CCM Facilities Ltd
Trident House Lower Ground Floor | 46-48 Webber Street
London | SE1 8QW | 020 7803 4777
www.ccmfacilities.com
Registered in England No: 2498745 | VAT No: 711 0089 83

Data Protection & GDPR (General Data Protection Regulation 2016/679) Policy

1. General Statement

CCM Facilities Ltd understands the importance of protecting personal information and is committed to complying with the General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 (DPA). It is committed to fostering a culture of transparency and accountability by demonstrating compliance with the principles set out in the Regulation.

The GDPR sets out the rules for how organisations must process personal data and sensitive personal data about living individuals. It gives individuals the right to find out what personal data is held about them by organisations and to request to see, correct or erase personal data held.

We need to collect and process personal data about the people (including employees and individuals) we interact with to carry out our business effectively.

We are committed to ensuring that employees are appropriately trained and supported to achieve compliance with the GDPR and DPA.

Endorsed by; G Doherty, Managing Director: Dated: 01/06/2019

2. Policy scope

2.1 This policy applies to all personal data collected and processed by us in the conduct of our business and applies to both electronic and manual filing systems.

2.2 This policy applies to all employees, whether permanent or temporary together with any relevant 3rd parties such as contractors and consultants.

3. Personal data definitions

3.1 Personal data is defined in the GDPR and DPA:

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Special categories of personal data relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Data protection principles

The GDPR and DPA outlines six principles which underpin the handling of personal data. To ensure compliance with the Regulation, we ensure that personal data is:

(a) Processed lawfully, fairly and in a transparent manner. In practice this means:

- Having legitimate grounds for collecting and using personal data.
- Not using personal data in a way that would have an adverse effect on the rights and freedoms of any individual.
- Being transparent about how we intend to use personal data and provide privacy notices where appropriate.
- Handling personal data in a way that people would reasonably expect.
- Ensuring that we do nothing unlawful with personal data.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In practice this means:

- Being clear about why we are collecting personal data and what we will do with it.
- Providing privacy notices when collecting personal data.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which personal data is processed. In practice this means only processing the personal data that is necessary.

(d) Accurate and, where necessary, kept up to date. In practice this means:

- Taking reasonable steps to ensure the accuracy of any personal data held.
- Ensuring that the source of the personal data is clear.
- Carefully considering any challenges to the accuracy of personal data.
- Considering whether it is necessary to update the information.

(e) Not kept for longer than is necessary for the purpose. In practice this means:

- Reviewing the length of time personal data is retained.
- Securely deleting personal data that is no longer needed.

(f) Processed in a manner that ensures the security of personal data using appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction. In practice this means:

- Designing and organising our security to fit the nature of the personal data held and the harm that may result from a breach.
- Ensuring that the right physical and security measures are implemented, backed by robust policies and procedures and reliable, well-trained employees.
- Ensuring we regularly audit our security measures.

4.2 We are able to demonstrate compliance with these principles.

5. Access to personal data

5.1 Employees will have access to personal data only where it is required as part of their job role.

5.2 People are entitled to make Subject Access Requests to ask whether the Company holds any personal data relating to them and, if so, to be given a description of and a copy of that personal data. Exemptions may apply in certain circumstances.

5.3 Subject Access Requests are dealt with in our Privacy Policy.

6. Data sharing

6.1 Personal data will not be transferred outside the European Economic Area

6.2 Personal data in any format will not be shared with a third party organisation without firstly obtaining consent from the Data Subject.

6.3 Privacy by design

6.4 We are committed to meeting the GDPR and DPA requirement to consider data privacy at all stages of processing.

6.5 The Company is able to demonstrate to Data Subjects and Regulators that personal data is handled in a responsible and secure way in compliance with the GDPR and DPA.

7. Roles and responsibilities

7.1 Data Security Officer has overall responsibility for our compliance with the GDPR and the DPA as a data controller and data processor.

7.2 All employees are responsible for ensuring that they familiarise themselves with this policy, our Data Protection Procedure and related documents.

8. Policy benefits

8.1 This policy will benefit the Company by:

- Promoting transparency and accountability and fostering a data protection culture across the organisation.
- Ensuring compliance with the GDPR and DPA.
- Ensuring employee confidence and compliance in the processing of personal data, being fully informed and aware of their responsibilities and obligations.

9. Compliance

9.1 Breaches of this policy and our GDPR /DPA compliance system will be investigated and appropriate actions taken.

10. Review

10.1 This policy will be reviewed annually or as business reasons dictate.

11. Duties of Sub-Contractors

CCM Facilities Ltd operates a supplier policy and maintains a preferred supplier list. We conduct due diligence on all suppliers before allowing them to become a preferred supplier. Our Data Protection and GDPR Policy and Privacy Policy is issued to all suppliers and they are required to confirm that no part of their business operations contradicts this policy.

12. Associated Policies

Our associated policies to the Data Protection and GDPR Policy are the following:

- Privacy Policy
- Security Policy
- Sub-Contractor Policy and Control