionaliteiten van de app gebruikt
- toestemmingen aan de app verleent (zoals camera, locatie, etc.)
- contact opneemt met onze klantenservice

5. Welke gegevens van jou gebruiken we?

We maken zorgvuldig onderscheid tussen gegevens die we moeten verwerken om onze diensten te leveren en gegevens waar we nooit toegang tot hebben:

Gegevens die we verwerken om onze diensten te leveren

Basisidentiteitsgegevens:

- naam
- e-mailadres
- telefoonnummer

Accountgegevens:

- app-voorkeuren en instellingen

Medische en gezondheidsgegevens:

- medische documenten waarvan je hebt gevraagd om deze samen te vatten of uit te leggen
- gespreksopnames waarvan je hebt gevraagd om deze samen te vatten

Gegevens die we alleen anoniem verwerken

Apparaatgegevens:

- apparaattype en -model (geanonimiseerd)
- versie van besturingssysteem (geanonimiseerd)
- unieke apparaat-ID's (geanonimiseerd)

Gebruiksgegevens:

- gebruikte app-functies (geanonimiseerd)
- tijd, frequentie en duur van app-gebruik (geanonimiseerd)
- app-prestatiegegevens (geanonimiseerd voor technische excellentie)

Gegevens waar we nooit toegang tot kunnen hebben

Inloggegevens:

- inloggegevens (versleuteld en verlaten nooit jouw apparaat)
- biometrische gegevens die worden gebruikt om de Ditto-app te vergrendelen

Medische en gezondheidsgegevens:

- alle medische gegevens die je aan de Ditto-app toevoegt en niet laat verwerken

Speciale opmerking over medische gegevens: Alle medische en gezondheidsgegevens worden uitsluitend in versleutelde vorm op jouw lokale apparaat opgeslagen. We kunnen nooit toegang krijgen tot of deze gegevens inspecteren. De enige uitzondering is wanneer je expliciet AI-verwerkingsfunctionaliteit activeert (door op de opnameknop te drukken of een document te laten uitleggen), waarna de specifieke gegevens die je hebt gekozen om te verwerken tijdelijk op onze beveiligde servers worden verwerkt. Deze verwerking omvat transcriptie van gesprekken, samenvattingen van transcripties en eenvoudige samenvattingen van geüploade medische documenten. We trainen onze AI-modellen nooit op jouw medische gegevens. Nadat de verwerking is voltooid, worden deze gegevens volledig uit onze systemen verwijderd, waarbij alleen technische en anonieme logbestanden worden bewaard.

Analytische gegevens:

- Gebruikers-ID (jouw Auth0 ID) en apparaatinformatie voor app-verbetering
- IP-adres (alleen gebruikt om stad/land te bepalen, daarna direct verwijderd)
- Zie Mixpanel's privacybeleid voor details: <https://mixpanel.com/legal/privacy-policy/>

6. Waarvoor gebruiken we jouw gegevens?

We gebruiken jouw persoonsgegevens alleen voor de specifieke doeleinden waarvoor we wettelijk gemachtigd zijn:

Levering van diensten: Om je de functionaliteit van de Ditto-app te bieden, inclusief de veilige opslag van jouw medische gegevens op jouw apparaat. De Ditto-app functioneert primair als een productiviteitstool die je helpt relevante informatie te loggen en samenvattingen te krijgen van jouw gegevens. We geven geen medisch advies.

Verwerking met expliciete toestemming: Wanneer je specifiek AI-verwerking van jouw medische gegevens aanvraagt (door op de opnameknop te drukken of een document te laten uitleggen), verwerken we deze gegevens tijdelijk op onze beveiligde servers op basis van jouw expliciete toestemming. Deze verwerking is uitsluitend bedoeld voor het transcriberen van gesprekken, het samenvatten van transcripties en het verstrekken van eenvoudige samenvattingen van geüploade documenten. Je wordt hiervan op de hoogte gesteld de eerste keer dat je deze functie gebruikt.

