MedQ Data Processing Agreement

Article 28 GDPR · Effective at subscription

Between:

The customer identified in the subscription or signature page ("Controller," "Practice")

And:

MedQ, sole proprietorship, registered office at Klossestraat 11 bus 101, De Pinte, Belgium, company number 0775672277, VAT BE0775672277 ("Processor," "MedQ")

(Each a "Party," together the "Parties.")

Effective Date: the date the Controller accepts these terms by subscribing to the MedQ Service, or the date of signature where this DPA is executed separately.

---

1. Background

The Controller has subscribed to the MedQ Service under the MedQ Terms of Service (the "Service Agreement"). In providing the Service, MedQ processes personal data on behalf of the Controller. This Data Processing Agreement ("DPA") sets out the terms of that processing in accordance with Article 28 of Regulation (EU) 2016/679 (the "GDPR") and the Belgian Law of 30 July 2018.

This DPA is incorporated into the Service Agreement. In case of conflict between this DPA and the Service Agreement on matters of personal data processing, this DPA prevails.

---

2. Definitions

Terms not defined in this DPA have the meaning given to them in the GDPR. In particular:

- **"Personal Data"** means any information relating to an identified or identifiable natural person processed by MedQ on behalf of the Controller in connection with the Service.
- **"Processing"** has the meaning in Article 4(2) GDPR.
- **"Data Subject"** means the natural person to whom Personal Data relates.
- **"Sub-processor"** means any third party engaged by MedQ to process Personal Data on its behalf.
- **"Personal Data Breach"** has the meaning in Article 4(12) GDPR.
- **"Service"** means the MedQ healthcare practice administration platform as described in the Service Agreement.

The subject matter, duration, nature and purpose of the processing, types of Personal Data, and categories of Data Subjects are described in **Annex 1**.

The technical and organisational security measures are described in **Annex 2**.

The list of authorised Sub-processors is maintained at the URL set out in **Annex 3**.

---

3. Roles of the Parties

The Controller is the data controller of the Personal Data. MedQ is the data processor and processes Personal Data only on the documented instructions of the Controller.

The Controller's documented instructions are: (a) this DPA, (b) the Service Agreement, (c) the Controller's use of the Service's documented features and configuration options (which constitute instructions), and (d) any further written instructions from the Controller that are consistent with the Service Agreement.

If MedQ believes a Controller instruction would result in a violation of the GDPR or other applicable data protection law, MedQ shall inform the Controller and may suspend execution of the instruction until clarified.

For the avoidance of doubt, MedQ acts as data controller (not processor) for: (i) data about the Controller's account, billing, and direct contacts; (ii) website visitor data; (iii) marketing data; (iv) platform telemetry; and (v) Personal Data of MedQ's own employees and contractors. These are governed by the MedQ Privacy Policy and are outside the scope of this DPA.

---

4. Obligations of MedQ

4.1 Processing only on documented instructions

MedQ processes Personal Data only on the Controller's documented instructions, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by Belgian or EU law. In such a case MedQ shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 Confidentiality

MedQ ensures that personnel authorised to process Personal Data have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality.

4.3 Security

MedQ implements the technical and organisational measures described in **Annex 2** to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

4.4 Sub-processors

The Controller provides **general written authorisation** for MedQ to engage Sub-processors, subject to this Section.

- MedQ maintains a current list of Sub-processors at the URL set out in Annex 3.
- MedQ shall inform the Controller of any intended addition or replacement of Sub-processors at least 30 days before the change takes effect, giving the Controller the opportunity to object on reasonable data protection grounds.
- If the Controller reasonably objects and MedQ cannot accommodate the objection, the Controller may terminate the affected portion of the Service Agreement without penalty, with pro-rata refund of pre-paid fees for the unused portion of the term.
- MedQ imposes data protection obligations on each Sub-processor by written contract that are no less protective than those in this DPA.

- MedQ remains fully liable to the Controller for the performance of its Sub-processors' obligations.

4.5 Assistance with Data Subject rights

Taking into account the nature of the processing, MedQ shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects to exercise their rights under Chapter III GDPR.

This assistance includes:

- Providing the Controller with the ability, through the Service's features, to access, rectify, erase, restrict, and export Personal Data of Data Subjects
- Forwarding to the Controller any Data Subject rights requests received directly by MedQ
- Providing reasonable technical assistance where the Service's standard features are insufficient

MedQ may charge a reasonable fee for assistance that goes substantially beyond standard support, where the volume or complexity of requests is excessive.

4.6 Assistance with controller compliance

MedQ shall assist the Controller, insofar as possible and taking into account the nature of processing and the information available to MedQ, in ensuring compliance with the Controller's obligations under Articles 32 to 36 GDPR. This includes:

- Cooperation on security of processing (Art 32)
- Notification of Personal Data Breaches to the Controller (Art 33; see Section 6 below)
- Assistance in communicating Personal Data Breaches to Data Subjects where required (Art 34)
- Assistance with Data Protection Impact Assessments and prior consultation where required (Art 35-36)

4.7 Return and deletion at end

On termination of the Service Agreement, MedQ shall, at the choice of the Controller:

- Delete all Personal Data, or
- Return all Personal Data to the Controller

and delete existing copies, unless Belgian or EU law requires storage of the Personal Data. The Controller has 30 days from termination to export Personal Data through the Service's export functionality or by requesting an export from MedQ.

