BJM

DENTAL LABORATORY

DATA PROCESSING AGREEMENT

UK GDPR| Dental practice client agreement

DOCUMENT STATUS	DETAIL
Prepared	1 November 2026
Parties	BJM Dental Laboratory Ltd and the named dental practice
Applicable law	England and Wales; applicable UK data protection legislation

Important: This document is a complete working draft, not a certification of compliance. Complete the practice details, verify service providers and security arrangements, agree retention instructions and obtain appropriate legal review before signing.

Agreement particulars

This Data Processing Agreement (the **Agreement**) is entered into on **[Date]** between the following parties:

DATA CONTROLLER - DENTAL PRACTICE	DATA PROCESSOR - LABORATORY
Legal name: [Insert full legal name] Address: [Insert full address] Contact: [Insert name / role] Email: [Insert email]	BJM Dental Laboratory Ltd Address: [Insert registered / principal address] Contact: Ben Mason, Director Email: bjmdentallab@yahoo.com [verify before signing]

The parties agree as follows. Schedules 1-5 form part of this Agreement.

1. Purpose and scope

1.1 This Agreement governs BJM Dental Laboratory Ltd (BJM) processing personal data on behalf of the Data Controller for the manufacture, repair, modification and supply of custom-made dental appliances and associated laboratory services.

1.2 This Agreement is intended to satisfy Article 28 of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended, and other applicable UK data protection requirements.

1.3 The subject matter, duration, nature and purposes of processing, types of personal data and categories of data subjects are described in Schedules 1 and 2.

1.4 This Agreement supplements the underlying laboratory services relationship. Where terms conflict regarding processing of personal data, this Agreement prevails to the extent required by applicable law.

2. Roles and responsibilities

2.1 The dental practice acts as Data Controller for patient information submitted to BJM. BJM acts as Data Processor when handling that information on the practice's behalf.

2.2 The Controller is responsible for establishing lawful bases and relevant special-category conditions, providing required privacy information, and ensuring submitted data is relevant, accurate and necessary.

2.3 BJM may separately act as an independent controller for its own staff, supplier, accounting and business administration records; those activities are outside the processor relationship under this Agreement.

3. Documented instructions

3.1 BJM shall process personal data only on documented instructions of the Controller, including regarding international transfers, unless processing is required by applicable UK law.

3.2 A submitted laboratory prescription or digital case is a documented instruction to carry out the processing reasonably necessary to fulfil that case, subject to this Agreement and further written instructions.

3.3 BJM shall not use identifiable patient information for unrelated marketing, publication, independent research or other unauthorised purposes.

3.4 Where law requires processing outside the Controller's instructions, BJM shall inform the Controller before processing unless the law prohibits notice on important public interest grounds.

3.5 BJM shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection legislation.

4. Confidentiality

4.1 BJM shall ensure persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Access to prescriptions, clinical images, digital scans and correspondence shall be restricted to personnel who need that information for their duties.

4.3 BJM shall provide appropriate confidentiality and data-handling instruction. Confidentiality obligations continue following termination of access or employment.

5. Security of processing

5.1 BJM shall implement appropriate technical and organisational measures required by Article 32 UK GDPR, taking account of the risks, state of the art, implementation costs and the nature, scope, context and purposes of processing.

5.2 Measures shall address, where appropriate, confidentiality, integrity, availability, resilience, restoration of access after incidents and regular testing or evaluation.

5.3 The reported current arrangements and controls requiring verification are listed separately in Schedule 3. Listing a proposed control does not represent that it has already been implemented.

5.4 BJM currently operates a shared laboratory email account using one password. BJM shall assess the access and accountability risks and introduce proportionate safeguards, including multi-factor authentication and individual access where feasible.

6. Sub-processors

6.1 BJM shall not engage a sub-processor for the Controller's personal data without prior specific or general written authorisation from the Controller.

6.2 Where general written authorisation is granted, BJM shall notify the Controller of intended additions or replacements and allow a reasonable opportunity to object before the change takes effect.

6.3 BJM shall impose appropriate written data protection obligations on authorised sub-processors, providing protections equivalent to those required of BJM by Article 28 UK GDPR.

6.4 BJM remains responsible to the Controller for the performance of authorised sub-processors' data protection obligations.

6.5 Schedule 4 records relevant service providers and the authorisation basis. It must be completed before signing.

7. International transfers

7.1 BJM shall not make restricted transfers of the Controller's personal data outside the UK without documented authorisation and compliance with applicable UK international transfer rules.

