

Data Protection and GDPR Policy

Updated on 5th August 2019

Counter Context Ltd has written this data security policy to ensure it is compliant with The General Data Protection Regulation (GDPR). Its aim is to depict all aspects of legal data protection in one summarising document. This is not only to ensure compliance with the GDPR but also to provide proof of compliance.

Counter Context Ltd are responsible for processing, maintaining and storing all personal and sensitive data in line with the GDPR Principles which are detailed below:

1. Personal data shall be:
 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 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, in accordance with [Article 89\(1\)](#), not be considered to be incompatible with the initial purposes ('purpose limitation');
 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
 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 in accordance with [Article 89\(1\)](#) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 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 ('integrity and confidentiality').

Data Concepts and Categories

Counter Context takes responsibility for acting as both a Data Controller¹ and Data Processor².

Counter Context Ltd store and process Personal Data³ belonging to Data Subjects⁴ on the following categories under the lawful basis⁵ underlined in the GDPR:

- Employee Personal and Sensitive Data⁵ – Under the lawful basis of: Contract.
- Client Personal Data – Under the lawful basis of: Contract and Legitimate Interest
- Stakeholder Personal Data – Under the lawful basis of: Public Interest

All data will be archived when it is no longer relevant and required. It will be archived for a number of years before being securely disposed of.

- Employee Data – Archived for 6 years
- Client Data – Archived for 6 years
- Stakeholder Data – Archived for 3 years

All personal data is obtained with explicit, specific and positive consent and used for its original purpose only. Consent and how it was obtained will also be stored. Data is stored securely as detailed below.

Personal Data of Stakeholders is used on behalf of clients to gauge public opinion via feedback, create reports and to ensure members of a specific community that may be affected by a client's work are informed of activity in their area.

¹ Data controller means 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.

² Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

³ Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those 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.

⁴ The Data Subject is a living individual to whom personal data relates.

⁵ Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Electronic Data

- All systems are virus protected and all patches/security updates and upgrades are regularly maintained.
- All systems, including access to individual computers, the server network and to mail clients, are password protected.
- Databases recording Sensitive or Personal Data such as names and contact details are stored separately to any consultation/survey responses and are password protected.
- Back-ups are undertaken every hour each day on a secure server and copied to an external hard drive and encrypted.
- Employee Personal and Sensitive Data is stored on a confidential server with limited access to those who require it.

Physical Data

- All consultation/survey responses are locked in dedicated filing cabinets and the keys to those are, in turn, secured in a locked cabinet, access to which is only available through the appointed security manager.
- Physical copies of Personal and Sensitive Data is kept to a minimum and locked in dedicated filing cabinet with a combination lock.
- No data storage devices/equipment, apart from the back-up hard drive, is taken off the business premises.
- The office is locked outside of office hours; access is restricted to staff members.
- The office building is security alarmed with cameras in and out of the main building and the offices.
- All confidential waste is securely disposed of and shredded via a specialist company, Russell Richardson.

The responsibility of these security measures being adhered to lies with individual members of staff and is monitored by line managers. All staff members are required to sign a confidentiality agreement which outlines their requirements and consequences for any breaches of confidentiality. As the company grows, the need for a dedicated Data Protection Officer will be reviewed.

Data Subject Access

Counter Context Ltd understands that Data Subjects have a legal right to access any Personal or Sensitive Data the company holds on them. They also have a right to request their data be removed from our databases. These requests must be completed within one month. Verification should always be obtained before sending Personal or Sensitive Data to someone at their request, this is to ensure that one Data Subject's details is not being sent to another person, either by error or deception. Verification should be simple, for example asking the person to confirm additional personal details that can be cross referenced for certainty. Depending on the sensitivity of the data we may require further identification to prevent harm from Sensitive Data reaching the wrong person.

Counter Context Ltd do not sell or share data with any third parties. The only instances that it is acceptable for the company to share details are with specific consent, for example, an employment reference for a previous employee, or when a stakeholder has requested communication with the client in special circumstances.

Data Breaches

Any breaches of confidentiality and security must be reported in line with the GDPR guidelines.

Signed:

Alexis Krachai
Managing Director