



Technical and organizational measures taken to secure personal data by Broadbean Technology Limited as a data processor (15 November 2019)

PHYSICAL ACCESS CONTROL

Measures to control access to premises and facilities where your data is processed and / or stored:

Broadbean Offices

The following measures are in force at Broadbean UK offices located in London.

- 24*7*365 Continuous manned reception & security guards
- Interior & Exterior CCTV Surveillance
- Security checks for visitors including visitor registration and passes
- Passes must be shown to access lifts
- Access control system using proximity cards at floor level
- Special access protection for server rooms via coded locks
- Security guidelines for utilization of mobile devices, e.g. laptops, iPads

Global Switch

You can read about the measures are in force at the Global Switch Data Centre located in London that Broadbean utilise by following this link:

<http://business.kcom.com/products/cloud/colocation/>

Amazon Web Services

You can read about the measures that are in force at the Amazon Web Services Data Centre located in Ireland that Broadbean utilise by following this link:

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

LOGICAL ACCESS CONTROL

Measures to prevent data processing systems from being used without authorization:

The following measures have been taken:

- Role-based access control following principle of least privilege
- Workstation password procedures (minimum of 8 characters including mixture of upper and lower case letters and numbers, 90 day's expiration, password history and prevention of reuse)
- Workstation automatic log-out or password protected screensaver after period without user activity
- Workstation personal firewall, anti-virus protection
- Server access procedures (SSH key authentication, passwords minimum of 12 characters, including at least 3 character types from upper case, lower case, numeric and non-alphanumeric)
- Remote access over VPN with multifactor authentication
- Network firewalls and Intrusion detection
- Centralised logging of access
- 2 factor authentication for remote access users via VPN



DATA ACCESS CONTROL

Measures that ensure that persons gain access only to such data as they are entitled to access in accordance with their access rights, and that, in the course of processing, your data cannot be read, copied, modified or deleted without authorization.

The following measures have been taken:

- authentication concept (access rights limited by profiles and roles)
- approval and assignment of access rights through authorized personnel only
- logging of access (full logging will be in place by no later than 25th May 2018)
- secure certified destruction of all desktop and datacentre storage media prior to disposal

DATA TRANSFER CONTROL

Measures to ensure that your data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of your data by means of data transmission facilities can be established and verified.

The following measures have been taken:

- secured data transfer (TLS or VPN)
- encrypted wireless access points
- firewall on connections between internal networks and internet
- firewall rules actively reviewed and managed

ENTRY CONTROL

Measures that include the establishment of an audit trail to document whether and by whom your data has been entered into, modified, deleted or removed

The following measures have been taken:

- authorization rules
- access rules
- full event logging (no later than 25th May 2018)

CONTROL OF INSTRUCTIONS

Measures to ensure that data being processed on behalf of you the Customer (as Data Controller) is processed solely in accordance with written Instructions between us:

The following measures have been taken: (or will be in place no later than 25th May 2018)

- Written data processing agreement (DPA) in place with all customers that sets out data elements and processing activities by product.
- Operational controls in place to ensure changes to the configuration of a Controller's account is properly authorised.
- Policy and process for documentation of any data processing instruction outside of normal contracted service provision

AVAILABILITY CONTROL

Measures to ensure that your data is protected against accidental destruction or loss.

The following measures have been taken:



- All production services run from at least Tier III standard certified data centre locations
- Disaster recovery policy
- Off-site backup and recovery procedures
- Real-time synchronised database slave
- Client files stored and backed up in highly durable cloud object store
- firewall protection
- anti-virus protection
- uninterruptable power supply (UPS)
- fire protection (early-warning-fire-detection, extinguishing system)
- water protection
- redundant air conditioning/cooling system
- All critical application services run load balanced configurations

SEPARATION CONTROL

Measures to ensure that Customer data collected for different purposes can be processed separately

The following measures have been taken:

- clear logical separation of data
- individual user profiles
- authorization concept
- separated systems for development and production environment