We trainen onze AI-modellen nooit op jouw medische gegevens. We kunnen anonieme beveiligings- en veiligheidscontroles uitvoeren om ervoor te zorgen dat jouw AI-output betrouwbaar en veilig is, maar de inhoud van de medische gegevens wordt niet opgeslagen—alleen technische

prestatiegegevens kunnen anoniem worden opgeslagen om ervoor te zorgen dat onze AI-modellen betrouwbaar blijven.

Basisfunctionaliteit zonder account: Je kunt de basisfunctionaliteit van de app gebruiken zonder een account. Dit omvat het handmatig loggen van afspraken met bijgevoegde foto's en documenten, en het maken van audio-opnames zonder verwerking via de server. Om technische redenen is een account nodig om AI-functionaliteiten te gebruiken.

Technische functionaliteit: Om ervoor te zorgen dat de app goed functioneert, inclusief probleemoplossing, data-analyse, testen en systeemonderhoud.

Beveiliging en naleving: Om jouw identiteit te verifiëren, fraude te voorkomen en te zorgen voor naleving van onze wettelijke verplichtingen met betrekking tot bescherming van medische gegevens.

Serviceverbetering: Om gebruikspatronen in geanonimiseerde, geaggregeerde vorm te analyseren om de functionaliteit en gebruikerservaring van onze app te verbeteren.

Communicatie: Om te reageren op jouw vragen, klantenservice te bieden en je belangrijke mededelingen over de app of jouw account te sturen.

We zullen jouw gegevens niet gebruiken voor andere doeleinden dan hierboven vermeld zonder voorafgaande toestemming van jou.

7. Hoe lang bewaren we jouw gegevens?

We bewaren jouw persoonsgegevens zo lang als:

- vereist door toepasselijke wetgeving
- noodzakelijk voor het doel waarvoor we jouw gegevens gebruiken
- je een actief account bij ons hebt

Voor accountgegevens bewaren we deze zo lang je een actief account hebt, plus een periode van 30 dagen na accountverwijdering om eventueel herstel van het account mogelijk te maken indien gevraagd.

Voor medische gegevens die je verwerkt met onze AI-functionaliteit worden deze gegevens alleen tijdelijk op onze servers opgeslagen tijdens de verwerkingsoperatie en automatisch verwijderd zodra de verwerking is voltooid en aan jouw apparaat is geleverd. Als je offline bent wanneer de verwerking is voltooid, bewaren we de gegevens tot 24 uur om levering bij herverbinding mogelijk te maken, waarna ze permanent worden verwijderd ongeacht de leveringsstatus.

Voor technische en gebruiksgegevens bewaren we technische logging maximaal 13 maanden om app-verbeteringen en probleemoplossing mogelijk te maken.

Als je meer wilt weten over hoe lang we specifieke gegevens over jou bewaren, neem dan contact met ons op.

8. Met wie delen we jouw gegevens?

We verkopen jouw persoonsgegevens nooit. We delen jouw gegevens alleen met de volgende zorgvuldig geselecteerde partijen en alleen wanneer noodzakelijk:

Dienstverleners (verwerkers):

- **Microsoft Azure** (cloudhosting en AI-verwerking): Alle gegevensverwerking vindt plaats binnen de EU
- **Auth0** (authenticatiediensten): Verwerkt inloggegevens en gebruikers-ID's
- **Mixpanel** (app-analytics): Alleen met jouw toestemming, alle gegevens blijven in de EU. DPA: <https://mixpanel.com/legal/dpa/>
- **Adjust** (installatiemeting): Alleen met jouw toestemming, alle gegevens blijven in de EU. DPA: <https://www.adjust.com/terms/dpa/>
- **Intuit MailChimp** (e-mailcommunicatie): Alleen je e-mailadres en voornaam voor onboarding en nieuwsbrieven

Al deze dienstverleners zijn contractueel gebonden om:

- Jouw gegevens alleen te verwerken volgens onze instructies
- Passende technische en organisatorische beveiligingsmaatregelen te implementeren
- Jouw gegevens niet te gebruiken voor hun eigen doeleinden
- Aan de AVG en andere toepasselijke wetgeving inzake gegevensbescherming te voldoen

Wettelijke verplichtingen:

