Data Processing Agreement ››› BIQE SaaS

Data Processing Agreement (DPA) — BIQE SaaS

Version: 1.0 — 3 May 2026
Service: BIQE handwritten text recognition SaaS at `ocr-handwriting.online`

Parties

This Data Processing Agreement (“DPA”) is entered into between:

(1) Processor: BIQE V.O.F. Nijstad 14 8281 BB Genemuiden The Netherlands KvK 69268916, VAT NL857810546B01 (“BIQE”, “Processor”, “we”, “us”, “our”)

and

(2) Controller: The Customer identified in the BIQE account or in the Order Form referencing this DPA (“Customer”, “Controller”, “you”, “your”)

(BIQE and Customer each a “Party”, together the “Parties”.)

Recitals

A. The Customer has subscribed to the BIQE handwritten text recognition SaaS at `ocr-handwriting.online` (the “Service”) under the BIQE Terms of Service (“Main Agreement”).

B. In the course of using the Service, the Customer may upload scanned documents that contain personal data within the meaning of Regulation (EU) 2016/679 (“GDPR”).

C. Where the Customer uploads such personal data for processing through the Service, the Customer acts as **Controller** and BIQE acts as **Processor** within the meaning of GDPR Art. 4(7) and 4(8).

D. The Parties wish to set out the terms governing such processing, in compliance with GDPR Art. 28.

This DPA forms an integral part of the Main Agreement. In the event of conflict between this DPA and the Main Agreement on matters of personal-data processing, this DPA prevails.

---

1. Definitions

Capitalised terms not defined in this DPA have the meanings given in the GDPR or the Main Agreement.

- **Personal Data** — any information relating to an identified or identifiable natural person (as defined in GDPR Art. 4(1)) that the Customer uploads to the Service or otherwise has BIQE process on its behalf.
- **Processing** — any operation performed on Personal Data, as defined in GDPR Art. 4(2).
- **Sub-processor** — any third party engaged by BIQE that processes Personal Data on behalf of BIQE in connection with the Service.
- **Data Subject** — the natural person to whom Personal Data relates.
- **Personal Data Breach** — a breach of security as defined in GDPR Art. 4(12).

---

2. Subject Matter, Nature, and Purpose of Processing

2.1 Subject matter

BIQE processes Personal Data on behalf of the Customer for the sole purpose of providing the Service: layout analysis, handwritten text recognition (HTR), and LLM-based correction of scans uploaded by the Customer.

2.2 Nature of processing

The Personal Data, when present in uploaded scans, is processed automatically by: - Storing the uploaded scan in cloud storage - Running the scan through the BIQE pipeline (layout detection, HTR, LLM correction) - Returning the recognised text to the Customer through the portal or

API - Deleting the scan and result automatically after the retention period (see §6)

BIQE does not manually review the contents of scans except where strictly necessary for security, debugging at the Customer's request, or legal compliance.

2.3 Purpose of processing

Provision of the Service as agreed in the Main Agreement. BIQE does not use Personal Data for any other purpose, including (without limitation) training AI models, marketing, or onward sale.

2.4 Duration of processing

For the duration of the Main Agreement, plus the retention periods set out in §6 of this DPA.

---

3. Categories of Personal Data and Data Subjects

3.1 Categories of Personal Data

The Personal Data processed depends entirely on the content of the scans the Customer uploads. Common categories in the Customer's expected use cases include:

- **Identification data** — names, signatures, dates of birth (e.g. in civil-registry records, parish books, deeds)
- **Contact data** — addresses, places of residence (e.g. in correspondence)
- **Family relationship data** — parentage, marital status (e.g. in genealogical records)
- **Free-text content** — anything written by hand or printed in the source document, which may include opinions, religious affiliation, health-related references, or other content depending on the source

The Customer is responsible for assessing what categories its specific source documents contain, including any **special categories of personal data** (GDPR Art. 9) such as religious, ethnic, health, or political data. The Customer must inform BIQE in writing if special-category data is involved at material scale (see §4.3).

