

D DOT

Privacy Policy

For D. DOT CGM, D DOT Mobile Application, Website and Connected Services
India Version | Full Stop to Diabetes Guesswork.

Document Item	Details
Policy owner	Dexvia Healthcare Private Limited
Product / App	D DOT CGM-Continuous Glucose Monitoring Sensor and D DOT mobile application
Website	www.ddot.health
Customer support	+91 800 800 2041 support@ddot.health
Registered / operating address	3rd Floor, Sreshta Primus, Road No 36, Jubilee Hills, Hyderabad, Telangana - 500033, India
Effective date	26 June 2026
Version	01
Territory	India, unless a separate local policy applies

Important legal review note

This Privacy Policy is a professional draft for D DOT release preparation. Before publication, Dexvia should have it reviewed by its legal, privacy, cybersecurity, regulatory and app-product teams. The final policy must match the actual app architecture, server locations, vendors, consent flows, retention settings and released features.

1. Introduction

Dexvia Healthcare Private Limited (“Dexvia”, “D DOT”, “we”, “us” or “our”) respects your privacy and is committed to protecting your personal information and health data.

This Privacy Policy explains how we collect, use, store, process, disclose, transfer and protect information when you use:

- The D. DOT CGM Continuous Glucose Monitoring System, including sensor, transmitter and related device information;
- The D DOT mobile application and connected app features;
- D DOT websites, including www.ddot.health;

- Customer support, warranty, replacement, adverse event reporting and feedback services;
- AI reports, health timeline, report upload, family/caregiver sharing, doctor sharing and connected care features, where available.

By creating an account, using the D DOT App, enabling optional features or providing information to us, you agree to the processing of your information as described in this Privacy Policy and in any additional consent screens shown in the app.

Medical privacy notice

The D DOT App may process health information, including glucose data, medication logs, insulin logs, lifestyle logs, medical reports and AI-generated summaries. This information can be sensitive. Please read this policy carefully before using optional features such as cloud backup, AI reports, document upload, family sharing or doctor sharing.

2. Who is responsible for your data?

For users in India, Dexvia Healthcare Private Limited is the entity responsible for deciding why and how your personal data is processed for the D DOT App, D. DOT CGM support services and D DOT connected services, unless a separate agreement or product notice states otherwise.

Role	Details
Data fiduciary / controller	Dexvia Healthcare Private Limited
Contact for privacy questions	support@ddot.health. Dexvia may create a dedicated privacy email such as privacy@ddot.health before publication.
Customer support	+91 800 800 2041
Address	3rd Floor, Sreshta Primus, Road No 36, Jubilee Hills, Hyderabad, Telangana - 500033, India
Manufacturer of OEM device	Infinovo Medical Co., Ltd., P.R. China. Manufacturer involvement, if any, is limited to technical, quality, regulatory, support or device-related processing as contractually permitted.

3. Relationship with other D DOT documents

This Privacy Policy should be read together with:

- D. DOT CGM User Manual / Instructions for Use;
- D DOT User Agreement / Terms and Conditions;
- Medical Disclaimer and Safety Information;
- Consent for Health Data Processing;

- Doctor Data Sharing Consent;
- Family/Caregiver Sharing Consent;
- AI Disclosure Statement;
- Data Retention Policy, if published separately.

If there is a conflict between this Privacy Policy and a more specific consent or legally required notice, the more specific notice will apply for that feature or processing activity.

4. Information we collect

We collect only the information that is reasonably necessary to provide, secure, improve and support the D DOT services, comply with law, and operate optional features selected by you.