- We kunnen jouw gegevens delen als dit wettelijk vereist is (bijvoorbeeld bij een gerechtelijk bevel of verzoek van wetshandhavingsinstanties)
- We zullen je hierover informeren, tenzij dit wettelijk verboden is

We delen jouw gegevens nooit met:

- Adverteerders of marketingbedrijven
- Data brokers
- Social media platforms (tenzij je ervoor kiest om onze app te verbinden)
- Andere derde partijen voor hun eigen commerciële doeleinden

9. Waar bewaren we jouw gegevens?

We verwerken en bewaren jouw gegevens uitsluitend binnen de Europese Economische Ruimte (EER):

- Jouw medische gegevens worden alleen in versleutelde vorm op jouw lokale apparaat opgeslagen.
- Wanneer je AI-verwerking initieert, worden jouw gegevens tijdelijk verwerkt op onze servers in Europese datacenters.
- Onze infrastructuur is gebouwd op het Microsoft Azure Platform met uitsluitend Europese datacenters.
- Alle aanvullende diensten die we gebruiken bevinden zich ook binnen de EER.

Dit zorgt ervoor dat jouw gegevens altijd worden beschermd onder EU-normen voor gegevensbescherming (AVG).

10. Hoe veilig zijn jouw gegevens bij ons?

Gegevensbeveiliging is onze hoogste prioriteit, vooral voor gevoelige medische informatie:

Lokale versleuteling: Alle medische gegevens op jouw apparaat zijn versleuteld met behulp van de native versleutelingsfunctionaliteit van iOS (voor Apple-apparaten) en Android. We beheren deze versleuteling niet en hebben geen toegang tot jouw versleutelingssleutels.

Biometrische authenticatie: De app ondersteunt biometrische authenticatie (zoals Face ID op iPhones) met behulp van de native implementatie van het apparaat. We hebben nooit toegang tot biometrische gegevens, omdat dit volledig door het besturingssysteem van jouw apparaat wordt afgehandeld.

Back-upopties: Gegevensherstel is alleen mogelijk via de native back-upfunctionaliteit van jouw apparaat (zoals Apple iCloud of Google Drive). Omdat we jouw gegevens niet op onze servers bewaren, kunnen we jouw gegevens niet herstellen als je jouw apparaat verliest en geen back-up hebt gemaakt.

Beveiligde infrastructuur: Onze infrastructuur is gebouwd op het Microsoft Azure Platform volgens Microsoft-beveiligingsstandaarden, een van de best beveiligde cloudplatforms die beschikbaar zijn.

Versleutelingsstandaarden: We gebruiken AES-256-versleuteling voor data at rest en TLS 1.3/HTTPS voor data in transit.

Toegangscontroles: We implementeren strikte toegangscontroles op basis van de principes van minimale rechten (Least Privilege) en need-to-know, waarbij Role-Based Access Control (RBAC) alle toegang tot gegevens regelt.

Tweefactorauthenticatie: Tweefactorauthenticatie is verplicht voor alle menselijke toegang tot gegevens en softwaresystemen van Ditto.

Regelmatige beveiligingstests: We voeren regelmatige kwetsbaarheidsscans uit, inclusief Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) en handmatige penetratietests.

Continue monitoring: We onderhouden continue monitoring, prestatiemetingen, toegangslogging en waarschuwingen om incidenten te detecteren en erop te reageren.

Personeelsscreening: Alle directeuren, werknemers en onderaannemers zijn verplicht een Verklaring Omtrent Gedrag (VOG) te verkrijgen en te overleggen.

Certificering: Ditto Care is bezig met het verkrijgen van NEN/ISO-certificering om onze beveiligingspraktijken verder te valideren.

Als je specifieke vragen hebt over hoe we jouw gegevens beveiligen, neem dan contact met ons op.

11. Wat zijn jouw rechten?

Onder de EU-wetgeving inzake gegevensbescherming (AVG) heb je de volgende rechten:

Recht op informatie: We moeten op een begrijpelijke en duidelijke manier uitleggen wat we met jouw gegevens doen en welke controle je hierover hebt. Daarom leggen we in dit privacybeleid gedetailleerd uit welke gegevens we van jou verzamelen en hoe we met jouw gegevens omgaan.