3.2 Categories of Data Subjects

Persons whose Personal Data appears in the scans uploaded by the Customer. Typical categories: - Historical persons (deceased, often pre-1900) — note that GDPR generally does not apply to data of deceased persons in most EU jurisdictions, but national law may extend protection (e.g. Italian and French law) - Living persons named in 20th-21st century records - The Customer's own staff or members (where relevant)

---

4. Customer (Controller) Obligations

4.1 Lawful basis

The Customer warrants that it has a lawful basis under GDPR Art. 6 (and where applicable Art. 9) for the processing it instructs BIQE to perform.

4.2 Customer instructions

The Customer's documented instructions to BIQE are: - This DPA - The Main Agreement - The configuration choices made by the Customer through the BIQE portal or API (e.g. tier selection, retention overrides if any)

Any further written instructions must be agreed by both Parties; BIQE may charge a reasonable fee for instructions falling outside the scope of the Service.

4.3 Special categories

The Customer must inform BIQE in writing in advance if it intends to upload, at material scale, scans containing **special categories of Personal Data** under GDPR Art. 9 (religious or philosophical beliefs, ethnic origin, health data, sexual orientation, biometric data, etc.) so that BIQE can assess whether additional safeguards are required.

4.4 Notice to Data Subjects

The Customer is responsible for providing all required notices and obtaining all required consents from Data Subjects under GDPR Art. 13 and 14.

---

5. Processor (BIQE) Obligations

BIQE undertakes to:

5.1 Processing on documented instructions

Process Personal Data only on the Customer's documented instructions (§4.2), including with regard to international transfers, unless required to do otherwise by EU or Member State law to which BIQE is subject. Where such legal obligation applies, BIQE will inform the Customer of that legal requirement before processing, unless the law prohibits it on important grounds of public interest.

5.2 Confidentiality

Ensure that personnel authorised to process the Personal Data are bound by confidentiality obligations (contractual or statutory).

5.3 Security measures

Implement appropriate technical and organisational measures as set out in **Annex II** to ensure a level of security appropriate to the risk.

5.4 Sub-processors

Engage Sub-processors only in accordance with §7 below.

5.5 Assistance with Data Subject requests

Taking into account the nature of the Processing, BIQE will assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights under GDPR Chapter III.

For Personal Data contained in uploaded scans: due to the unstructured nature of scanned content, BIQE cannot search inside scans for individual mentions of Data Subjects. BIQE can: - Delete a specific Customer-job (and its result) on request, including from cloud storage - Provide a copy of all data BIQE holds about the Customer's account

The Customer remains responsible for identifying which scans contain a particular Data Subject's data.

5.6 Assistance with Controller obligations

Assist the Customer, taking into account the nature of the Processing and information available to BIQE, with: - GDPR Art. 32 — security of processing - GDPR Art. 33-34 — Personal Data Breach notification - GDPR Art. 35 — Data Protection Impact Assessments - GDPR Art. 36 — prior consultation with the supervisory authority

5.7 Personal Data Breach notification

Notify the Customer **without undue delay**, and in any event within **72 hours** of becoming aware of a Personal Data Breach affecting the Customer's data, providing at minimum: - Nature of the breach - Categories and approximate number of Data Subjects affected - Likely consequences - Measures taken or proposed to mitigate

Notification will be sent to the primary email address on the Customer's account. The Customer is responsible for keeping that address current.

5.8 Return or deletion at end of processing

Upon termination of the Main Agreement, at the choice of the Customer: - (a) Delete all Personal Data, except where Union or Member State law requires storage (e.g. Dutch fiscal retention of billing records under Art. 52 AWR — these do not contain scan content), or - (b) Return the Personal Data to the Customer in a structured, commonly-used, machine-readable format, then delete the data within 30 days

The default, absent instruction, is option (a).

5.9 Compliance demonstration and audits

Make available to the Customer all information necessary to demonstrate compliance with GDPR Art. 28 and allow for and contribute to **audits**, including inspections, conducted by the Customer or a mandated auditor, subject to:

- Reasonable advance written notice (at least 30 days unless a Personal Data Breach situation justifies shorter notice)
- A maximum of one audit per calendar year, save in case of demonstrated material concern or supervisory-authority requirement
- Reasonable scope and duration
- The Customer bearing its own costs and reasonable BIQE costs (€ 250 per hour, capped at the equivalent of 5 working days unless the audit reveals material non-compliance)
- Confidentiality obligations applying to all information disclosed

In lieu of a direct audit, BIQE will provide its **ISO 27001 certification** and corresponding audit report, which is generally accepted as adequate evidence of technical and organisational measures.

