Chartsign Privacy Policy

Company : Chartsign Limited (“the Company”) Registered in England and Wales

Company number: 01927705

Policy Name: Information Security and Data Protection

Date: 25th May 2018

Version: 01

The General Data Protection Regulations 2018 – GDPR: The Company processes personal data in relation to its own staff, training delegates and individual client contacts – therefore it is a “*data processor*” for the purposes of the General Data Protection Regulations 2018. The Company holds personal data on individuals (“*data subjects*”) for the following:

- Accounts and records (legal and contractors)
- Design, delivery of purchase orders

The General Data Protection Regulations data principles: The General Data Protection Regulations 2018 requires the Company as data processor to process data in accordance with the principles of data protection. Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or

rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

"*Personal data*" means, any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. "*Processing*" means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, mainframe, desktop, laptop, iPad, Blackberry ® or other mobile device. Personal data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Sensitive personal data: Article 9 of the GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data in respect of the following is "*sensitive personal data*" and will not be gathered by the company unless in specific circumstances and not without prior consent. Any information held on any of these matters WILL NOT be passed on to any third party.

- Any offence committed or alleged to be committed by them.
- Proceedings in relation to any offence and any sentence passed.
- Physical or mental health or condition.
- Racial or ethnic origins.
- Sexual life.
- Political opinions.
- Religious beliefs or beliefs of a similar nature.
- Whether someone is a member of a trade union.

Information security: From a security point of view, only those staff listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ("database" includes paper records or records stored electronically). However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date. In addition all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who have access to personal data.
- Passwords should not be disclosed.
- Email should be used with care.
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended.
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail.
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. Such material should be shredded or stored as confidential waste awaiting safe destruction.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact. A failure to observe the contents of this policy will be treated as a disciplinary offence.

Subject access requests: Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15) Fees: The company will provide a copy of the information free of charge. However, the company may also charge a reasonable fee to comply with requests for further copies of the same information, though there will be no charge for all subsequent access requests.

Any fee will be based on the administrative cost of providing the information.

Timescales: Information will be provided without delay and at the latest within one month of receipt. Where requests are complex or numerous the period of compliance will be extended by a further two months. If this is

the case, the individual will be informed within one month of the receipt of the request with an explanation of why the extension is necessary

APPENDIX: List names of those responsible for adding, amending or deleting data; and responsible for responding to subject access requests

Claire Gordon, Kranthi Puppala (Data Controllers & Processors) Chartsign Limited Technocentre, Coventry University Technology Park, Puma Way, Coventry, CV1 2TT; email: claire@chartsign.com; T: +44(0) 7909 118908