CCL GDPR

Data Protection Policy

May 2018

Context and overview

Key details

- Policy prepared by: Chris Ballinger
- Approved by board / management on: 09/05/2018
- Policy became operational on: 09/05/2018
- Next review date: 09/05/2019

Introduction

Customer Consulting Ltd (CCL) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the European Privacy Regulation called GDPR.

Why this policy exists

This data protection policy ensures Customer Consulting Ltd:

- Understand what GDPR is and how it impacts us
- Understands individuals rights around personal data
- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

Customer Consulting Ltd is committed to a policy of protecting the rights and privacy of individuals, including, staff, associates, clients and customers, in accordance with the General Data

Protection Regulation (GDPR) May 2018. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Customer Consulting Limited understand that the Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Under the GDPR individuals have:

1. The right to access
2. The right to be forgotten
3. The right to data portability
4. The right to be informed
5. The right to have information corrected
6. The right to restrict processing
7. The right to object
8. The right to be notified

General Data Protection

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals, for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs), and may include facts or opinions about a person.

For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of CCL
- All staff of CCL
- All contractors, suppliers and other people working on behalf of Customer Consulting Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Driving License
- Passport Information
- · CRB Check's
- · …plus any other information relating to individuals.

Below is a list of personal data that we believe will be affected at CCL:

Individual	What data we might have?	Where it would be stored?	Who would have access to it?
Employees	▪ Address ▪ Phone Number ▪ D.O.B ▪ Salary ▪ Driving Licence ▪ Passport ▪ Email Address ▪ Bank Details	▪ CCL Server ▪ Hard Copies	▪ Directors ▪ Company Secretary ▪ Office Manager
Recruitment Applicants	▪ Address ▪ Phone Number ▪ Email Address	▪ CCL Server ▪ Hard Copies	▪ Directors ▪ Company Secretary ▪ Office Manager
Consultants	▪ Address ▪ Phone Number ▪ D.O.B ▪ Salary ▪ Driving Licence	▪ CCL Server ▪ Hard Copies ▪ Company Contact Database	▪ Directors ▪ Company Secretary ▪ Office Manager ▪ CCL Staff

	▪ Passport ▪ Email Address ▪ Bank Details ▪ CV		
Clients	▪ Address ▪ Phone Number ▪ Email Address	▪ ACT ▪ Company Contact Database	▪ Directors ▪ Company Secretary ▪ Office Manager ▪ CCL Staff
Prospects	▪ Phone Number ▪ Email Address	▪ ACT ▪ Company Contact Database	▪ Directors ▪ Office Manager ▪ CCL Staff
Client Customer Data	▪ Varies depending on the client	▪ Company Server or wherever the client tells us to store it	▪ Directors ▪ Office Manager ▪ CCL Staff

Data protection risks

This policy helps to protect CCL from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, the information being given out inappropriately
- **Failing to offer a choice.** For instance, all individuals should be free to choose how the company uses data relating to them
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Customer Consulting Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Customer Consulting Ltd meets its legal obligations.
- The **data protection officer** is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule
  - Arranging data protection training and advice for the people covered by this policy
  - Handling data protection questions from staff and anyone else covered by this policy

- Dealing with requests from individuals to see the data Customer Consulting Ltd holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Not to retain personal data for longer than is necessary to ensure compliance with the legislation and any other statutory requirements. This means CCL will undertake a regular review of the information held and implement a weeding process. CCL will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

- The **IT manager (EBS IT)**, is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The **Directors** are responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their managers
- Customer Consulting Ltd will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Printouts not to be left on printers
- Operate a clean desk policy
- Ensure pc is locked when away from the desk
- Ensure pc is shut down at end of the working day
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should request help from their manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Office Manager or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. Customer Consulting Limited keep hard copies of HR and other personal data in a filing cabinet which is locked at all times. This can only be accessed by the Directors, the Data Controller and the Office Manager.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Customer Consulting Ltd unless the business can make use of it, we only rely on legitimate interests for using data. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Client Data

Because we would not be the main controller of our client's data, they would have the sole responsibility for the personal data on their customers. Whilst we would follow our data protection procedures written in this policy, e.g. storing data safely, not passing on data to other people. Ultimately, we will follow the client's data policy guidelines which they stipulate.

Data accuracy

The law requires Customer Consulting Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Customer Consulting Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call
- Customer Consulting Ltd will make it easy for data subjects to update the information Customer Consulting Ltd holds about them. For instance, via the company website
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months (CPS and CTPS).

Subject access requests

All individuals who are the subject of personal data held by Customer Consulting Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.

- Be informed how to keep it up to date.
- Be informed of how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at chris.ballinger@customerconsulting.com. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.
If they want the information to be deleted Customer Consulting will:

- Check for electronic and hard copies
- Check on ACT/ Company Database / Server

The data controller will always verify the identity of anyone making a subject access request before handing over any information. This will be done by:

- Calling the person to confirm who they are.

The process that Customer Consulting will carry out to ensure we are complying with subject access requests is:

1. Confirm if the individual is who they say they are
2. Check all platforms for electronic copies
3. Send any data we have on the individual
4. Delete or update the information we have
5. Send an email to confirm deletion or updating of information
6. Update data log of the subject access request

Business to Business Marketing

CCL carry out b2b marketing and therefore under the new GDPR will follow the below:

- Only market to business by call and email to try and prospect and get new business
- Have a do not contact consent at the bottom of our emails sent out
- If they request us to take them off our databases then we will
- We will never market to sole traders
- We will only rely on legitimate interests
- We won't call people on the CPS and CTPS list
- We will update the CPS and CTPS each year.

Safeguarding personal data

CCL will ensure the safeguarding of personal data held by the company by:

- Having password protected computers
- Having password protected databases
- Keeping all hard copies of personal data locked with limited access
- Locking the office
- Getting staff, clients and consultants to sign confidentiality agreements.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Customer Consulting Ltd UK Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential or restricted to Customer Consulting Ltd access only. Therefore it is Customer Consulting Ltd policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of Customer Consulting Ltd to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Customer Consulting Ltd email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the Customer Consulting Ltd may be accessed by someone other than the recipient for system management and security purposes.

Process for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998. Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection

which is available from the website. For help or advice on any data protection or freedom of information issues, please do not hesitate to contact: The Data Protection Officer (DPO).

Glossary

Data Controller

A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. The term comprises not only individuals but also organisations such as companies and other corporate bodies of persons.

Data processor

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data subject

Any living individual who is the subject of personal data.

Personal data

Information which relates to a living individual who can be identified from that data, from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing

Any operation or set of operations performed upon personal data, whether or not by automatic means. These include collecting, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Sensitive personal data

Personal data which consists of data related to the data subject's racial or ethnic origin political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the commission of offences or criminal proceedings.