5.10 Notification of unlawful instructions

Inform the Customer immediately if, in BIQE's opinion, an instruction infringes GDPR or other applicable data-protection law.

---

6. Data Retention and Deletion

Data	Retention period
Uploaded scans (in cloud storage)	Automatically deleted **30 days** after upload
OCR/HTR results in customer portal	Available for 30 days, then automatically removed
Customer account data	Retained while account is active; deleted within 90 days after account closure (subject to legal retention)
Billing records (no scan content)	**7 years** (Dutch fiscal law — Art. 52 AWR)

The Customer may at any time request earlier deletion of specific Customer-jobs through the portal or by written request to `info@biqe.biz`.

---

7. Sub-processors

7.1 General authorisation

The Customer **hereby grants general authorisation** to BIQE to engage Sub-processors for the provision of the Service.

7.2 Current Sub-processors

The current list of Sub-processors at the date of this DPA is:

Sub-processor	Role	Location of processing
Google LLC / Google Ireland Ltd. (Google Cloud Platform)	Hosting (compute, storage)	United States (`us-east1`)
OpenRouter, Inc.	LLM-routing for the correction step in the HTR pipeline	United States, with onward routing to selected LLM providers
Stripe Payments Europe Ltd. (EU) / Stripe, Inc. (non-EU)	Payment processing, invoicing	Ireland (EU customers) / US (non-EU customers)
Drift.com, Inc. (Resend)	Transactional email delivery	United States

This list is also published in the BIQE Privacy Policy at `ocr-handwriting.online/legal/privacy` and is updated when changes occur.

7.3 Sub-processor obligations

BIQE warrants that it will: - Impose data-protection terms on each Sub-processor that are no less protective than those in this DPA - Remain fully liable to the Customer for the Sub-processor's compliance

7.4 Notification of changes

BIQE will give the Customer at least **30 days' notice** of any planned addition or replacement of a Sub-processor (by email to the account contact and by updating the Privacy Policy).

The Customer may **object** to a new Sub-processor on reasonable, documented data-protection grounds within 14 days of notification. If objection cannot be resolved, the Customer may terminate the Main Agreement for the part of the Service that cannot be provided without the new Sub-processor, with pro-rata refund of unused prepaid fees.

---

8. International Data Transfers

8.1 Transfers to third countries

The Customer acknowledges that Personal Data is transferred to and processed in the **United States** (Google Cloud Platform `us-east1` region; OpenRouter; Resend) and to other locations as listed in §7.2.

8.2 Transfer mechanisms

For transfers outside the European Economic Area (EEA), the Parties rely on:

- **EU-U.S. Data Privacy Framework** (DPF) — where the Sub-processor is certified
- **Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914), Module 2 (Controller to Processor) where applicable, or Module 3 (Processor to Sub-processor) for onward transfers — incorporated by reference

The Parties agree that Customer's signing of this DPA, combined with BIQE's signed SCCs with each US-based Sub-processor, satisfies the requirement of GDPR Art. 46 for these transfers.

8.3 Supplementary measures

BIQE has assessed the transfer in light of *Schrems II* (CJEU C-311/18) and applies the following supplementary measures: - All transfers in transit use TLS 1.2 or higher - Cloud storage is configured for encryption at rest (Google-managed keys) - Access by Sub-processor personnel is limited to operational necessity

8.4 EU-region option

BIQE is evaluating migration to a European GCP region (e.g. `europe-west4`). Customers with strict data-residency requirements should contact BIQE before signing this DPA to discuss feasibility, lead time, and any additional commercial terms.

---

9. Liability

The liability provisions of the Main Agreement (Section 11 — Limitation of Liability) apply to claims arising under this DPA, except as required otherwise by mandatory law.

For the avoidance of doubt: liability under the GDPR (Art. 82) cannot be contractually limited as between Data Subjects and a controller or processor, but the Parties' contractual liability *to each other* is governed by the Main Agreement.

