BRIGHTMINDED

DATA PROTECTION POLICY

Last updated: 19 March 2025

- C O N F I D E N T I A L -

1. Introduction

BrightMinded Ltd (“BrightMinded”, “we” or “us”), company number 07573613, is a private company registered in England and Wales. BrightMinded is registered with the Information Commissioner’s Office, registration number ZA027827.

BrightMinded is a UK-based bespoke software development company focusing on the development of custom web-based and mobile solutions for commercial applications. BrightMinded establishes long-term relationships, providing support, maintenance, hosting and new feature provision.

Please also refer to the **BrightMinded Privacy Policy** for details of personal data collection, use, security, retention, and data rights.

This Data Protection Policy and the BrightMinded Privacy Policy form an integral part of the **BrightMinded Information Security Policy**.

1. Data Protection Officer

BrightMinded has not appointed a Data Protection Officer (DPO), as permitted under the General Data Protection Regulation for companies whose scale makes it impossible for this person to be independent
or non-conflicted.

The three BrightMinded executive directors are responsible for maintaining an up to date risk assessment of the business. These are John Mooren, Dan Murray, and Cristiano Solarino. One of these will be assigned as project leader to you and will manage data protection aspects of our work with you.

2. Data Controller vs Data Processor

BrightMinded’s data protection policies are designed to protect customer personal data used to manage our relationship. For further information see our Privacy Policy, ‘What we do with your data’.

Where BrightMinded acts as a data processor or sub-processor, as defined by the GDPR, our data protection policies are designed to protect your and your customers’ personal data when it is accessible by BrightMinded employees or temporarily stored on our computers for testing or debug purposes.

Where BrightMinded acts as a data processor or sub-processor, the data controller has the right to request us to delete or amend some or all of the data controller’s data, with the exception of any copies kept for legal or financial reporting requirements.

3. Data protection

Our data protection policy was designed following the risk assessment work detailed in the Appendix.

3.1. Physical access to BrightMinded office

Access to the building housing the BrightMinded office is protected by a staffed reception desk during office hours and keycode door entry outside office hours. Access to the floor of the BrightMinded office is via two doors, which both are protected with a digital key lock. Access to the BrightMinded office is via a door with a physical lock. Unsupervised access is restricted to:

- BrightMinded staff
- Platform 9 maintenance and cleaning team

3.2. Personal computer security measures

Employee's computers are protected by strong passwords and are automatically logged out after an inactivity timeout. All hard drives are encrypted at the disk partition level. Hardware is owned by BrightMinded. Personal hardware is not permitted to access the BrightMinded information systems with the exception of personal mobile phones of BrightMinded staff and authorised individuals accessing cloud-based services like Gmail, Trello and Slack, although downloading of files containing client data is not permitted on any personal hardware.

Working data is backed up or managed using a number of different and specialized systems including:

- BitBucket for all code items
- Google drive and G Suite for customer data, working documents, proposals, accounting information
- Web based services such as Clockify, Trello, BaseCamp, Slack and Skype for planning and client communications
- Web based services such as Xero and AFH Payroll for accounting and payroll services
- AWS cloud servers for live customer data where we are responsible for hosting
- Digital Ocean Automated Backups for backing client volumes

3.3. Email marketing

Any personal data used for email marketing has/will have consent obtained in advance and include unsubscribe instructions.

3.4. Staff contracts

BrightMinded employment contracts summarize employees' responsibilities under our Privacy Policy and data protection regulations.

Employees must return computer equipment on ceasing employment

3.5. Regular staff training

All staff whose work may involve processing personal data will receive regular training on their responsibilities under our Privacy Policy.

Training will be provided to all new employees as part of their induction.

Training will be provided to any existing employees who have not yet received it.

All employees will receive a training refresher at least every twelve months or following a change in applicable law, regulation or BrightMinded policy.

BrightMinded will keep a record of the training that has been undertaken by each employee.

3.6. Access control to client data

Where we are responsible for hosting a live and staging environment with client data, access is restricted by SSH Public-Private key encryption on an employee by employee basis. Each cloud server is further protected using OS level permissions, only the directors and the system administrator have root access to any machine. Access to staging machines is further restricted to the office network.

Client admin portals or other sources of data shared with clients are accessed through a shared collection of usernames and strong passwords. These username / password combinations are stored in a shared encrypted vault provided by 1Password.