After the 30-day export window, MedQ deletes live Personal Data. Personal Data persisting in backups is deleted on the schedule set out in the Privacy Policy.

4.8 Audits

MedQ makes available to the Controller all information necessary to demonstrate compliance with this DPA. On reasonable request, and no more than once per calendar year (except following a Personal Data Breach), the Controller (or a third-party auditor mandated by the Controller and bound by confidentiality, and not a competitor of MedQ) may conduct an audit of MedQ's compliance with this DPA, subject to:

- At least 30 days' advance written notice
- Reasonable scope, duration, and timing agreed with MedQ
- Conduct during normal business hours with minimum disruption
- The Controller bearing its own audit costs and reimbursing MedQ for time spent if the audit exceeds one business day
- Compliance with MedQ's reasonable security and confidentiality requirements
- Findings being treated as confidential information of MedQ

Where MedQ holds relevant third-party audit reports or certifications (currently none, see Section 4.9), these may be provided in satisfaction of the audit right.

4.9 Certifications

MedQ does not currently hold ISO 27001, SOC 2, or comparable third-party certifications. The Controller acknowledges this and accepts that the technical and organisational measures in Annex 2, together with the audit rights in Section 4.8, constitute appropriate compliance demonstration.

4.10 Records of processing

MedQ maintains records of categories of processing activities carried out on behalf of the Controller in accordance with Article 30(2) GDPR. These records are made available to the Belgian Data Protection Authority on request.

---

5. Obligations of the Controller

The Controller warrants and undertakes that:

- It has a lawful basis under the GDPR for the processing it instructs MedQ to perform
- Where processing involves special categories of data under Article 9 GDPR (including health-related data as described in the MedQ Privacy Policy), the Controller has a valid lawful basis under Article 9(2), typically Article 9(2)(h) read together with Belgian health-care confidentiality law
- It has provided Data Subjects with the information required by Articles 13 and 14 GDPR
- It has obtained any consents required for the processing
- Its instructions to MedQ comply with the GDPR and other applicable law
- It has implemented appropriate technical and organisational measures on its own side, including secure user credentials, role configuration, and device security
- It complies with Belgian patient rights law in its handling of Data Subject relationships

---

6. Personal Data Breach

6.1 Notification to Controller

MedQ shall notify the Controller without undue delay, and in any event within **48 hours**, after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller. The notification shall, at minimum:

- Describe the nature of the breach, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned

- Communicate the name and contact details of MedQ's point of contact for further information
- Describe the likely consequences of the breach
- Describe the measures taken or proposed to address the breach, including, where appropriate, measures to mitigate possible adverse effects

Where it is not possible to provide all information at once, MedQ provides it in phases without undue further delay.

6.2 Cooperation

MedQ cooperates with the Controller and provides reasonable assistance, including in:

- The Controller's notification to the Belgian Data Protection Authority under Article 33 GDPR (typically within 72 hours of the Controller's awareness)
- The Controller's communication to affected Data Subjects under Article 34 GDPR where required
- Investigation and remediation of the breach

6.3 No admission

A notification under this Section does not constitute an acknowledgement by MedQ of fault or liability for the breach.

---

7. International data transfers

Where MedQ or a Sub-processor processes Personal Data outside the European Economic Area, the transfer is subject to one or more of the following safeguards under Chapter V GDPR:

- An EU Commission adequacy decision applicable to the recipient country (Art 45)
- Standard Contractual Clauses adopted by the European Commission (Art 46(2)(c)), 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

MedQ identifies in the Sub-processor List which Sub-processors are subject to such transfers and the applicable mechanism. A summary of MedQ's Transfer Impact Assessments is available to the Controller on request.

The Controller hereby authorises MedQ to enter into Standard Contractual Clauses with Sub-processors on the Controller's behalf where required for such transfers, in the form adopted by the European Commission.

---

8. Liability

The liability of each Party under this DPA is subject to the limitation of liability set out in the Service Agreement. The Parties acknowledge that liability between controller and processor in respect of the rights of Data Subjects is governed by Article 82 GDPR.

For documented administrative fines imposed on the Controller by the Belgian Data Protection Authority or another competent supervisory authority and directly resulting from

MedQ's proven breach of this DPA, MedQ's liability is capped as set out in the Service Agreement.

---

9. Term and termination

This DPA takes effect on the Effective Date and continues for the duration of the Service Agreement. On termination of the Service Agreement, the obligations in Sections 4.7 (return and deletion) and any other Sections that by their nature should survive (including Sections 4.2, 6.2 in respect of breaches occurring during the term, and 8) survive.

---

10. General

10.1 Governing law and jurisdiction

This DPA is governed by Belgian law. The courts of Gent, Belgium have exclusive jurisdiction over any dispute arising from this DPA, subject to mandatory rules conferring jurisdiction elsewhere.

