LEGAL & COMPLIANCE

Privacy & Data Protection Policy

Version 1.0 Effective Date May 2026 Next Review May 2027

Owner Data Protection Officer

Registered with the Information Commissioner's Office — Registration No. ZB384076

CONTENTS

SECTION 01

Who We Are

Business and Service Solutions Limited (trading as BA2S Ltd) is a company registered in England and Wales (Company No. 7197748), with its registered office at First Floor, 6 Nelson Street, Southend-on-Sea, SS1 1EF.

We provide teleradiology and specialised reporting services, digital pathology services, healthcare transformation consultancy, and staffing services to NHS organisations and other healthcare providers across the United Kingdom.

For the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, Business and Service Solutions Limited is the Data Controller in respect of personal data we collect and process about our clients, website visitors, job applicants, and staff. In the context of teleradiology services delivered on behalf of NHS Trusts and other healthcare providers, we act as a Data Processor, processing patient data solely under the documented instructions of the relevant Data Controller.

Data Protection Officer: Our DPO is responsible for overseeing compliance with this policy and applicable data protection law.

Contact: sol@ba2sltd.com

ICO Registration: ZB384076

SECTION 02

Data We Collect

Client and Partner Data

When engaging with us as a client, commissioner, or business partner, we may collect and process the following categories of personal data:

- Name, job title, and professional contact details
- Email address, telephone number, and postal address
- Communication and correspondence records
- Contractual and financial information relevant to the delivery of services

Patient Data (Teleradiology and Clinical Services)

In providing teleradiology reporting and related clinical services on behalf of NHS Trusts and other healthcare providers, we process special category personal data relating to patients, including:

- Patient name, date of birth, NHS number, and relevant demographic identifiers

- Medical imaging data including X-ray, CT, MRI, and other diagnostic images
- Clinical history and referral information
- Radiological reports and diagnostic findings

Patient data is processed solely in our capacity as a Data Processor, under the lawful instructions of the referring NHS organisation or healthcare provider acting as Data Controller.

Website Visitors

When you visit our website at www.ba2sltd.com, we may collect standard technical data including your IP address, browser type, pages visited, and time of access, for the purposes of website security and performance monitoring. We do not use this data for marketing profiling.

SECTION 03

Lawful Basis for Processing

Processing Activity	Lawful Basis	Special Category Basis (where applicable)
Teleradiology reporting for NHS patients	Article 6(1)(e) — Public task	Article 9(2)(h) — Health care provision
Client and contract management	Article 6(1)(b) — Contract performance	N/A
Legal and regulatory compliance	Article 6(1)(c) — Legal obligation	N/A
Legitimate business operations	Article 6(1)(f) — Legitimate interests	N/A
Secondary or research use of data	Article 6(1)(a) — Consent	Article 9(2)(a) — Explicit consent

SECTION 04

How We Use Your Data

We use personal data only for the purposes for which it was collected or as otherwise permitted by applicable law. Specifically, we use data to:

- Deliver teleradiology reporting and diagnostic services to NHS organisations and healthcare providers
- Manage contractual relationships with clients, partners, and subcontractors
- Comply with legal, regulatory, and NHS governance obligations
- Maintain clinical audit trails and quality assurance records
- Respond to subject access requests and exercise of data subject rights
- Manage complaints, incidents, and service improvement activities
- Communicate with clients and stakeholders regarding service delivery

We will never sell personal data to third parties, nor use it for unsolicited marketing without explicit consent.

SECTION 05

Data Retention

We retain personal data only for as long as is necessary for the purpose for which it was collected, and in accordance with applicable legal and NHS records management requirements.

Data Category	Retention Period
Patient data processed under clinical contracts	Duration of contract plus 7 years, or as directed by the Data Controller
Client and partner contact records	Duration of relationship plus 6 years
Consent records	Duration of contract plus 7 years

Data Category	Retention Period
Security testing and audit logs	Minimum 3 years
Correspondence and complaints records	6 years from resolution

Records are stored and managed in line with the NHS Records Management Code of Practice for Health and Social Care. On expiry or termination of any clinical contract, all patient records held by us will be returned to the relevant Data Controller at no cost.

SECTION 06

Your Rights

Under UK GDPR, individuals whose personal data we process as a Data Controller have the following rights. Where we act as a Data Processor on behalf of an NHS organisation, requests relating to patient data should be directed to the relevant NHS organisation as Data Controller.

RIGHT TO BE INFORMED

To receive clear information about how your data is used, as set out in this policy.

RIGHT OF ACCESS

To request a copy of the personal data we hold about you within one month of your request.

RIGHT TO RECTIFICATION

To request correction of inaccurate or incomplete personal data without undue delay.

