Data Security, GDPR and the BIS Platform

MAY 2018 (reviewed and updated May 2021)

The purpose of this document is to outline the measures Broker Information Services have taken to ensure Data Security and compliance with GDPR. In the main, these measures relate to data either entered and saved in the BIS Platform by the authorised user or data which is populated automatically via the data feeds from the Data Providers.

Encryption

All personally identifiable information (PII) is strongly encrypted before being stored in the database. Key rotation (encryption keys) is performed every 30 days.

All data transferred between the system and the user is encrypted using SSL, non-encrypted access is not available.

All documents uploaded to the system are encrypted as they are written to the disk.

As the encryption takes place at source on our system all backups (uploaded documents and database dumps) are encrypted.

Security

Our primary servers are hosted in a datacenter located in Dublin which is ISO27001 compliant. This is the BT datacenter in Dublin (Citywest). Click here for details of the BT Datacenter.

These servers are behind industry leading firewalls with a very restrictive set of access rules and redundancy.

Backups

After 30 days encrypted documents are transferred to our mass storage in a Zurich datacenter. This facility is compliant with SSAE16/SAS70. For further details, please click here.

A full daily backup regime is in place for documents held in our mass storage facility in Zurich.

Cyber Security

Exposure to Cyber attack is virtually inevitable in the current world and something that must be taken seriously both from a protection of personal data and financial perspective. At BIS we have taken the following steps to minimise the risk in this area.

Staff Training

Our staff are all fully aware of the sensitivity of the data held by BIS and we run quarterly training sessions around cyber security awareness.

Vulnerability Testing

We have invested significantly in software that allows us to run regular (weekly) tests to identify and rectify any vulnerabilities identified in the system.

Penetration Testing

Penetration testing is basically calling in the services of professionals in the field to attempt to hack into the system and to further identify any processes that should be adopted to minimise the possibility of success in this area. We carry out frequent such exercises for the comfort of ourselves, our suppliers and subscribers.