Category	Examples
Account and identity information	Name, mobile number, email address, age/date of birth, gender, password/OTP authentication details, profile photo if added, account ID and login history.
Contact and support information	Address, customer support requests, warranty/replacement details, invoices, seller details, complaint details, call/chat/email records and support ticket information.
Device and sensor information	Sensor serial number, lot/batch number, expiry date, QR code/pairing details, sensor status, transmitter/device identifier, app version, phone model, operating system and Bluetooth status.
CGM and glucose data	Sensor glucose readings, reading time, glucose trend arrows, alerts, calibrations, glucose history, AGP/TIR reports, time above/below range and system events.
Medication and insulin logs	Medication schedule, taken doses, missed doses, adherence percentage, insulin events and user-entered notes. The app does not recommend medication changes or insulin doses.
Lifestyle and wellness logs	Meals, diet logs, hydration, sleep, activity, steps, exercise, mood, stress, energy level, symptoms, menstrual logs, recovery context and other user-entered events.
Medical reports and documents	PDFs, images or files uploaded by you, such as lab reports, prescriptions, discharge summaries, imaging reports or other medical records, including extracted/OCR text where supported.
AI and derived information	AI-generated summaries, evidence references, trend explanations, health timeline insights, D DOT Health Score where supported, correlation-style observations and report explanations.
Sharing and recipient information	Family member, caregiver, loved-one, friend or doctor details you provide for sharing, access permissions, sharing duration and activity records.
Technical and usage information	App logs, crash logs, diagnostics, IP address, device identifiers, approximate location where required for Bluetooth scanning, interaction history and security logs.
Marketing and communication preferences	Communication consent, notification preferences, app announcements and feedback, where applicable.

5. Information you provide about others

If you add a family member, caregiver, doctor, emergency contact, loved one, friend or other recipient, you confirm that you have the right to provide their contact details and that the sharing is lawful and appropriate. You should not add another person without their knowledge where the app feature requires their participation or consent.

6. App permissions we may request

Some app features require device permissions. You may refuse a permission, but some features may not work properly.

Permission	Purpose
Camera	To scan the sensor QR code, upload medical report images, capture food photos or support document upload features where available.
Bluetooth / nearby devices	To detect, pair and communicate with the CGM sensor.
Location	On some Android versions, location permission may be required for Bluetooth scanning. We do not use this to track your physical movement unless a separate feature and consent apply.
Notifications / critical alerts	To send glucose alerts, app reminders, medication reminders, sharing alerts and service notifications where enabled.
Storage / files / photos	To upload reports, export data, save PDFs or attach screenshots/photos to support requests.
Background app activity	To receive sensor data and alerts when the app is not open.
Health app integrations	To import or export selected data with services such as Apple Health or Google Health Connect, if supported and authorized by you.

7. How we use your information

We use your information for the following purposes:

Purpose	Examples
Provide core CGM services	Pair sensor, receive glucose readings, display trends, generate alerts, maintain logbook and show CGM status.
Create and manage your account	Register, authenticate, secure login, verify contact details and maintain profile settings.
Generate reports and summaries	Prepare glucose reports, AGP-style summaries, Time in Range, trend summaries and exports.
Support optional health-intelligence features	Health timeline, D DOT Health Score, correlation-style insights, evidence references and wellness summaries where available.
Provide AI reports and explanations	Explain reports, uploaded documents and patterns in plain language, based on data available in your account and your consent.

Enable user-controlled sharing	Share selected data with family, caregivers, loved ones, friends or healthcare professionals when authorized by you.
Medication and wellness tracking	Help record medication, insulin, meals, hydration, activity, sleep, mood, stress, energy, symptoms and menstrual logs where supported.
Customer support and warranty	Troubleshoot sensor/app issues, process replacement requests, verify lot/serial numbers and respond to complaints.
Safety, adverse event and regulatory reporting	Investigate device complaints, serious incidents, quality issues, cybersecurity issues and regulatory reporting obligations.
Security and fraud prevention	Protect accounts, detect suspicious activity, prevent misuse and maintain audit logs.
Product improvement and analytics	Improve app performance, reliability, safety, usability and feature quality, preferably using de-identified or aggregated data where possible.
Legal compliance	Comply with applicable laws, lawful requests, audits, dispute resolution, tax, accounting, medical device and data protection obligations.

8. AI Health Coach, AI Reports and evidence-based insights

The D DOT App may include AI-powered features such as AI Health Coach-style conversations, AI-generated reports, evidence-based insights, health timeline summaries, report explanations and medical document understanding.