RIGHT TO ERASURE

To request deletion of your data where there is no compelling reason for continued processing.

RIGHT TO RESTRICTION

To request that we limit processing of your data in certain circumstances.

RIGHT TO PORTABILITY

To receive your data in a structured, commonly used, machine-readable format.

RIGHT TO OBJECT

To object to processing based on legitimate interests or for direct marketing purposes.

RIGHTS RE: AUTOMATED DECISIONS

Not to be subject to solely automated decisions that produce significant legal effects.

To exercise any of the above rights, please contact our Data Protection Officer at sol@ba2sltd.com. We will respond within one calendar month of receiving your request.

SECTION 07

Technical & Organisational Security Measures

Business and Service Solutions Limited implements and maintains robust technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or alteration. Our measures include:

Data Encryption

All patient data in transit is protected using AES-256 encrypted VPN connections conforming to NHS Digital connectivity standards. Data at rest is encrypted using AES-256 across all storage environments.

Access Controls

Access to personal data is controlled through role-based access controls (RBAC), with multi-factor authentication (MFA) enforced for all remote access. Access events are logged to an immutable audit trail and reviewed monthly by our Information Governance lead.

Infrastructure Resilience

Our reporting infrastructure operates with a Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour. Business continuity and

disaster recovery plans are tested bi-annually with documented outcomes retained for audit.

Security Testing

We conduct quarterly vulnerability scanning of all systems processing personal data. Annual penetration testing is carried out by Cyber Academy Ltd, a CREST-approved provider, with findings tracked to remediation within agreed timescales.

Information Security Standards

Business and Service Solutions Limited holds ISO 9001 certification and operates in line with ISO 27001 information security controls, with formal ISO 27001 certification actively being pursued.

NHS Data Security and Protection Toolkit

We are completing our submission to the NHS Data Security and Protection (DSP) Toolkit as an NHS Business Partner, with a scope specifically covering the provision of Teleradiology services. Evidence of submission is available to NHS organisations on request prior to contract commencement.

Staff Training

All staff with access to personal data complete mandatory information governance and data protection training on induction and annually thereafter. Data protection policies are reviewed bi-annually and updated to reflect any change in regulatory requirements or operational practice.

SECTION 08

International Data Transfers

Business and Service Solutions Limited processes all patient personally identifiable data (PID) entirely within the United Kingdom. No element of our supply chain, including radiologist reporting partners and technology providers, involves the transfer of patient PID outside the UK.

This position is contractually confirmed with all subcontractors and partners. Any future change to this arrangement would require prior Information Governance review and written agreement with the relevant Data Controller or Beneficiary before any transfer takes place, and would be governed by the appropriate legal safeguard under UK GDPR Chapter V.

SECTION 09

Consent & Withdrawal

The primary lawful basis for processing patient data in the context of teleradiology reporting is Article 6(1)(e) (public task) and Article 9(2)(h) (health care provision). Patient consent is not therefore the primary mechanism for routine clinical processing.

Where we do rely on consent as a lawful basis, for example in relation to secondary or research use of data, consent is obtained through the referring Trust's patient consent pathway at the point of referral. Consent is recorded with a timestamp, the version of the consent form presented, and the identity of the individual providing consent.

Withdrawing consent: Where processing is based on consent, individuals have the right to withdraw that consent at any time. On receipt of a withdrawal request, we will cease the relevant processing within 48 hours. Withdrawal of consent does not affect the lawfulness of any processing carried out prior to withdrawal. To withdraw consent, please contact us at sol@ba2sltd.com.

SECTION 10

Complaints

If you have a concern about how we handle your personal data, we ask that you contact our Data Protection Officer in the first instance at sol@ba2sltd.com. We

will acknowledge your concern within five working days and aim to resolve it within one calendar month.

If you are not satisfied with our response, or if you believe we are processing your personal data in a manner that is not compliant with applicable data protection law, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office

Website: ico.org.uk

Helpline: 0303 123 1113

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

SECTION 11

Policy Review

This policy is reviewed annually by our Data Protection Officer, or sooner in the event of a material change to our processing activities, applicable legislation, or regulatory guidance. The current version and effective date are shown at the top of this page.

We will notify relevant clients and partners of any material changes to this policy through our standard communications channels.

SECTION 12

Contact Us

Data Protection Officer

For all data protection enquiries, subject access requests, consent withdrawals, or complaints, please contact our Data Protection Officer directly.

Email: sol@ba2sltd.com

Post: Data Protection Officer, Business and Service Solutions Limited, First Floor, 6 Nelson Street, Southend-on-Sea, SS1 1EF

ICO Registration: ZB384076