

Data Protection Policy



This Data Protection Policy takes account of UK and EU law and conventions and specifically addresses the General Data Protection Regulations 2018 (GDPR).

1. Data Protection Policy

Anyone who obtains personal information ("data") about other individuals is a 'data controller' and is thus regulated by the Data Protection Act 1998 and the GDPR. The legislation controls what can lawfully be done with information and gives individuals certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a data controller has about them and ask for copies of data. There is also now an enhanced set of Individual Rights that an organisation needs to respect.

CS2 is a data controller in relation to all the information that the organisation obtains about employees, agency workers, suppliers, clients and contractors.

We must be able to demonstrate that any personal data we handle is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date where necessary
- kept for no longer than is necessary where data subjects are identifiable
- processed securely and protected against accidental loss, destruction or damage.

CS2 is committed to following these principles. Data will be retained only as long as necessary.

Data will be kept in a secure system whether manual or computerised, to the best of our ability at all times. When transmitting data this will be password protected and/or encrypted.

The Act prohibits the transfer of data outside the European Economic Area to countries that do not have similar protection of data except in some circumstances or with the subject's consent. CS2 has no intention of sharing personal data outside the UK.

2. Access to Data

James Bedster will act as Data Protection Officer and be supported in this role by RSK.

A request for access to any personal data that relates to an individual will be made by a written request using the Data Access Request form and the originator's details will be verified. The completed form must be returned to the Data Protection Officer. There are no fees chargeable for this.

There may be certain circumstances where a person's consent cannot be obtained or is not legally required. Before releasing personal data to external organisations (including the police) the organisation will seek to obtain legal advice on its obligations and where necessary ask for a court order or a magistrates' warrant before release of personal information about employees, clients or suppliers.

CS2 policy is to provide copies of all data that the organisation is obliged to disclose to third parties within 40 working days of receipt of a request being received by the data protection compliance officer.

CS2 considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect us to be obliged to comply with a further request before a year has elapsed unless there are exceptional circumstances. It is our policy to ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken (see paragraph 3 below).

For the purposes of the DPA and the GDPR, data is any personal information that is collected on an individual for whatever purpose and which is then recorded, processed or stored in some way for legal, business, technical or organisational reasons.

The information can be paper based and filed manually, or electronically and saved on computerised systems or in a “cloud” database. The GDPR extends this to include biometric or visual images that can identify a person, and any automated processing that takes place. CS2 will undertake an audit of all types of data collection, recording and processing taking place and repeat this on an annual basis. We will review the reasons for the data being obtained and justify why this should continue or make a decision it will no longer be obtained. Similarly, we will review the way in which the data is stored and processed to ensure all appropriate safeguards are in place and security/confidentiality measures are effective and will:

- carry out a risk assessment of data systems and act on the results;
- maintain up-to-date security systems (for example, using firewalls and encryption technology);
- restrict access to personal data to only those who demonstrate that they need it;
- train staff on data security; and
- review data security regularly.

3. Individuals' Rights

Data subjects will have the:

- **right to be informed about the processing of their personal data** – the Guidance on Data Protection and this document sets out how the organisation is complying with the data protection requirements for the processing of personal data;
- **right to rectification if their personal data is inaccurate or incomplete** – requests to amend data will normally have to be processed within one month;
- **right of access to their personal data** and supplementary information, and the right to confirmation that their personal data is being processed;

A handwritten signature in black ink, appearing to read 'David S Jay'.

David S Jay BSc(Hons) FRICS
Director

Last Review Date: June 2025
Next Review Date: June 2026