

MedQ Privacy Policy

Early Access · Effective 2026-05-14

Effective Date: 2026-05-14 **Last Updated:** 2026-05-14 **Version:** 2.0 (Early Access)

1. Introduction

This Privacy Policy describes how MedQ (“we,” “us,” “our”) collects, uses, shares, and protects personal data. MedQ is in **Early Access**: the product is operational and commercially available, but operated by a small team. We meet our legal obligations under the EU General Data Protection Regulation (GDPR), the Belgian Law of 30 July 2018, the Belgian Law of 22 August 2002 on patient rights, and applicable ePrivacy rules in full. We are honest about the scale of the operation and do not claim certifications we do not hold.

1.1 Operator information

- **Trading name:** MedQ
- **Legal form:** Sole proprietorship (Eenmanszaak), Belgian law
- **Company registration:** 0775672277
- **VAT number:** BE0775672277
- **Registered address:** Klossestraat 11 bus 101, De Pinte, Belgium
- **Privacy contact:** contact@medq.be

1.2 Our two roles under GDPR

As a data processor: When healthcare practices use MedQ to manage their patients’ appointment and administrative information, the practice is the **data controller** and MedQ is the **data processor** acting on the practice’s documented instructions. The terms of that processing are governed by a separate **Data Processing Agreement (DPA)** entered into between the practice and MedQ. Patients should generally direct rights requests concerning their appointment data to the practice that holds the relationship with them.

As a data controller: MedQ is the controller for data about its direct customers (practice administrators, billing contacts, support correspondence), website visitors, marketing recipients, and platform telemetry.

This Privacy Policy describes both roles. Where the distinction matters, we state which capacity applies.

2. Scope

This Privacy Policy applies to healthcare providers and practice staff using MedQ, patients whose appointment and administrative information is processed through MedQ, visitors to medq.be, recipients of our marketing communications, and anyone contacting our support team.

2.1 What MedQ does and does not process

MedQ is administrative healthcare software for appointment scheduling, patient flow, waiting-room management, and related practice workflows. MedQ does **not** store or process

clinical records, diagnoses, treatment notes, or prescription data, and is not built or operated as an Electronic Health Record.

However, some information processed through MedQ can, in context, reveal information about a patient's health. Examples include the specialty of the practice, the type of appointment (in a multi-specialty practice), and practice-specific attributes such as pregnancy status used for scheduling in obstetrics. Such information is treated as a **special category of personal data** under Article 9 GDPR, with the legal basis described in Section 4.5 and the safeguards in Section 10.

We treat this honestly because pretending otherwise would put both MedQ and our customers in a worse legal position.

3. Information we collect

3.1 Patient administrative information (MedQ as processor)

Through the practice's use of MedQ:

Identifying information: first and last name, date of birth where required, patient reference assigned by the practice.

Contact information: email, telephone, postal address (where collected by the practice), preferred language.

Appointment information: date, time, duration, type, status, provider assigned, check-in timestamp, queue position, administrative notes, notification history.

Practice-specific attributes: where the practice's workflow requires, attributes such as pregnancy status (obstetrics), age category (paediatrics), or similar administrative attributes.

Generated identifiers: check-in codes, confirmation tokens, queue display codes, session records.

3.2 Provider and practice information (MedQ as controller)

Names, professional titles, work contact details, practice name and registration identifiers, working hours and availability, account credentials (passwords stored as salted hashes, never plaintext), role and permission assignments, user preferences.

3.3 Billing information (MedQ as controller)

Billing contact details, payment method information (handled by our payment processor, never stored on MedQ servers in full), invoices, subscription history.

3.4 Technical information (MedQ as controller)

IP address (truncated where possible for analytics), device type, operating system, browser version, pages visited, features used, timestamps, referring URL, error reports and diagnostic logs, cookie and session identifiers.

3.5 Customer support and feedback (MedQ as controller)

Correspondence with our support team, bug reports, feature requests, survey responses.

3.6 Marketing data (MedQ as controller)

Subscriber contact details, engagement metrics where applicable, marketing preferences.

4. Legal basis for processing

4.1 Performance of a contract (Art 6(1)(b))

Provision of the MedQ service, account management, billing, and customer support.