AI features may process CGM glucose data, medication logs, insulin logs, lifestyle logs, uploaded reports, OCR text, symptoms, menstrual logs, health timeline events and other data you provide or authorize.

AI outputs may include references to source data used by the app, such as CGM data, medication logs, sleep logs, activity data, hydration logs or uploaded reports. These references are intended to improve transparency. They do not mean that a doctor reviewed or approved the AI output.

AI medical limitation

AI outputs are for informational and educational purposes only. They do not diagnose disease, prescribe treatment, recommend insulin doses, recommend medicine changes, replace medical advice, replace a blood glucose meter when symptoms do not match readings, or act as an emergency monitoring service.

Where third-party AI infrastructure or cloud service providers are used, Dexvia will require appropriate contractual, technical and organizational safeguards. If AI processing requires transferring personal data outside India or to another service provider, we will do so only in accordance with applicable law, this policy, user consent where required and our vendor controls.

9. Medical report upload and OCR processing

If you upload medical reports, prescriptions, discharge summaries, lab reports, imaging reports or other documents, the app may process the file, extract text using OCR, generate summaries and link the document to your health timeline or reports.

- Upload only documents that belong to you or that you are legally authorized to upload.
- Check uploaded documents carefully. OCR can be inaccurate or incomplete.
- AI explanations of reports are simplified summaries and may not capture every clinical detail.
- Do not make treatment decisions based only on uploaded-report summaries or AI explanations.
- Delete documents that you no longer want stored, subject to legal, regulatory, safety and backup limitations.

10. Legal basis and consent

We process personal data when you give consent, when processing is necessary to provide a service requested by you, when required for compliance with law, or when otherwise permitted under applicable law.

For optional features, the app may ask for separate consent or permission. Examples include cloud backup, AI reports, medical report upload, family sharing, doctor sharing, marketing communications and health app integrations.

You may withdraw consent for optional processing through app settings or by contacting us. Withdrawal of consent may disable related features. It will not affect processing already completed before withdrawal, and we may continue to retain or process information where required or permitted by law, medical device obligations, dispute resolution, safety investigations or regulatory reporting.

11. Sharing with family, caregivers, loved ones and doctors

The D DOT App may allow you to share selected information with family members, caregivers, loved ones, friends or healthcare professionals. You control who can access your data, what data can be shared, and how long access remains active, where supported by the app.

Sharing type	Possible data shared
--------------	----------------------

Family / caregiver / loved-one sharing	Live glucose readings, glucose trends, high/low glucose events, medication adherence, wellness updates, reports, AI summaries and emergency-style alerts where supported.
Doctor sharing	CGM trends, AGP/TIR reports, medication adherence summaries, medical records, lifestyle insights, AI-generated summaries and progress reports where supported.
Health app integrations	Selected glucose, activity, sleep or wellness data exchanged with supported third-party health platforms if authorized by you.

Once you share information with a recipient or third-party service selected by you, that recipient may process, store, disclose or use the information according to their own privacy practices. Dexvia may not control how your chosen recipient uses the data after receiving it. Review the recipient carefully before sharing.

12. Service providers and processors

We may use trusted service providers to help us operate the D DOT App and services. These may include cloud hosting, database management, analytics, crash reporting, customer support, SMS/OTP, email, payment, AI infrastructure, cybersecurity, document processing, regulatory support and quality management providers.

We require service providers to process personal data only for authorized purposes, protect it using appropriate safeguards, and not use it for their own unrelated purposes.

13. When we disclose information

We may disclose personal information only in the following situations:

- With your consent or at your direction, including family/caregiver/doctor sharing;
- To service providers who help us provide and secure the services;
- To the OEM manufacturer, regulatory consultants, quality teams or technical partners where needed for support, safety, complaint investigation, regulatory compliance or product improvement;
- To comply with law, court orders, government requests, regulatory obligations, medical device reporting, MvPI/CDSCO reporting or lawful investigations;
- To protect the rights, safety, security or property of users, Dexvia, service providers or the public;
- In connection with a merger, acquisition, financing, restructuring or business transfer, subject to appropriate privacy protections and legal requirements.