Recht op inzage: Je kunt ons altijd vragen om de gegevens die we over jou hebben in te zien.

Recht op correctie: Je kunt ons vragen om jouw gegevens te corrigeren als deze onjuist of onvolledig zijn.

Recht van bezwaar: Je kunt bezwaar maken tegen de verwerking van jouw gegevens als je het niet eens bent met de manier waarop we met jouw persoonsgegevens omgaan.

Recht op dataportabiliteit: Je kunt ons vragen om je de digitale gegevens die we over jou hebben te sturen. Momenteel stelt de Ditto-app je in staat om opnames op jouw lokale apparaat op te slaan en gegenereerde samenvattingen en uitleg te exporteren. We zijn toegewijd aan dataportabiliteit en ontwikkelen actief een uitgebreider mechanisme om jouw volledige Ditto medische bibliotheek te

exporteren. We verwachten deze verbeterde functionaliteit binnen 2025 uit te brengen. In de tussentijd kan ons ondersteuningsteam helpen bij handmatige verzoeken om gegevensexport indien nodig.

Recht op beperking: Je kunt vragen om het gebruik van jouw gegevens te beperken. Dit betekent dat we in bepaalde gevallen jouw gegevens alleen mogen opslaan maar niet mogen gebruiken.

Recht om vergeten te worden: Je kunt ons vragen om alle gegevens die we over jou hebben te verwijderen. We zullen dan alle gegevens verwijderen die naar jou te herleiden zijn. In sommige gevallen kunnen of mogen we jouw gegevens nog niet verwijderen als we een wettelijke verplichting hebben om deze te bewaren.

Proces voor gegevensverwijdering: Je hebt volledige controle over jouw gegevens en kunt jouw account met alle bijbehorende gegevens op elk moment direct vanuit de app verwijderen. Ga gewoon naar Instellingen > Account > Account verwijderen en volg de instructies op het scherm.

Wanneer je jouw account verwijdert:

- Alle accountinformatie wordt binnen 30 dagen permanent uit onze systemen verwijderd
- Omdat jouw medische gegevens alleen op jouw apparaat worden opgeslagen (en optioneel in jouw persoonlijke iCloud-back-ups), zal het verwijderen van de app van je telefoon deze gegevens volledig verwijderen
- Alle tijdelijke verwerkingsgegevens op onze servers worden onmiddellijk verwijderd
- Er blijft geen persoonlijk identificeerbare informatie in ons bezit achter

Houd er rekening mee dat als je iCloud- of Drive-back-ups op jouw apparaat hebt ingeschakeld, Apple en Google's back-updiensten jouw app-gegevens kunnen bewaren volgens hun beleid. Je kunt deze back-ups beheren via de instellingen van jouw apparaat.

We voltooien het proces van accountverwijdering binnen 30 dagen na jouw verzoek, en meestal veel eerder.

Recht om een klacht in te dienen: Je kunt een klacht indienen over de manier waarop we met jouw gegevens omgaan. Als je een klacht hebt, lossen we deze graag voor je op. Neem hiervoor contact met ons op. Je kunt jouw klacht ook indienen bij je nationale gegevensbeschermingsautoriteit. We hopen natuurlijk dat het niet zover komt, maar indien nodig kun je ook naar de rechter gaan. In dat geval is de rechtbank op de plaats van vestiging van Ditto Care B.V. degene die jouw klacht zal behandelen.

Hoe dien ik een verzoek of klacht in? Je kunt jouw verzoek of klacht bij ons indienen door een e-mail te sturen naar privacy@ditto.care. We verwerken elk verzoek of elke klacht binnen 30 dagen. Als je meerdere aanvragen of klachten indient of als je een complex verzoek of klacht indient, kan dit meer tijd in beslag nemen. In dat geval nemen we uiterlijk binnen 60 dagen contact met je op. We

kunnen je vragen om jezelf te identificeren. In dat geval zullen we je vragen bepaalde informatie te verstrekken om er zeker van te zijn dat je de juiste persoon bent van wie de persoonsgegevens in het geding zijn.

