Privacy Policy

Manuel Mobile App – Privacy Policy

Last updated: 20 May 2025

---

1. Who we are

Manuel B.V. (KvK: 96013540), Burgemeester Bosmastraat 3, Winterswijk, The Netherlands – referred to as **"Manuel", "we", "us", or "our"** – develops and operates the Manuel mobile application (the **"App"**). We are the *controller* of the personal data processed via the App under the EU General Data Protection Regulation (**GDPR**).

Contact for privacy matters: **info@manuel.chat**

---

2. Scope of this policy

This Policy explains how we collect, use, share and secure information about you when you:

- install or use the App (iOS / Android);
- interact with notifications or in-app messages;
- contact us via the App's support features.

It does **not** cover data processed on websites outside the App.

---

3. What data we collect

Category	Examples	Collected by	Linked to you?
Account details	name, email address, phone number, company, user role	Manuel backend	Yes
Identifiers	device ID, IP address, app-generated user ID	Manuel backend	Yes

Usage data	screens visited, buttons tapped, time on page, crash logs	Microsoft Clarity (SaaS), Manuel backend	No (aggregated unless required for support)
Knowledge-items (internal)	answers or documents you mark as *Keep* in the "Kenniscentrum"	Manuel backend	Yes (visible only to your company)
Communications	support tickets, survey responses	HubSpot, Survicate	Yes
Diagnostics	crash traces, performance metrics	Firebase Crashlytics	No
Push-notification token	OneSignal device token	OneSignal	Yes

No precise geolocation is collected. The App does not request GPS permission.

---

4. Why we process your data and legal bases

Purpose	Legal basis (GDPR Art. 6)
Create & maintain your user account	Contract (Art. 6 (1)(b))
Provide core App functions incl. document search & knowledge-items	Contract
Deliver push notifications	Legitimate interest (Art. 6 (1)(f)); you can disable in your OS settings
Analytics & product improvement	Legitimate interest; we pseudonymise / aggregate where possible
Marketing emails (opt-in)	Consent (Art. 6 (1)(a))
Compliance & security	Legal obligation / Legitimate interest

You may withdraw consent at any time; this does not affect prior processing.

5. Third-party processors

We share data **only** with vendors that act on our behalf under a Data Processing Agreement (**DPA**) and offer GDPR-compliant safeguards:

Vendor	Purpose	Data shared	Location
Google Cloud Platform (europe-west4 – Amsterdam)	Hosting & storage	All backend data	EU
OpenAI (LLM API – Azure West EU)	Generative AI answers	Prompt text & anonymised metadata	EU
Anthropic Claude (LLM API – AWS eu-central-1)	Generative AI answers	Prompt text & anonymised metadata	EU
Google AI Gemini (LLM API – europe-west9)	Generative AI answers	Prompt text & anonymised metadata	EU
HubSpot Inc.	CRM & in-app chat	Account & support data	EU Data Centre (Frankfurt)
Microsoft Clarity	Session analytics	Usage data (pseudonymised)	EU
Survicate Sp. z o.o.	In-app surveys	Survey responses	EU
OneSignal Inc.	Push notifications	Device token, basic identifiers	USA ⇢ SCCs

We **do not sell** personal data and we do not allow third parties to use it for their own purposes.

6. Data retention

Data set	Retention period
Account & content	While account is active + 12 months, then anonymised
Knowledge-items	While subscription is active (always viewable in Kenniscentrum); deleted within 90 days after contract ends or on request
Analytics & crash logs	26 months (Google default), then aggregated
Marketing consents	Until withdrawn + 24 months (audit)
Support tickets	6 years (statutory limitation)

After expiry, data is securely erased or irreversibly anonymised.

7. International transfers

Where we transfer data outside the EEA, we rely on:

- Adequacy decisions (EU–US Data Privacy Framework), or
- Standard Contractual Clauses (SCCs) approved by the European Commission, plus supplementary measures.

8. Security measures

- Encryption in transit (TLS 1.2+) and at rest (AES-256).
- Network isolation & firewalling in Google Cloud VPC.
- Role-based access (RBAC) with MFA for all operators.
- Regular penetration tests and vulnerability scans.
- Continuous monitoring & automated incident alerts.

9. Your privacy rights

You can exercise the following rights free of charge:

- Access your data
- Rectification

- Erasure ("right to be forgotten")

- Restriction of processing

- Data portability (JSON/CSV)

- Objection to processing (incl. direct marketing)

- Lodge a complaint with the Dutch DPA (🦁 Home)

Send requests to **info@manuel.chat** – we will respond within 30 days.

---

10. Children

The App is **not directed to children under 16**. We do not knowingly collect personal data from children. If you believe a child has provided data, contact us so we can delete it immediately.

---

11. Changes to this Policy

We may update this Policy to reflect technical or legal changes. We will notify you in-app or by email and post the new version here at least 7 days before it takes effect.

---

12. Contact

Questions?

Email: Info@manuel.chat

Post: (KvK: 96013540), Burgemeester Bosmastraat 3, Winterswijk, The Netherlands

---

By installing or using the App you acknowledge that you have read and understood this Policy.

Manuel Mobile App – Privacy Policy Last updated: 21 May 2025

Important notice – No Tracking: The Manuel mobile application does **not** use Apple's Identifier for Advertisers (IDFA) and does **not** track you across apps or websites owned by other companies within the meaning of Apple's App Tracking Transparency (ATT) Framework.

1. **Who we are**

  Manuel B.V. (KvK 96013540), Burgemeester Bosmastraat 3, 7101 GX Winterswijk, The Netherlands ("Manuel", "we", "us", "our") develops and operates the Manuel mobile

application (the "App"). We are the controller of the personal data processed via the App under the EU General Data Protection Regulation ("GDPR").

