



DATA PROTECTION POLICY: bstardigital Ltd

Company Number: 16560818

1. OVERVIEW This Policy contains the data protection policy of **bstardigital Ltd** (the Company). It establishes our commitment to **Digital Sovereignty**, ensuring that while we provide the infrastructure (the bstarOne engine), users and staff maintain the highest standards of data integrity and privacy.

2. AMENDMENTS The Company reserves the right to amend, replace, or remove the contents of this policy from time to time, in its absolute discretion. Any amendments or revisions will be notified to staff by email and subsequently incorporated into future editions.

3. COMPLIANCE REQUIREMENT Staff members are required to familiarise themselves with the contents of this policy and comply with it at all times.

4. LEGAL FRAMEWORK The Company is committed to complying with its data protection obligations under the Data Protection Act 2018 (the DPA 2018), the UK General Data Protection Regulation (the UK GDPR), and the **bstarOne AI Ethics Framework**.

5. FRAMEWORK FOR USE This policy provides a framework for the appropriate use of personal data (i.e., any information which relates to an identifiable individual).

6. SCOPE OF POLICY All staff members (including employees, casual workers, officers, and agency workers) must comply with this policy. Any breach of this policy will be taken extremely seriously and may lead to disciplinary action up to and including dismissal.

7. RESPONSIBILITY FOR COMPLIANCE **Alex Hahn** is the person responsible for the Company's data protection compliance. If any staff member has any concerns regarding this policy, they should raise these with Alex Hahn.

8. TRAINING & INDUCTION The Company will provide training to all staff about data protection and the specific **Zero-Training AI protocols** on induction. Staff dealing with "Brand DNA" or high-level client infrastructure will undergo additional specialized training.

9. DATA PROTECTION PRINCIPLES To comply with Data Protection Law, all staff must act in accordance with the following principles:

- **A. Lawfulness & Transparency:** Process data lawfully, fairly, and in a transparent way.
- **B. Purpose Limitation:** Collect data for specified, explicit, and legitimate purposes.
- **C. Data Minimisation:** Ensure data is adequate, relevant, and limited to what is necessary.
- **D. Accuracy:** Keep data accurate and up to date; erase or correct inaccuracies promptly.
- **E. Storage Limitation:** Do not keep data in an identifiable form for longer than necessary.
- **F. Integrity & Confidentiality:** Process data securely to protect against unauthorized or unlawful processing, loss, or damage.

10. STAFF RESPONSIBILITIES & AI PROTOCOLS Staff with access to personal data:

- Must adhere to the principles listed in Section 9.
- Must ensure that interaction logs involving **Alex (the AI assistant)** are handled via the Company's isolated infrastructure.
- Must not use personal data to train external or public AI models (Strict Zero-Training Protocol).
- Must not access personal data without proper authorization.
- Must report any loss of data or personal data breach to Alex Hahn immediately.

11. SENSITIVE PERSONAL DATA The Company may process sensitive personal data (e.g., racial/ethnic origin, health data, biometric data). According to UK statistics from the ICO and ONS, sensitive data handling remains the highest-risk area for data breaches, occurring in approximately 22% of reported incidents. Consequently, such data must only be processed with explicit consent. Staff must notify Alex Hahn before processing any sensitive data to determine if a Data Protection Impact Assessment (DPIA) is required.

12. DATA SUBJECT RIGHTS We facilitate the following rights for all data subjects (Clients, Staff, and Partners):

- **a) Right of Access:** Subject Access Requests (SAR) for copies of held data.
- **b) Right to Portability:** Requesting data transfer to another company or private server.
- **c) Right to Rectification:** Correcting inaccurate data.
- **d) Right to Erasure:** The "Right to be Forgotten."
- **e) Right to Sovereignty:** Ensuring custom AI configurations and Brand DNA remain the property of the data subject.

13. PERSONAL DATA BREACHES Staff must immediately report actual or suspected breaches. The Company is required to notify the **Information Commissioner's Office (ICO)** about serious breaches within **72 hours** of discovery.

14. DATA PROTECTION IMPACT ASSESSMENTS (DPIA) A DPIA is mandatory for high-risk processing, such as introducing new AI logic, sharing data with Vanguard partners, or implementing new automated tracking tools (**bstarAna**).

Signed: *Alex Hahn* CEO, **bstardigital Ltd**

Signed:

Alex Hahn

CEO

12 Jan 2026