7.2 Where required, BJM shall ensure an appropriate transfer mechanism, such as adequacy regulations or approved contractual safeguards, and any required transfer risk assessment.

7.3 Cloud storage, email hosting, scanning platforms and remote support services shall be checked for storage or access outside the UK.

8. Data subject rights

8.1 Taking account of the nature of the processing, BJM shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in responding to requests to exercise data protection rights.

8.2 BJM shall forward requests concerning the Controller's patient information without undue delay and shall not independently disclose, amend or erase those records except on documented instruction or as required by law.

8.3 The Controller remains responsible for determining and responding to applicable rights requests.

9. Personal data breaches

9.1 BJM shall notify the Controller without undue delay after becoming aware of a personal data breach affecting personal data processed on the Controller's behalf.

9.2 As an operational target, BJM shall aim to give initial notice within 24 hours of awareness, even if investigation is incomplete. This target does not replace the legal duty to notify without undue delay.

9.3 As available, notification shall describe the incident, affected records and individuals, known or likely consequences, containment and remediation steps, and a contact for follow-up.

9.4 BJM shall provide additional relevant information as it becomes available and cooperate with the Controller. The Controller is responsible for assessing its own ICO and individual notification obligations.

10. Assistance to the Controller

10.1 Taking account of the nature of processing and information available, BJM shall reasonably assist the Controller with security obligations, breach response, data protection impact assessments and prior consultation with the ICO where required.

10.2 The parties shall cooperate reasonably on data protection issues arising from laboratory services.

11. Retention, return and deletion

11.1 BJM proposes a standard retention period of **10 years from the completion of each individual laboratory case** for laboratory prescriptions and associated digital case records.

11.2 This period applies to the Controller's patient data only where agreed as a documented instruction and consistent with applicable legal obligations; Schedule 5 records that instruction.

11.3 Records shall not be kept beyond the applicable period unless continued retention is required by law or otherwise lawfully authorised.

11.4 Paper records are confidentially shredded in-house. Electronic records shall be securely deleted when required, including through documented backup deletion or expiry procedures.

11.5 At the end of the provision of services, BJM shall, at the Controller's choice, delete or return all personal data processed on its behalf and delete existing copies, unless applicable UK law requires storage.

11.6 Where law requires continued storage, BJM shall protect the information and restrict further processing to lawful purposes. Reasonable confirmation of deletion or return shall be provided upon request.

12. Information, audits and inspections

12.1 BJM shall make available to the Controller all information necessary to demonstrate compliance with Article 28 obligations and allow for and contribute to audits and inspections by the Controller or its mandated auditor.

12.2 Audits shall be conducted with reasonable arrangements to preserve the confidentiality and security of other clients' information; such arrangements shall not prevent fulfilment of statutory audit rights.

12.3 BJM shall address substantiated compliance deficiencies within an appropriate timescale.

13. Accuracy and minimisation

13.1 The Controller shall provide only personal data reasonably necessary for the case. BJM shall take reasonable steps to protect against unauthorised alteration and notify the Controller of material inaccuracies identified.

13.2 Corrections to patient information shall be undertaken in accordance with documented Controller instructions.

14. Duration, termination and review

14.1 This Agreement takes effect on signature and remains in force for as long as BJM processes personal data on behalf of the Controller.

14.2 Termination of laboratory services is governed by the underlying commercial terms. The return and deletion obligations in clause 11 apply on conclusion of processing.

14.3 Confidentiality, security and lawful retention obligations survive termination where applicable. The parties shall review this Agreement following material legal, technical or operational changes.

15. Liability and governing law

15.1 Each party remains responsible for its own obligations under applicable data protection legislation. Nothing in this Agreement excludes liability where exclusion is prohibited by law.

15.2 This Agreement is governed by the laws of England and Wales, subject to mandatory applicable data protection law.

16. Contacts and notices

16.1 Each party shall designate a contact for data protection matters and communicate changes without undue delay.

16.2 Urgent security and breach notifications shall be communicated promptly through the nominated contact channels.

Schedule 1 - Description of processing

Subject matter: Provision of dental laboratory services for the Controller.

Nature and purpose: Receipt, examination, recording, storage and use of prescriptions, clinical information, digital scans and photographs to design, manufacture, repair, modify and supply dental appliances.

Typical processing: Receipt of conventional or digital submissions; communication with practices; case planning and production; collection and delivery coordination; handling queries, remakes and traceability.

Duration: During the services and any applicable lawful, agreed retention period.

