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 People Network Consultancy (PNC).

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;

- **data subject access requests (SARs**) – a data subject can at any time request access to their personal data and a process for such requests will be devised. A SAR will be responded to within 20 working days of receipt (as per GDPR requirements);
- **right to be forgotten** by having their personal data deleted or removed on request where there is no compelling reason for an organisation to continue to process it – any data subject will be given the opportunity to challenge any data held on them and ask for its removal;
- **right to restrict processing of their personal data**, for example, if a data subject considers that processing is unlawful or the data is inaccurate – as for the right to be forgotten;
- **right to data portability of their personal data** for their own purposes (data subjects will be allowed to obtain and reuse their data) – data will be kept in a format capable of portability/transferability;
- **right to object to the processing of their personal data** for direct marketing, scientific or historical research, or statistical purposes – as for the right to be forgotten.

4. Lawful Basis

The basis for keeping personal data of business contacts of clients, suppliers and contractors is contractual, ie business could not proceed without recording certain key details. The details recorded in this case may include name, business contact address(es), business contact phone number(s), business email address(es), organisation name, professional qualifications, accreditations, job title.

For prospective clients who are part of a framework then the basis is legitimate interest.

For prospective clients who have been approached by us the basis is consent which if declined, the details are deleted from our records.

5. Breach of Data Protection Policy or Legal Requirements

Any suspected or actual breach of this policy whether direct or indirect, malicious or unintentional must be reported immediately to the Data Protection Manager and the ICO (Information Commissioner's Office) informed.

The organisation will implement its contingency plan in order to immediately protect personal data and resolve the cause of the breach.

Any breach will be recorded in the breach log.

6. Contact Details

Any communication regarding CS2's Data Protection Policy can be addressed to DPO, CS2 Limited, Bridgewater House, 4 Queensbridge, Northampton, NN4 7BF or email dpo@cs2.co.uk

June 2021