4.2 Legitimate interests (Art 6(1)(f))

- Security monitoring, fraud and abuse prevention
- Product analytics in aggregate or pseudonymised form
- Direct marketing to existing business customers about similar products (soft opt-in under Belgian Code of Economic Law Art VI.110)
- Internal record-keeping, dispute defence, exercise of legal claims

A balancing test has been conducted and is available on request.

4.3 Legal obligation (Art 6(1)(c))

- Belgian accounting and tax law (invoice retention for seven years)
- GDPR record-keeping and breach-notification obligations
- Responses to lawful requests from competent authorities

4.4 Consent (Art 6(1)(a))

- Non-essential cookies and similar technologies
- Marketing communications where soft opt-in does not apply
- Where the practice (as controller) relies on patient consent for specific processing

Consent can be withdrawn at any time without affecting the lawfulness of processing prior to withdrawal.

4.5 Special category data (Art 9)

Where MedQ processes data that may reveal health information (see Section 2.1), the lawful basis is:

- **Art 9(2)(h)** processing necessary for the management of health or social care systems and services, performed by or under the responsibility of a healthcare professional bound by professional secrecy, **or**
- **Art 9(2)(a)** explicit consent obtained by the practice from the patient

In both cases, MedQ acts on the documented instructions of the practice (as controller) and applies the safeguards required by Article 9(3) and Belgian healthcare confidentiality law.

5. How we use information

5.1 Service delivery

Patient check-in and waiting-room management, appointment scheduling and calendar synchronisation, sending confirmations and reminders on behalf of the practice, real-time queue and display updates, authentication and access control.

5.2 Customer communication

Account, billing, and service notifications, technical support, product and security advisories, marketing communications where you have not opted out.

5.3 Operations

Availability and performance monitoring, security monitoring and incident response, diagnostic logging and error resolution, backups and disaster recovery, product improvement and debugging.

5.4 Legal and regulatory

Compliance with GDPR, Belgian data protection law, applicable healthcare law, cooperation with competent regulators, defending or pursuing legal claims.

6. Automated decision-making

MedQ does not make decisions about patients that have legal or similarly significant effects through solely automated means within the meaning of Article 22 GDPR. Automated processing inside MedQ is limited to operational features (slot availability, reminder scheduling, queue ordering) which support but do not replace decisions made by practice staff.

If this changes, this Privacy Policy will be updated and, where required, separate notice will be provided.

7. Information sharing

7.1 Within the practice

Patient administrative information is accessible inside the practice to authorised users as configured by the practice's administrator. MedQ enforces role-based access controls; the practice determines who has access to what.

7.2 Sub-processors

We engage carefully selected sub-processors to operate the service. Our current sub-processors are listed in our **Sub-processor List**, published at <https://medq.be/subprocessors> and updated when changes occur. The list identifies each sub-processor's name, function, location, and the transfer mechanism for any data transfer outside the EEA.

Categories of sub-processors currently engaged include:

- Cloud hosting and infrastructure (servers, storage, networking)
- Transactional email delivery
- Payment processing
- SMS delivery (where the practice has enabled SMS reminders)
- Push notification gateways (where applicable)
- Error monitoring and diagnostics (limited diagnostic data)

All sub-processors are bound by written contracts that impose data protection obligations no less protective than those in our DPA with the practice.

7.3 Changes to sub-processors

We give controllers at least 30 days' notice of intended changes to the sub-processor list. The controller may object on reasonable data protection grounds.

7.4 Legal disclosures

We may disclose information where required by law or where we believe in good faith that disclosure is necessary to comply with legal process, protect the rights or safety of MedQ, customers, or others, investigate fraud or security incidents, or respond to a request from a competent authority.

7.5 Business transfers

In the event of a merger, acquisition, reorganisation, or sale of all or part of our business, personal data may be transferred as part of that transaction. We will provide notice in advance and the receiving entity will be bound by terms no less protective than this Privacy Policy.

7.6 No marketing use of patient data

We do not use patient administrative information for any marketing purpose. We do not sell personal data.

7.7 No cross-tenant sharing

Each practice's data is logically isolated. We do not share one practice's data with another.

