GCP 255	Data Protection Policy

Document History

Section	Changes made	Date
All	New Document	May 2018

Cherwell Valley Silos Limited ("CVS") is required to keep and process certain information about its employees, customers, suppliers etc in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

CVS may, from time to time, be required to share personal information with other organisations.

This policy is in place to ensure all employees are aware of their responsibilities and outlines how CVS complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and CVS believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

We take seriously our duties, and the duties of our employees, under the General Data Protection Regulations ("GDPR"). This policy sets out employees' obligations in relation to any personal data that they handle.

Frequently used terms in this Policy

Data protection law is complex and technical. Below, we set out definitions of a few key terms to assist with your understanding.

Data controller — the body which, alone or jointly with others, determines the purposes and means of the processing of personal data. (As an employer, you will be a data controller in respect of your employees' personal data)

Data processor — a body which processes personal data on behalf of the controller. (An organisation that processes personal data only on your instructions, such as a payroll provider, will be a data processor).

Data subject	an identified or identifiable natural person (i.e. the individual to whom personal data relates)
Personal data	information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Data includes electronic (including that on mobile phones and other devices) and manual information. Personal data covered by the regulations is not just the obvious. Individual business email addresses are deemed personal data and hence covered. Personal data is held on telematics/tachographs/cameras/cctv etc. Broadly anything that can be used to identify an individual is covered!
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Data protection compliance

We will process personal data to comply with the eight principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

Legal bases for processing

The legal basis for processing any personal data will be identified prior to data being processed.

There is a sub-category of personal data, known as special category. The GDPR places more restrictions on the processing of special category data than on ordinary personal data. CVS does not process special category data.

The legal bases for processing ordinary personal data are:

- The processing is necessary to comply with a legal obligation (other than one arising from a contract)
- The processing is necessary to perform a contract with the individual, or to take steps to enter into a contract at the individual's request
- The processing is necessary for your legitimate interests, or the interests of a third party if you are disclosing it to them, and those interests are not outweighed by the interests, rights or freedoms of the individual (BUT note that public authorities are not permitted to rely on this legal basis)
- The individual consents to the processing (BUT note that there are lots of conditions that must be met for consent to be valid under the GDPR and there are additional problems with using it in the employment relationship, so we do not recommend using this legal basis for processing – see Problems with consent, below)
- The processing is necessary to protect the vital interests of the individual or another person (life and death situations)

Right to fair processing information

Under the GDPR, individuals have the right to receive 'fair processing information', telling them how CVS processes their personal data.

CVS must therefore provide the required fair processing information to individuals we hold data for. The document in which this information is presented is referred to as a privacy notice.

The GDPR sets out a detailed list of information that must be included in a privacy notice. This is linked to the GDPR concept of "granularity", which embodies the need to give detailed, specific information to individuals – a generic, catch all statement won't be sufficient. It is also linked to the requirements of transparency and fairness.

CVS must regularly update all Privacy Notices prepared.

The right of access - Subject Access Request ("SAR")

The GDPR gives individuals a number of rights in relation to their personal data. One of these is that an individual can make a request concerning the personal data held about them. This request could come from an employee, customer, supplier, contact etc and as a company CVS must be able to respond to such a request, free of charge, within 30 days.

Any such requests must be dealt with in accordance with CVS's Subject Access Requests Procedures and Guidelines policy.

Other individual rights

In addition to the right of subject access, the GDPR also gives individuals the following rights in relation to their personal data:

- Right to receive fair processing information
- Right to object to processing
- Rights to erasure, to restrict processing, and to rectification
- Right to data portability
- Restrictions on decisions being taken by automated means

As with SARs, the timeframe for responding to an individual rights request is 30 days.

Any requests in respect of these individual rights should be dealt with in the same way as SAR's.

The exemption for requests that are "manifestly unfounded or excessive", described above in relation to SARs, applies to the other individual rights as well, but in most cases employers are likely to find the exemption difficult to establish.

If an employee receives any such request, he/she should pass it to the Finance Director immediately.

Privacy Impact Assessments

Should CVS adopt new practices in future (eg adoption of new technology, changing of processing practices) then we need to devise and implement a Data Protection Impact Assessment (DPIA) process to ensure legal compliance. **If an employee becomes aware of any planned changes that may require this he/she should let the Finance Director know. NO such changes can be made before a DPIA has been prepared.**

Data Breaches

A data breach is defined in the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A data breach includes accidental leaks, such as an employee typing the wrong email address; or losing a smartphone

CVS must be able to inform the Information Commissioner's Office of any major data breach within 72 hours. **If an employee becomes aware of any breaches he/she should advise the Finance Director know immediately.**

Data security

Everyone has rights with regard to the way in which their personal data is handled. During the course of the company's activities, we will collect store and process personal data not only about our employees but also about our customers, suppliers and other third parties.

If an employee acquires any personal data in the course of his/her duties, he/she must ensure that the use of the information is for a relevant purpose and that it is not kept longer than necessary. If an employee receives personal information in error by whatever means, he/she must inform the Finance Director. If an employee is in any doubt about what to do with personal information, he/she should seek advice from the Finance Director.

An employee must also ensure that the information is accurate and up to date, insofar as it is practicable to do so.

Employees are obliged to comply with data protection law and the data principles set out above when processing personal data on our behalf (including that of other employees). In particular they are obliged to comply with the provisions set out below and/or any other guidelines produced by the company relating to personal data and/or any other management instructions.

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Use password-protected and encrypted software for the transmission and receipt of emails
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft. Passwords should be strong, not shared and regularly changed'
- Employees will not use their personal laptops or computers for trust purposes.

- All necessary employees are provided with their own secure login and password. Passwords should be strong, not shared and regularly changed'
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, employees will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, employees will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from CVS premises accepts full responsibility for the security of the data.
- Before sharing data, all employees will ensure that adequate security is in place to protect it and that whoever is to receive the data has been outlined in a privacy notice (copies available on the CVS website or from the Finance Director).
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of CVS containing sensitive information are supervised at all times.
- The physical security of CVS's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The IT Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

CCTV

CVS understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

CVS notifies all employees and customers/suppliers visiting the site of the purpose for collecting CCTV images via Privacy Notices and on site signage.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

Data retention

Data will not be kept for longer than is necessary and any data no longer required will be deleted as soon as practicable. Further information is provided in the company's Privacy Notices.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Conclusion

Compliance with the GDPR, is the responsibility of all members of employees of CVS. Any breach of the Data Protection Policy may lead to disciplinary action being taken. Any questions or concerns about the interpretation or operation of the policy should be referred to the Finance Director.

If you require any further information on the GDPR, or how any aspect is implemented at CVS please make contact the Finance Director.