10.2 Order of precedence

In case of conflict between this DPA and the Service Agreement on matters of personal data processing, this DPA prevails.

10.3 Changes

MedQ may update this DPA to reflect changes in applicable data protection law or in the operation of the Service. Material changes are notified to the Controller in line with the change procedure in the Service Agreement.

10.4 Signature

Where the Controller accepts the Service Agreement (including by online subscription), the Controller is deemed to have accepted this DPA. Where a manually signed DPA is required, an authorised representative of the Controller and MedQ shall sign below.

Controller

Name: _____

Title: _____

Date: _____

Signature: _____

MedQ

Name: Laurent Meersman

Title: Sole Proprietor

Date: _____

Signature: _____

Annex 1 — Description of the processing

Subject matter
Provision of the MedQ healthcare practice administration platform to the Controller, including patient check-in, appointment scheduling, waiting-room management, patient administrative database management, scheduling and display, and appointment notifications.

Duration
For the duration of the Service Agreement, plus a 30-day export window and applicable backup retention periods after termination.

Nature and purpose of processing
Collection, recording, organisation, structuring, storage, retrieval, use, transmission, dissemination (to the extent of sending notifications on behalf of the Controller), restriction, erasure, and destruction of Personal Data, for the purpose of supporting the Controller's administrative healthcare operations.

Types of Personal Data
- Identifying data: name, date of birth, patient reference
- Contact data: email, telephone, postal address, preferred language
- Appointment data: date, time, duration, type, status, provider assignment, check-in timestamp, queue position, administrative notes
- Practice-specific attributes that may relate to health (Article 9 GDPR): for example, pregnancy status in obstetrics, age category in paediatrics, or similar administrative attributes configured by the Controller
- Account and authentication data of Controller's staff: name, work contact, role, credentials (hashed)
- Generated identifiers: confirmation tokens, check-in codes, queue codes, session records

Categories of Data Subjects
- Patients of the Controller
- Staff of the Controller using the Service
- Legal representatives of patients where applicable

Categories of recipients
- The Controller's authorised staff
- MedQ personnel acting on behalf of MedQ
- Authorised Sub-processors listed in Annex 3
- Competent authorities where required by law

Annex 2 — Technical and organisational measures

The following measures are implemented to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

Pseudonymisation and encryption
- Encryption in transit: TLS 1.2 or higher for all connections to the Service
- Passwords stored as salted hashes; plaintext passwords are not stored

Confidentiality

- Role-based access control at application and infrastructure level, applying the principle of least privilege
- Multi-factor authentication available for provider accounts; recommended for administrators
- Restricted access to production systems on a need-to-know basis
- Personnel under confidentiality obligations
- Sub-processors under written contracts imposing equivalent obligations
- Logical isolation of tenant data; tenants cannot access each other's data

Integrity

- Change management procedures for production deployments
- Application and operating system patching; emergency patching for security-relevant vulnerabilities
- Monitoring and alerting on system events and anomalies
- Application-level validation and access checks

Availability and resilience

- Automated full server backups via the hosting provider, run daily and retained for 7 days, stored on infrastructure separate from the production server within the same EEA region
- Production infrastructure hosted in commercial data centres (Hetzner, Nuremberg, Germany) with environmental and physical controls operated by the hosting provider
- Documented operational runbooks
- A formal backup operator arrangement for extended primary operator unavailability is being established as part of the Early Access programme; until that arrangement is in place, the Controller is informed via this DPA of the sole-operator status, and recovery in such events relies on documented runbooks and pre-arranged credential access

Network security

- Firewall rules controlling inbound and outbound traffic, with conntrack-based matching
- Isolated container networking; database services not directly exposed to the public internet
- Reverse proxy with TLS termination

Regular testing and evaluation

- Periodic review of access rights
- Vendor due diligence on Sub-processors
- Vulnerability disclosure programme: security@medq.be
- Logging and review of security-relevant events

Incident response

- Documented incident response procedure
- Personal Data Breach notification to Controller within 48 hours of awareness (see Section 6 of the DPA)
- Cooperation with Controller on regulator notifications and Data Subject communications

Limitations acknowledged

MedQ does not currently hold third-party certifications such as ISO 27001 or SOC 2. The Controller accepts that the measures above, together with the audit rights in Section 4.8 of

the DPA, constitute appropriate compliance demonstration for an Early Access product at this stage. Measures evolve with the product; the Controller is informed of material changes.

Annex 3 — Authorised Sub-processors

The current list of Sub-processors is maintained at:

https://medq.be/subprocessors

The list identifies for each Sub-processor: name, role, country of processing, and applicable transfer mechanism where processing takes place outside the European Economic Area. The list is updated on changes, with notification to Controllers as set out in Section 4.4 of this DPA.

At the date of this DPA, the categories of Sub-processors engaged include: cloud hosting and infrastructure, transactional email delivery, payment processing, SMS delivery (where enabled by the Controller), push notification delivery (where applicable), error monitoring and diagnostics, and customer support tooling.

End of DPA.