8. International data transfers

Personal data processed by MedQ is primarily stored on infrastructure located within the European Economic Area (currently Germany). Where a specific sub-processor processes data outside the EEA, we rely on:

- EU Commission adequacy decisions, where they apply
- Standard Contractual Clauses (SCCs) adopted by the European Commission, supplemented by additional technical and organisational measures where required following a Transfer Impact Assessment
- EU-US Data Privacy Framework certification of the recipient, where applicable
- Other mechanisms recognised under Articles 46–49 GDPR

A summary of our TIA conclusions for sub-processors that process data outside the EEA is available on request.

9. Data retention

9.1 Patient administrative data (controller-determined)

While MedQ is the processor, retention is configured by the practice as controller. Defaults in MedQ:

- **Active appointments and patient records:** for the duration of the subscription, plus 30 days after termination for export
- **Cancelled or completed appointments:** retained until the practice deletes them or sets a shorter retention policy
- **Notification and reminder logs:** 24 months, then deleted

The practice is responsible for ensuring its retention configuration complies with Belgian healthcare and accounting law.

9.2 Provider account and billing data

- **Account information:** while the subscription is active, plus 12 months
- **Billing records and invoices:** 7 years, as required by Belgian accounting law
- **Authentication credentials:** while the account is active; deleted on closure

9.3 Technical and security logs

- **Application logs:** 90 days
- **Security and access logs:** 12 months
- **Aggregated, pseudonymised analytics:** indefinite

9.4 Backups

Daily backups retained for 14 days, weekly backups for 8 weeks, monthly backups for 12 months. Data deleted from the live system persists in backups until the relevant backup expires.

9.5 Marketing and support

- **Support tickets:** 24 months from closure
- **Marketing subscribers:** until unsubscribe, plus suppression list entry to honour the opt-out

9.6 Deletion procedure

At the end of the retention period or on valid deletion request, data is securely deleted using methods designed to make recovery infeasible. Pseudonymised aggregates may be retained for statistical purposes.

10. Data security

We are transparent about what we do and do not do. We do not currently hold ISO 27001, SOC 2, or similar formal certifications. We do implement the measures below, which are appropriate to the nature, scope, and risks of the processing.

10.1 Technical measures

- **Encryption in transit:** TLS 1.2 or higher for all connections
- **Encryption at rest:** AES-256 for stored databases and backups
- **Authentication:** salted password hashes; multi-factor authentication available for provider accounts and recommended for administrator accounts
- **Access control:** role-based access at application and infrastructure level; principle of least privilege
- **Network security:** firewall rules with conntrack-based controls, isolated container networking, database services not directly exposed to the public internet
- **Monitoring:** continuous monitoring of system availability, performance, and security events with alerting on anomalies
- **Patching:** routine application and operating system patching; emergency patching for security-relevant vulnerabilities

10.2 Organisational measures

- Written policies governing access, change management, and incident response
- Confidentiality obligations on personnel and sub-processors
- Restricted access to production systems on a need-to-know basis
- Periodic review of access rights
- Vendor due diligence on sub-processors

10.3 Vulnerability disclosure

Security researchers and customers are invited to report suspected vulnerabilities to **security@medq.be**. We commit to acknowledging reports within 5 business days and to working in good faith on remediation. We do not pursue legal action against researchers who act in good faith and within the scope of our disclosure policy.

10.4 Personal data breach notification

- Where MedQ is processor, the controller is notified without undue delay and in any event within 48 hours of MedQ becoming aware of the breach, with sufficient information for the controller to meet its own Article 33 obligations.
 - Where MedQ is controller, we notify the Belgian Data Protection Authority within 72 hours where required by Article 33 GDPR, and affected data subjects without undue delay where Article 34 applies.
-

11. Cookies and similar technologies

11.1 Categories used

Strictly necessary: required for the service to function (authentication, session management, security tokens, load balancing). These do not require consent.

Functional: set with your consent to remember preferences such as language and interface settings.

Analytics: we do not currently use analytics tooling on the marketing website or in the Service. If we begin to use analytics in the future, we will update this Privacy Policy and the cookie consent banner accordingly before any such cookies are set.

11.2 Cookie consent

A consent banner is presented on first visit and allows you to accept or refuse non-essential cookies. You can change your choice at any time via the cookie settings link in the footer.

