MiFIDII & GDPR Compliance

These are two separate regularity requirements; however they are linked in that MIFIDII will take precedence over some of the GDPR requirements, specifically in the right to have your data removed from a database and to not have your voice or SMS communications recorded.

There is also common ground between the two regulations in that any data held must be held securely and with a content management system that will enable the rapid retrieval of the data for management and regulatory audit.

The data held within the HSC product includes:

- External customer records for directory dialling and incoming call lookup.
- Internal user records for internal directory and handset/device identification
- Incoming and outgoing call records, also linked with names from the internal directories
- Voice call recordings*
- SMS messages*
- MMS Messages*
- Historical record of mobile location*

Data Location and Access

All data is held within the Mainstream Digital data centres, these are secure locations both from physical access and cyber access.

The data centres are totally owned and operated by Mainstream Digital and do not house or host any third-party equipment or services, therefore the only personnel that can access the sites are Mainstream employees and government or regulatory bodies personnel with the approved security clearance.

Mainstream Digital is a UK company and therefore governed under UK law, making the data held in its data centres subject only to UK law and not accessible by foreign governments or their agencies without the approval of a UK court.

Security Compliance and Certification

- ISO9001 (Quality Management)
- ISO27001/2 (Information Security Management)
- ISO22301 (Business Continuity)
- Cyber Essentials, IASME and GDPR compliant
- IL2/IL3 compliant
- Multi location and load balanced servers (99.999% reliability)

* Only relevant if these optional services are selected