We do not sell your personal health data. We do not use your personal health data for targeted advertising without your specific consent. We do not allow service providers to use your health data for their own advertising.

14. International transfers

Dexvia intends to operate D DOT as an India-first service. Primary servers for D DOT services should be controlled by Dexvia and located in India, unless the final app architecture or vendor setup states otherwise.

Some processing may involve service providers, technical support, manufacturer support, AI infrastructure or cloud systems located outside India. Where personal data is transferred outside India, Dexvia will take steps required by applicable law, including contractual safeguards, access controls and security measures. Transfers may also be limited by any country or territory restrictions notified by the Government of India.

Implementation check before publication

Before publishing this policy, confirm the actual server locations, cloud providers, AI providers, support tools, analytics tools and cross-border data flows. Do not state “India-only storage” unless that is technically true for all relevant personal data and backups.

15. Security measures

We use administrative, technical and organizational safeguards designed to protect personal data against unauthorized access, loss, misuse, alteration, disclosure or destruction. Measures may include:

- Encryption of data in transit and at rest where appropriate;
- Access controls, role-based permissions and authentication;
- Secure passwords, OTP and account protection controls;
- Logging, monitoring and review of access to systems;
- Firewalls, intrusion detection and malicious code protection where applicable;
- Backup, recovery and continuity controls;
- Vendor agreements requiring security safeguards;
- Cybersecurity reviews and incident response procedures.

No internet, Bluetooth, cloud or mobile app system is completely secure. You are responsible for keeping your phone, app account, password, OTP and device access secure. Do not share login credentials. Use phone lock, app lock and updated operating systems where available.

16. Personal data breach

If we become aware of a personal data breach affecting your personal data, we will assess the incident and notify affected users and/or authorities as required by applicable law. Notifications may be provided through email, SMS, in-app notice, phone call or other appropriate methods.

17. Data retention

We retain personal data only for as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law, medical device obligations, regulatory reporting, safety investigation, warranty, accounting, tax, dispute resolution or fraud prevention.

Data type	Indicative retention approach
Account and contact data	Retained while your account is active and for a reasonable period after closure, or longer if required for legal, tax, accounting, support or dispute purposes.
CGM and health data	May be retained for up to 8 years from last active use or as specified in the D DOT Data Retention Policy, unless deletion is requested and no legal/regulatory reason requires retention.
Device, lot, complaint and adverse event records	Retained as required for medical device quality, safety, complaint investigation, MvPI/CDSCO, warranty and regulatory obligations.
Uploaded medical reports	Retained until deleted by you or account closure, subject to legal, backup, safety, dispute and regulatory limitations.
App logs and security logs	Retained for security, audit, troubleshooting and incident response for the period needed, and at least where required by applicable rules or law.
De-identified or aggregated data	May be retained for product improvement, analytics, research, safety and statistical purposes where it no longer identifies you.

When personal data is no longer required, we will delete, anonymize or isolate it from active processing according to our retention and deletion procedures.

18. De-identified, aggregated and research use

We may use de-identified, anonymized or aggregated information for product improvement, safety monitoring, analytics, research, reporting, regulatory submissions, model evaluation and business planning. We will not use such information to identify you unless legally permitted and necessary for safety, fraud, security or compliance purposes.

If we conduct clinical research, publish findings or share datasets with external researchers, we will use appropriate consent, ethics approval, de-identification or legal safeguards as applicable.

19. Children and minors

D. DOT CGM is intended for adults aged 18 years and above unless the approved product labeling, app release and applicable law allow otherwise. The app is not intended for unsupervised use by children.

If the app is used for or by a child, parent or lawful guardian consent must be obtained as required by applicable law. We do not knowingly undertake tracking, behavioral monitoring or targeted advertising directed at children.

If you believe a child has provided personal data without required consent, contact us so we can review and take appropriate action.

20. Your rights and choices

Subject to applicable law and verification of your identity, you may have the right to:

- Access a summary of personal data being processed and how it is processed;
- Request correction of inaccurate or misleading personal data;
- Request completion or updating of incomplete or outdated personal data;
- Request erasure of personal data where retention is no longer necessary or legally required;
- Withdraw consent for optional processing;
- Manage sharing permissions and revoke recipient access where supported;
- Nominate another individual to exercise rights in the event of death or incapacity, where applicable law permits;
- Raise a grievance with Dexvia and, where legally permitted, approach the relevant data protection authority after using our grievance mechanism.