---

10. Term and Termination

10.1 Term

This DPA enters into force on the date of acceptance by the Customer (whether by signature, by execution of an Order Form referencing this DPA, or by written acceptance) and remains in force for as long as BIQE processes Personal Data on behalf of the Customer.

10.2 Survival

The following provisions survive termination as long as BIQE retains any Personal Data of the Customer: §5.2 (confidentiality), §5.7 (breach notification for residual data), §5.8 (return or deletion), §5.9 (compliance demonstration).

10.3 Termination of Main Agreement

Termination of the Main Agreement automatically terminates this DPA, without prejudice to surviving obligations under §10.2 above.

---

11. Miscellaneous

11.1 Conflicts

In the event of conflict between this DPA and the Main Agreement on matters of personal-data processing, this DPA prevails. On all other matters, the Main Agreement prevails.

11.2 Updates

BIQE may update this DPA from time to time to reflect changes in law, the Service, or Sub-processors. Material updates will be notified to the Customer with at least 30 days' notice.

11.3 Governing law

This DPA is governed by Dutch law. Disputes are subject to the exclusive jurisdiction of the courts of the district of Overijssel, the Netherlands, in line with the Main Agreement.

11.4 Counterparts and electronic signature

This DPA may be signed in counterparts, including electronically. Acceptance through signature (physical or electronic) or by execution of an Order Form referencing this DPA constitutes binding acceptance.

Annex I — Description of Processing

Item	Description
Categories of Data Subjects	Persons whose data appears in scans uploaded by the Customer (see §3.2)
Categories of Personal Data	As described in §3.1; depends on Customer's source material
Special categories of data	Possible (depending on source material); see §4.3
Frequency of transfer	Continuous, on demand whenever the Customer submits a job
Nature of processing	OCR/HTR processing (see §2.2)
Purpose of processing	Provision of the Service (see §2.3)
Retention period	See §6
Sub-processors	See §7.2

Annex II — Technical and Organisational Security Measures

BIQE implements the following measures, in line with GDPR Art. 32 and ISO 27001:

Organisational measures

- ISO 27001 certified (DigiTrust certificate available on request)
- Personnel bound by confidentiality
- Access on a need-to-know basis
- Documented incident response procedures
- Regular review of security measures

Technical measures — confidentiality

- HTTPS (TLS 1.2+) for all customer-facing connections
- Encryption at rest for cloud storage (Google-managed keys)
- Bcrypt hashing for user passwords (no plaintext storage)
- TOTP two-factor authentication available, with Fernet-encrypted secrets at rest
- API keys generated using cryptographically secure random functions
- SSH key-only access to production servers (no password logins)

Technical measures — integrity

- Append-only audit log of authentication and authorisation events
- Database integrity checks (`PRAGMA integrity_check`) and foreign-key constraints
- Atomic write patterns for code deployments with read-back verification
- Schema migrations tracked in `schema_migrations` table

Technical measures — availability

- Daily automated cleanup processes (audit-log retention, scan-file lifecycle)
- Service health monitored via systemd unit status
- Best-effort recovery from sub-processor outages (no SLA guarantee — see Main Agreement §8)

Technical measures — resilience

- Database backups before every schema migration
- Code-deploy patches use idempotency markers and pre-write validation
- Rollback procedures documented for each deploy

Pseudonymisation and minimisation

- Authentication logs use hashed identifiers where possible
- Audit-log entries to deleted users have their actor reference set to NULL (per FK ON DELETE SET NULL)
- Customer-portal access scoped per organisation; no cross-organisation visibility

Sub-processor management

- Sub-processors selected on the basis of security posture, ISO/SOC certifications, GDPR-compliance commitments
- Written agreements with each Sub-processor; SCCs where applicable
- Sub-processor list reviewed at least annually

Signature Block

For BIQE V.O.F.:

Name: _____ Title: _____ Date: _____ Signature: _____

For Customer:

Customer (legal entity name): _____ Name of signatory: _____ Title: _____ Date: _____ Signature: _____

End of Data Processing Agreement — BIQE V.O.F. — Version 1.0 — 3 May 2026.