Controller rights: To give documented instructions, request assistance and compliance information, audit arrangements, and direct return or deletion at the end of services.

Controller obligations: Lawful collection and disclosure, transparency to patients, data minimisation, accurate submissions and appropriate instructions.

Schedule 2 - Data subjects and categories

Data subjects: Patients of the dental practice, including adults and children, and relevant clinical personnel named in case information.

Types of personal data: Patient names, identifiers and dates of birth; prescriptions; clinical instructions; dental and relevant medical information; intraoral scans and digital impressions; clinical photographs; tooth shades and designs; case histories; and relevant communications.

Special-category data: Health information, including identifiable dental clinical records and treatment-related images.

Volume: Variable, depending on cases submitted. No fixed annual patient volume is assumed.

Schedule 3 - Security measures

A. Current arrangements reported by BJM

- Password-protected laboratory computers; digital case files stored on laboratory computers.
- External hard drive backups; no cloud backup service reported.
- Shared laboratory email address accessed using one password.
- Physical prescriptions retained; confidential paper shredding performed in-house.
- Xero used for accounting and invoicing (patient-data scope to be confirmed).

B. Controls requiring confirmation or implementation

- Documented authorised access, confidentiality obligations and staff awareness.
- Multi-factor authentication and improved accountability for shared mailbox access.
- Operating system updates, anti-malware measures and secure network configuration.
- Encryption and physical protection of relevant computers and external drives.
- Email and scan platform hosting locations, access permissions and contractual terms.
- Backup recovery testing and defined deletion / backup expiry process.

- Secure paper record storage, breach response procedure and periodic security reviews.

Important: Section B is an action list, not a statement of existing compliance.

Schedule 4 - Sub-processor register and authorisation

Complete this schedule before signature. Include each provider that processes patient information on BJM's behalf, the relevant contractual arrangements, hosting/access location and any transfer safeguards. Do not treat a provider as an authorised sub-processor until the Controller has given the required written authorisation.

Service / provider	Processing purpose	Status / checks
Yahoo - email	Case correspondence and prescriptions	Access/location: confirm
iTero - scans	Digital scan transfer / storage	Access/location: confirm
Capital Industrial Ltd	IT support; patient-data access uncertain	Access/location: confirm
External hard drives	Local backup - BJM-controlled	Not a third-party provider
Cloud backup	Not applicable - none reported	Not a sub-processor
Xero - accounting	Accounting; patient-data scope to confirm	If applicable: confirm

Authorisation method: [ ] Specific written authorisation for the providers above [ ] General written authorisation subject to notice and right to object.

Controller special conditions or objections:

_____

Schedule 5 - Agreed retention instruction

The Data Controller selects one option:

[ ] **Standard:** Authorise BJM to retain laboratory prescriptions and associated digital case records for 10 years from the completion date of each individual case, subject to applicable law and the termination/deletion provisions of this Agreement.

[ ] **Alternative:** Apply the following documented lawful retention instruction:

_____

_____

The parties acknowledge that legal obligations may require certain records to be kept, and that retention instructions should be reviewed if circumstances or applicable law change.

Execution - signatures

By signing, each party confirms its agreement to these terms and the completed schedules.

FOR THE DATA CONTROLLER	FOR BJM DENTAL LABORATORY LTD
Practice / legal entity: _____	Name: Ben Mason Position: Director

FOR THE DATA CONTROLLER	FOR BJM DENTAL LABORATORY LTD
Name / position: _____	Signature: _____
Signature: _____	Date: _____
Date: _____	

Pre-signature completion checklist

This checklist is part of the review pack, not a representation that the items are complete.

[ ] Insert the full legal names, addresses, contacts and execution date for both parties.

[ ] Confirm BJM's registered/principal address and the contact email shown in the agreement.

[ ]Confirm Yahoo, iTero and Capital Industrial Ltd patient-data scope; secure required

a

[ ] Confirm data locations, international access and any necessary UK transfer safeguards.

[ ] Verify implemented security controls; resolve or formally assess the shared-password risk and document backup deletion.

[ ] Confirm with the practice the 10-year case retention instruction or agree a lawful alternative in Schedule 5.

[ ] Review the contract against any applicable medical-device recordkeeping obligations and the practices' own requirements.

[ ] Have the completed agreement reviewed by a suitably qualified UK legal/data protection adviser before issue and signature.

Document control

Document owner	BJM Dental Laboratory Ltd
Prepared	1 November 2026
Approval / effective date	[To be completed following review]
Next review	[To be set on approval]