Privacy contact: info@manuel.chat

2. Scope and where to find this Policy This Policy applies when you:

- install or use the App (iOS / Android);
- interact with push notifications or in-app messages;
- contact us via the App's support features.

You can read this Policy at any time under **Settings › Privacy Policy** in the App and on https://manuel.chat/privacy.
It does not cover data processed on websites or services outside the App.

3. What data we collect

Category	Examples	Collected by	Linked to you?
Account details	Name, email address, phone number, company, user role	Manuel backend	Yes
Identifiers	App-generated user ID, internal device ID, IP address (server logs). **No IDFA collected**.	Manuel backend	Yes
Usage data	Screens visited, buttons tapped, session length	Microsoft Clarity*, Manuel backend	No (aggregated unless required for support)
Knowledge items	Answers or documents you mark as "Keep" in the Knowledge Centre	Manuel backend	Yes (visible only to your company)
Communications	Support tickets, survey responses	HubSpot, Survicate	Yes
Diagnostics	Crash traces, performance metrics	Firebase Crashlytics	No
Push-notification token	OneSignal device token	OneSignal	Yes

*Microsoft Clarity ("session-replay") is **disabled by default on iOS** and only records a session after you enable "Help improve Manuel" under Settings › Privacy.*

We do not collect precise or coarse device geolocation and the App never requests GPS permission.

4. Why we process your data and legal bases

Purpose	Legal basis (GDPR Art. 6)
Create & maintain your user account	Contract (Art. 6 (1)(b))
Provide core App functions incl. document search & knowledge items	Contract
Deliver push notifications	Legitimate interest (Art. 6 (1)(f)); you can disable in OS settings
Analytics & product improvement (pseudonymised/aggregated)	Legitimate interest
Marketing emails (opt-in)	Consent (Art. 6 (1)(a))
Compliance & security	Legal obligation / Legitimate interest

You may withdraw consent at any time; this does not affect processing carried out before withdrawal.

5. How you can manage your data (incl. in-app deletion)

Delete account in-app:

- Open **Settings › Account › Delete account**.
- Confirm deletion; we immediately log you out and queue your account and associated personal data for permanent erasure within **30 days** (unless retention is required by law – e.g. billing records).

Delete knowledge items:
Inside the Knowledge Centre tap ⋯ › **Delete**.

Export your data:
Open **Settings › Account › Export data** to download a JSON/CSV archive.

If you cannot access the App, email info@manuel.chat.

6. Third-party processors

We share data only with vendors acting on our behalf under a Data Processing Agreement (DPA) and offering GDPR-compliant safeguards *and* an Apple Privacy Manifest ("PrivacyInfo.xcprivacy") for their SDK:

Vendor	Purpose	Data shared	Location / Transfer mechanism
Google Cloud Platform (europe-west4 – Amsterdam)	Hosting & storage	All backend data	EU
OpenAI (Azure West EU)	Generative-AI answers	Prompt text & anonymised metadata	EU
Anthropic Claude (AWS eu-central-1)	Generative-AI answers	Prompt text & anonymised metadata	EU
Google AI Gemini (europe-west9)	Generative-AI answers	Prompt text & anonymised metadata	EU
HubSpot Inc.	CRM & in-app chat	Account & support data	EU (Frankfurt DC)
Microsoft Clarity	**Session-replay** analytics (opt-in)	Usage data (pseudonymised)	EU
Survicate Sp. z o.o.	In-app surveys	Survey responses	EU
OneSignal Inc.	Push notifications	Device token, basic identifiers	USA → SCCs

We do not sell personal data and we do not allow third parties to use it for their own purposes.

7. Data retention

Data set	Retention period
Account & content	While account is active + 12 months, then anonymised
Knowledge items	While subscription is active; deleted within 90 days after contract ends or on request
Push-notification tokens	24 months after last app activity
Analytics & crash logs	26 months (Google default), then aggregated
Marketing consents	Until withdrawn + 24 months (audit)
Support tickets	6 years (statutory limitation)

After expiry, data is securely erased or irreversibly anonymised.

8. International transfers Where we transfer data outside the European Economic Area we rely on:

- Adequacy decisions (e.g. EU–US Data Privacy Framework), or
- European Commission Standard Contractual Clauses (SCCs) plus supplementary measures (encryption, access controls).

9. Security measures & incident reporting

- Encryption in transit (TLS 1.2+) and at rest (AES-256).
- Network isolation & firewalling in Google Cloud VPC.
- Role-based access control (RBAC) with multi-factor authentication.
- Regular penetration tests and automated vulnerability scans.
- Continuous monitoring & incident alerts.
- **If a personal-data breach occurs, we will notify the Dutch Data Protection Authority and affected users within 72 hours, in accordance with Articles 33-34 GDPR.**

10. Your privacy rights You have the right to:

- Access your data
- Rectify inaccurate data
- Erase data ("right to be forgotten")
- Restrict processing
- Data portability (JSON/CSV)
- Object to processing (including direct marketing)

To exercise these rights use the in-app tools (see §5) or email **info@manuel.chat**. We respond within 30 days.

11. Children
The App is **not directed to children under 13 years (US COPPA) or 16 years (EU GDPR)**. We block registration below that age. If you believe a child has provided personal data, contact us so we can delete it immediately.

12. Changes to this Policy
We may update this Policy to reflect technical or legal changes. We will notify you in-app or by email and post the new version here at least **seven (7) days** before it takes effect. The revision date at the top indicates the latest change.

13. Contact Email: **info@manuel.chat**
Post: Manuel B.V., Burgemeester Bosmastraat 3, 7101 GX Winterswijk, The Netherlands