To exercise these rights, contact support@ddot.health. Dexvia may require identity verification and account ownership confirmation before acting on a request.

21. Your responsibilities

You are responsible for:

- Providing accurate account, health and contact information;
- Not impersonating another person;
- Not uploading reports or data that you are not authorized to upload;
- Keeping your phone, account, password and OTP secure;
- Reviewing sharing permissions regularly;
- Using app and AI outputs only within the medical limitations described in the user manual and AI Disclosure Statement;
- Using a blood glucose meter and seeking medical advice when symptoms do not match app readings or during emergencies.

22. Cookies, analytics and website data

Our website may use cookies, pixels, device identifiers or similar technologies to operate the website, remember preferences, understand usage, improve services and secure access. Where required, we will request consent for optional cookies or analytics. You can manage cookies through browser settings, but some website features may not work properly if disabled.

23. Marketing communications

We may send service messages related to your account, sensor, app, safety, warranty, policy changes or support. These are not marketing messages and may be necessary for service operation.

We will send promotional messages, offers or newsletters only where permitted by law and where you have not opted out. You may opt out of marketing communications through app settings, unsubscribe links or by contacting us. You may still receive important service, safety or legal notices.

24. Third-party links and services

The D DOT App or website may contain links to third-party websites, app stores, payment gateways, health platforms or services. Their privacy practices are governed by their own policies. Dexvia is not responsible for third-party privacy practices after you leave our services or authorize a third-party integration.

25. Grievance redressal and contact

For privacy questions, data-rights requests, consent withdrawal, grievances or complaints, contact:

Contact item	Details
Company	Dexvia Healthcare Private Limited
Email	support@ddot.health
Phone	+91 800 800 2041
Address	3rd Floor, Sreshta Primus, Road No 36, Jubilee Hills, Hyderabad, Telangana - 500033, India
Website	www.ddot.health
Grievance / privacy officer	To be appointed and inserted before publication, if required by law or company policy.

We will respond to privacy requests and grievances within the period required by applicable law. Some requests may take longer if they are complex, require verification, involve safety/regulatory records, or require coordination with service providers.

26. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. The updated version will show a new effective date or version number. If we make material changes, we may notify you through the app, website, email, SMS or other appropriate method. Continued use of the services after the effective date means the updated policy applies, unless additional consent is required by law.

27. Summary table for users

Question	Answer
What data do we collect?	Account, device, CGM, health logs, uploaded reports, AI outputs, sharing permissions, support records and app technical data.
Why do we collect it?	To provide CGM services, alerts, reports, AI explanations, sharing, support, warranty, safety, security and legal compliance.
Do we sell health data?	No. We do not sell personal health data.
Can users share data?	Yes, where supported and authorized by the user. Users should review recipients carefully.
Can consent be withdrawn?	Yes for optional processing, subject to legal, safety, regulatory and service limitations.
Are AI outputs medical advice?	No. AI outputs are informational and educational only.
Where is data stored?	D DOT is intended to be India-first. Confirm final server and vendor architecture before publication.
Who to contact?	support@ddot.health or +91 800 800 2041.

Appendix A: Consent and feature mapping

Feature	Consent / notice expectation
Core CGM monitoring	Required app notice and account/device consent for glucose processing and alert delivery.
Cloud backup / sync	Clear consent or setting explaining cloud storage and sync.
AI Health Coach / AI Reports	Separate AI disclosure and consent or clear enablement screen.
Medical report upload / OCR	Specific consent for document upload, OCR extraction and AI explanation.

Family / caregiver sharing	Separate sharing consent identifying recipient, data types and access duration where supported.
Doctor sharing	Separate sharing consent identifying doctor/provider and shared report/data scope.
Marketing communications	Opt-in or opt-out as legally required.
Health app integrations	User-directed authorization through platform permissions and app settings.