Access to these various systems is reviewed as required by the Information Security Committee.

4. Data Retention

Our customers', partners', potential and ex-customer contact data

The length of time we keep your personal data depends on whether we have an ongoing business relationship and need to retain it. We will retain your personal data for a period of time after a business relationship ends where we have an ongoing business need to retain it, and for practical purposes of maintaining contact. An example would be our many customers who use us for project work from time to time. You can request this data be deleted, or can request to see what data we hold about you.

Software we write for our customers

BrightMinded retain copies of code we have written for our customers, but this code will not include personal data. All code is stored securely off-site in BitBucket repositories, and may also exist in development, staging or production environments, depending on the stage each customer project is at.

Customer platform data

Customer platform personal data will be stored as required by the customer, who is in this case defined as the Data Controller under the GDPR. Our experience is that this is usually with a cloud provider, or on customer's own servers.

From time to time BrightMinded may download customer databases to its own computers for testing or debugging purposes. In these cases, access to data will be limited to required employees as described above, and the data will be destroyed once testing is complete. Where appropriate all personal data will be pseudonymized, so long as this does not prevent testing or diagnosis. Customers can stipulate alternative arrangements for testing and debugging if required.

Disposal and destruction

All sensitive or personal data will be destroyed at the end of its operational use or any required retention period.

5. Disaster recovery

Please see the BrightMinded Business Continuity Plan.

6. Designing security from the ground up

The security of the platform we build and host for you is defined by you as Data Controller. We will share our expertise on security matters and build the platform according to your requirements. Examples include user access and authentication, data encryption, network protection, secure data centres, disaster recovery, security monitoring, and training your own staff to avoid phishing attacks. This is in additional to best-practice platform availability, updates and innovation, and ability to scale.

We will also provide a list of sub-processors that we use to support your platform, such as cloud service, email or other messaging providers.

All of this information can be used to prepare your own privacy policy and data protection policy.

APPENDIX - Risk assessment and mitigation

We have assessed data privacy and protection risks according to the following principles:

- Process personal data fairly and lawfully
- Loss / accidental erasure of data
- Personal information accidentally leaked or stolen from BrightMinded
- Storage of excessive or irrelevant data
- Disclosure of personal data to inappropriate people
- Data is inaccurate, insufficient, out of date or kept for too long

Principle	**BrightMinded Risk**	**Mitigation**
Process personal data fairly and lawfully	Retention of personal data without consent.	BrightMinded email template and any marketing emails come with data deletion instructions. Note that retention of contact information internally is not contradictory to GDPR, it is the use of this data that can contravene GDPR.
	Send marketing emails without consent	Consent email sent to all marketing contacts ahead of or

		with first marketing email. All marketing emails use service such as MailChimp which automatically include unsubscribe instructions.

Loss / accidental erasure of data	Accidental deletion of customer data while acting as Data Processor	Appropriate backup and recovery regime discussed with each customer, for whom BrightMinded store customer data, and implemented.
Personal information accidentally leaked or stolen from BrightMinded	BrightMinded laptop stolen	All BrightMinded laptops have encrypted hard drives.
	Customer data stored on a personal unencrypted device	BrightMinded staff prohibited from using personal devices to store customer data.
	Data accessed inappropriately via BrightMinded hardware or insecure storage of access passwords	Hard drive encryption prevents access without passwords, and passwords are stored securely in 1Password vault.
Storage of excessive or irrelevant data		Acting as Data Controller, we store limited personal data required to maintain contact with customers, partners and others. Acting as Data Processor, BrightMinded will only store pseudonymised customer data on its own encrypted drives or secure servers temporarily for testing or debugging purposes. The cloud-storage of platform data will be determined by the customer (Data Controller).
Disclosure of personal data to inappropriate people	Accidental disclosure though office visits.	Staff are made aware of the risks of inviting visitors to the office, and visitors, as far as practical, are kept to the neutral meeting rooms. Hosts will ensure that any visitors in the main part of the office will be supervised at all times.

	Discussing clients or projects over the telephone.	Staff are trained in identifying appropriate stakeholders before discussing project details over the telephone.
Data is inaccurate, insufficient, out of date or kept for too long		In transferring data from a customer system for staging or testing purposes files are timestamped to allow age identification. This timestamp is then used to remove old data in periodic sanitation checks. Assign clear responsibilities for data management