12. Welke regelgeving is van toepassing op dit privacybeleid?

Ons privacybeleid voldoet aan:

- De Europese Algemene Verordening Gegevensbescherming (AVG)
- Toepasselijke nationale wetgeving inzake gegevensbescherming
- De Nederlandse Uitvoeringswet AVG
- Regelgeving voor medische hulpmiddelen, waar van toepassing
- Apple App Store-richtlijnen en -beleid

13. Welke tracking-technologieën gebruiken we?

In tegenstelling tot websites die cookies gebruiken, gebruiken mobiele applicaties verschillende technologieën om informatie te verzamelen en op te slaan:

App-analytics: We gebruiken anonieme app-analytics om te begrijpen hoe gebruikers met onze app omgaan, technische problemen te identificeren en de gebruikerservaring te verbeteren. Dit identificeert jou niet persoonlijk.

Apparaat-ID's: We kunnen unieke apparaat-ID's verzamelen om veilige authenticatie en basisfunctionaliteit te garanderen. We gebruiken deze ID's niet voor cross-app tracking, advertenties of profiling. Je kunt deze ID's op elk moment resetten in de instellingen van jouw apparaat.

Lokale opslag: We slaan jouw medische gegevens en app-voorkeuren lokaal op jouw apparaat op in versleutelde vorm om app-functionaliteit te bieden, zelfs als je offline bent.

Pushnotificaties: Met jouw toestemming kunnen we pushnotificaties versturen om je te informeren over nieuwe app-releases, je te herinneren aan aankomende gebeurtenissen die je in de app hebt ingevoerd, en je te informeren wanneer AI-verwerking van jouw gegevens is voltooid. Deze notificaties gebruiken alleen gegevens die je al binnen de app hebt verstrekt. Pushnotificaties zijn optioneel en kunnen worden uitgeschakeld in de instellingen van jouw apparaat.

E-mail: Ditto gebruikt Intuit MailChimp om onboarding- en nieuwsbrief-e-mails te versturen. Alleen je e-mailadres en voornaam wordt gedeeld met MailChimp. Alle e-mails van Ditto bevatten afmeldingslinks die jouw gegevens uit deze dienst zullen verwijderen.

SDK's van derden: Onze app bevat de volgende software development kits (SDK's) van derden:

1. Auth0 (v2.10.0)

- Heeft toegang tot gebruikersauthenticatiegegevens
- Verwerkt inloggegevens
- Slaat authenticatietokens op
- Kan e-mailadressen en gebruikers-ID's verzamelen

2. Firebase Crashlytics (v11.10.0)

- Verzamelt app-gebruiksgegevens en crashrapporten
- Kan apparaatinformatie bevatten (model, OS-versie)
- Let op: We gebruiken de privacyvriendelijke "WithoutAdIdSupport"-versie voor Analytics om jouw privacy te verbeteren

3. Mixpanel

- Doel: App-gebruiksanalytics om de gebruikerservaring te verbeteren
- Gegevens: Gebruikers-ID, apparaatinfo, app-interacties
- IP-verwerking: Jouw IP-adres wordt alleen gebruikt om stad/land te bepalen, daarna direct verwijderd (niet opgeslagen)
- Opslag: alleen EU-servers
- Privacybeleid: <https://mixpanel.com/legal/privacy-policy/>
- Jouw gegevens worden nooit gebruikt voor advertenties of cross-app tracking

4. Adjust

- Doel: Meten van app-installatiebronnen en campagne-effectiviteit
- Gegevens: Apparaat-ID's (IDFV op iOS, Android ID), sessiegegevens, apparaatmetadata
- IP-verwerking: IP-adres gebruikt voor attributie, daarna direct verwijderd
- Opslag: EU-servers (EU-eindpunt geconfigureerd)
- Geen gevoelige gegevens: verzamelt geen locatie-, gezondheids- of berichtgegevens
- Privacybeleid: <https://www.adjust.com/terms/privacy-policy/>
- Verwerkersovereenkomst: Beschikbaar op <https://www.adjust.com/terms/dpa/>

Deze SDK's zijn contractueel gebonden om gegevens alleen te verwerken zoals expliciet door ons geïnstrueerd en in overeenstemming met toepasselijke wetgeving inzake gegevensbescherming.

