

Data protection policy

This is a statement of the data protection policy adopted by Synergie Group PLC. Responsibility for the updating and dissemination of the policy rests with Synergie's Information Protection Officer. The policy is subject to regular review to reflect, for example, changes to legislation or to the structure or policies of the FSA. All staff are expected to apply the policy and to seek advice when required.

Synergie depends on Information and Communications Technology (ICT) systems to process data for mailing. Security of these systems and the data they hold, and of the hardware and networks on which they operate is necessary both to honour Synergie's obligations to providers of data as registered under the Data Protection Act, and to protect Synergie's systems and data from accidental or deliberate damage, loss or corruption. This policy statement is intended to effect implementation of the overall information security policy in respect of data held in ICT systems. All staff have a responsibility to comply with Synergie's policy on confidentiality of data and to comply with this statement of policy on data security.

We regard the lawful and correct treatment of personal information by the Financial Services Authority as important to the achievement of our objectives and to the success of our operations, and to maintaining confidence between those with whom we deal and ourselves. We therefore need to ensure that our organisation treats personal information lawfully and correctly.

The Data Protection Act 1998 came into force on 1 March 2000. Under the Data Protection Act, anyone processing personal information must comply with eight principles of good information handling. The eight principles state that the data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept longer than necessary;
- processed in accordance with the individual's rights;
- secure;
- not transferred to countries outside the European Economic area, unless there is adequate protection.

Data access and disposal

Access to each data store is limited to those needing such access to do their job (including 'privileged' system staff): the system design facilitates such access. Each member of staff with such access is personally responsible for maintaining the confidentiality of the data to which he/she has access. The Data Owner determines who should have access to data and the retention requirements (usually 3 months unless otherwise specified). If data is to be deliberately destroyed, then the Data Owner or their agent (whether internal or externally contracted) must ensure that destruction takes place in conditions compliant with the Data Protection Act.

Physical security

Data whether in electronic or physical form is subject to physical security control appropriate to its nature. Physical access is determined on the same basis as data access unless there are over-riding security reasons for doing otherwise.

Contingency

System specifications define the requirements for back up copies of programmes and data appropriate to the requirements of the system as determined by the Data Owner, institutional and legal requirements.

Data transfer

Supplied either as password protected ZIP files to Synergie's FTP or uploaded to the client's FTP and Synergie's Data Processing department are granted access. All passwords are sent separately to the data file, access to the client's FTP is granted via telephone. Proofs and Data Drops are supplied as password protected ZIP files, passwords are issued as above. Once proofs are lasered any wrecks are shredded and disposed of in a secure manner.

Synergie policy document version 5.6. Updated October 2009