11.3 Cookie list

A detailed list of cookies (name, purpose, provider, duration) is maintained on our cookie page at <https://medq.be/cookies>.

11.4 PWA storage

MedQ is also available as a Progressive Web App. Where installed, limited cached data may be stored locally to enable offline functionality and performance. Cached data is removed when you clear browser storage or uninstall the PWA. Push notification payloads do not contain identifying patient information.

12. Your rights

12.1 Rights under GDPR

You have the right to: access your personal data and obtain a copy; rectify inaccurate or incomplete data; erase (“right to be forgotten”) in defined circumstances; restrict processing in defined circumstances; portability in a structured, commonly used, machine-readable format; object to processing based on legitimate interests, including direct marketing (where you object to direct marketing, we stop immediately and without need for justification); withdraw consent at any time where processing is based on consent; not be subject to a decision based solely on automated processing producing legal or similarly significant effects (MedQ does not perform such processing, see Section 6).

12.2 How to exercise rights

If your request concerns appointment or patient data held by a healthcare practice: contact the practice directly. The practice is the controller of that data, and MedQ as processor cannot grant or deny access without the practice’s authorisation. We will assist the practice in responding.

If your request concerns data for which MedQ is controller (account, marketing, website use): contact contact@medq.be with your name, the nature of your request, and information to verify your identity.

We respond within one month, extendable by two further months for complex requests, in line with Article 12(3) GDPR.

12.3 Right to lodge a complaint

If you believe we have not handled your personal data in accordance with applicable law, you may lodge a complaint with the Belgian Data Protection Authority:

Gegevensbeschermingsautoriteit / Autorité de protection des données Drukpersstraat 35 / Rue de la Presse 35 1000 Brussels, Belgium **Email:** contact@apd-gba.be **Website:** www.gegevensbeschermingsautoriteit.be

You may also lodge a complaint with the supervisory authority in your EU/EEA member state of residence.

13. Marketing communications

We send service-related notices, security advisories, and product updates to customer contacts. These are required for the operation of the service and are not “marketing” in the regulatory sense.

For promotional communications, we send these only to subscribers and to existing business customers about products and services similar to those already purchased (soft opt-in, Belgian Code of Economic Law Art VI.110 §4). Every promotional email contains a clear and free unsubscribe link. You can unsubscribe at any time by clicking the link or contacting contact@medq.be.

We do not engage in profiling for marketing purposes.

14. Children and minors

MedQ is intended for use by healthcare practices and their authorised staff (adults). Patient information processed through MedQ may relate to minors, in which case the practice is responsible for the legal basis, consent (where applicable), and compliance with Belgian patient rights law:

- For children under 12, the patient's legal representative exercises patient rights
- Between 12 and 18, the patient is involved according to age and maturity, in consultation with the legal representative, in line with the Law of 22 August 2002 on patient rights

The Belgian age of digital consent for information society services is 13 (Law of 30 July 2018, Article 7), which applies if a patient personally creates an account in any patient-facing surface.

We do not knowingly collect personal data directly from individuals under 13 without involvement of a legal representative.

15. Data Protection Impact Assessment

Processing patient data through a multi-tenant healthcare SaaS involves the assessment required by Article 35 GDPR. MedQ maintains a Data Protection Impact Assessment covering the processing operations described in this Privacy Policy (current version: 1.0, 2026-05-14). A summary is available to controllers (practices) on request, to support their own DPIA obligations.

16. Records of processing activities

In accordance with Article 30 GDPR, MedQ maintains records of processing activities for both its controller and processor roles. These records are available to the Belgian Data Protection Authority on request.

17. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in our processing practices, new features, or legal requirements. Material changes will be communicated by email to account holders at the registered contact address, in-application notice on next login, and update to the "Last Updated" date at the top of this document.

For material adverse changes, we provide at least 30 days' advance notice. Continued use of MedQ after the effective date constitutes acceptance. If you do not accept the changes, you may terminate your subscription as set out in the Terms of Service.

18. Contact

General and privacy inquiries: contact@medq.be **Security:** security@medq.be **Postal:** MedQ, Klossestraat 11 bus 101, De Pinte, Belgium **Data Protection Officer:** contact@medq.be (acting DPO contact for the sole proprietorship)

Last Updated: 2026-05-14