Je hebt controle over jouw gegevens: Je kunt app-toestemmingen beheren via de instellingen van jouw apparaat. Je kunt ook alle lokale gegevens verwijderen door de app te deïnstalleren, hoewel dit alle medische gegevens die je lokaal hebt opgeslagen permanent zal verwijderen.

14. Wat doen we met gegevens van minderjarigen?

Speciale bescherming voor minderjarigen: We erkennen dat medische informatie van minderjarigen speciale bescherming vereist:

- Onze app is niet ontworpen voor of gericht op gebruikers onder de 16 jaar.
- Als je jonger bent dan 16 jaar, moet je toestemming hebben van een ouder of wettelijke voogd om de Ditto-app te gebruiken.
- Ouders/voogden van minderjarigen zijn verantwoordelijk voor het toezicht op het gebruik van de app door hun kind en het beheren van de toestemming voor het verwerken van hun gegevens.
- We implementeren leeftijdsverificatiemaatregelen zoals vereist door toepasselijke wetgeving.
- Als we erachter komen dat we persoonsgegevens van een minderjarige hebben verzameld zonder ouderlijke toestemming, zullen we stappen ondernemen om die informatie te verwijderen.

15. Offline functionaliteit

De Ditto-app is ontworpen met offline toegang als prioriteit:

- Alle jouw medische gegevens worden lokaal op jouw apparaat opgeslagen in versleutelde vorm
- Je kunt jouw volledige medische bibliotheek bekijken, organiseren en beheren zonder internetverbinding
- Je kunt eerder gegenereerde samenvattingen en uitleg raadplegen terwijl je offline bent
- Je kunt nieuwe medische documenten, foto's en handmatige notities toevoegen terwijl je offline bent

Een internetverbinding is alleen vereist voor:

- Initiële accountcreatie en authenticatie
- AI-verwerking van nieuwe gegevens voor samenvattingen of uitleg
- Het ontvangen van app-updates en niet-kritieke notificaties

Deze offline-first benadering zorgt ervoor dat jouw medische informatie toegankelijk blijft, zelfs in gebieden met beperkte connectiviteit, zoals ziekenhuizen of medische faciliteiten met netwerkbependingen.

16. Overige informatie

App-monetisatie: De Ditto-app is gratis te gebruiken voor alle gebruikers. Er is geen betaald abonnement nodig.

Classificatie als medisch hulpmiddel: De Ditto-app wordt gepositioneerd als een productiviteitstool die je helpt relevante informatie te loggen en samenvattingen te krijgen van de gegevens die je invoert. Het kwalificeert niet als een medisch hulpmiddel onder de EU MDR. We geven geen medisch advies en voegen altijd disclaimers toe aan alle output dat alle informatie zorgvuldig moet worden gecontroleerd.

Geografische beschikbaarheid: Momenteel is de Ditto-app gericht op beschikbaarheid in Nederland.

Protocol bij datalekken: In het onwaarschijnlijke geval van een datalek dat jouw persoonsgegevens treft, zullen we voldoen aan alle toepasselijke meldingsvereisten onder de Europese wetgeving inzake gegevensbescherming. Omdat we minimale gebruikersgegevens op onze servers opslaan en medische gegevens voornamelijk alleen op jouw apparaat worden opgeslagen, is het risico op significante datalekken verminderd.

Azure OpenAI Service Privacy: Wanneer we jouw gegevens verwerken met AI-mogelijkheden, maken we gebruik van Microsoft's Azure OpenAI Service met de volgende privacybeschermingen:

- **Geen training op jouw gegevens:** De AI-modellen zijn staatloos – jouw gegevens worden nooit gebruikt om de basismodellen te trainen, opnieuw te trainen of te verbeteren.
- **Regionale gegevensverwerking:** Alle gegevens worden verwerkt binnen Europese datacenters en verlaten nooit de Europese Economische Ruimte.
- **Inhoudsfiltering:** Real-time inhoudsfilters beoordelen inputs en outputs zonder jouw gegevens op te slaan.
- **Misbruikmonitoring:** Geautomatiseerde systemen monitoren op misbruik zonder menselijke beoordeling, tenzij specifiek gemarkeerd. Als beoordeling nodig is:
 - Gegevens blijven versleuteld en alleen toegankelijk voor geautoriseerde Microsoft-medewerkers
 - Gegevens worden afzonderlijk opgeslagen in dezelfde regio als onze implementatie
 - Gegevens worden maximaal 30 dagen bewaard
 - Voor Europese implementaties bevinden beoordelaars zich ook binnen de EER

Voor meer informatie over deze privacybeschermingen kun je de officiële Azure OpenAI-documentatie van Microsoft bezoeken.

17. Heb je een vraag over dit privacybeleid?

Als je vragen hebt over ons privacybeleid of hoe we met jouw gegevens omgaan, neem dan contact met ons op via:

E-mail: privacy@ditto.care

Adres: Ditto Care B.V., Aert van Nesstraat 45, 3012CA Rotterdam, Nederland

We helpen je graag bij het uitleggen van alle aspecten van onze privacypraktijken.

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.
- **Privacy-friendly analytics:** We use Mixpanel and Adjust for app improvement with your consent. All analytics data stays in the EU and you can opt-out anytime.
- **No tracking:** We don't do cross-app tracking or share your data with third parties for advertising.
- **Minimal collection:** We only collect the minimum data needed to provide our service, e.g. technical logging and consented 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 28 October 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?
2. Who uses your data?
3. Whose data do we use?
4. How do we get your data?
5. What data of you do we use?
6. What do we use your data for?
7. How long do we store your data?
8. Who do we share your data with?
9. Where do we store your data?
10. How safe is your data with us?
11. What are your rights?
12. Which rules apply to this privacy statement?
13. Which tracking technologies do we use?
14. What do we do with data of minors?
15. Offline Functionality
16. Other

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

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.

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., Aert van Nesstraat 45, 3012CA, 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.

Analytics Data:

- User identifier (your Auth0 ID) and device information for app improvement
- IP address (used only to determine city/country, then immediately discarded)
- Add See Mixpanel's privacy policy for details: <https://mixpanel.com/legal/privacy-policy/>

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. **Mixpanel** for analytics (data processor, EU servers only, IP addresses discarded after geolocation, DPA: <https://mixpanel.com/legal/dpa/>). **Adjust** for attribution analytics (data processor, EU endpoint, DPA: <https://www.adjust.com/terms/dpa/>)

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 or Drive backups on your device, Apple and Google'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.

Email: Ditto uses Intuit MailChimp to send onboarding and newsletter emails. Only your email address and first name is shared with MailChimp. All Ditto's emails contain unsubscribe links which will delete your data from this service.

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 Crashlytics (v11.10.0)**
 - Collects app usage data and crash reports
 - May include device information (model, OS version)
 - Note: We use the privacy-friendly "WithoutAdIdSupport" version for Analytics to enhance your privacy
3. **Mixpanel**
 - Purpose: App usage analytics to improve user experience
 - Data: User ID, device info, app interactions
 - IP processing: Your IP address is used only to determine city/country location, then immediately discarded (not stored)
 - Storage: EU servers only
 - Privacy policy: <https://mixpanel.com/legal/privacy-policy/>
 - Your data is never used for advertising or cross-app tracking
4. **Adjust**
 - Purpose: Measure app installation sources and campaign effectiveness
 - Data: Device identifiers (IDFV on iOS, Android ID), session data, device metadata
 - IP processing: IP address used for attribution then immediately discarded
 - Storage: EU servers (EU endpoint configured)
 - No sensitive data: Does not collect location, health or message data
 - Privacy policy: <https://www.adjust.com/terms/privacy-policy/>
 - DPA: Available at <https://www.adjust.com/terms/dpa/>

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., Aert van Nesstraat 45, 3012CA Rotterdam, The Netherlands

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