DATA PROTECTION POLICY

CLIPFINE
GROUP OF COMPANIES

1. Policy Statement

1.1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. About this Policy

2.1. It is the Policy of Clipfine to comply with the Data Protection Act 2018 (DPA), and good practice at all times.

2.2. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3. The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Stewart Milne - HR Department and deputised by Peter Hahn – Quality and Compliance. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

3. Definition of Data Protection Terms

3.1. **Data** is information, which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address, or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5. **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6. **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on Clipfine's behalf.

3.7. **Processing** is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.

4. Procedures for data processing

4.1. Each of the 'trading entities' of the Clipfine Group have registered with the Information Commissioner's Office for data protection. Clipfine's data protection procedures are audited by The National Security Inspectorate (NSI) as part of our NSI Guarding Gold and Security Industry Association Approved Contractors Scheme certifications.

4.2. Clipfine have established within our ISO 9001: 2015 Quality Management System effective Personal Information Management procedures (PIMs system). The "PIMs" enables the implementation of this policy which is compliant with the requirements of DPA and BS 10012: 2017 "Specification for a Personal Information System".

4.3. The "PIMs" procedures for data processing which includes the identification of all external and internal stakeholders; individuals with responsibility within the "PIMs system" with controls to ensure that the minimum personal data collection and processing is adequate, secure, strictly necessary, not excessive for the specific purpose and is:

4.3.1. Processed fairly, lawfully and retained securely and only as long as is necessary.

4.3.2. Processed for limited purposes and in an appropriate way.

4.3.3. Not kept for longer than the necessary purpose.

4.3.4. Not transferred to people or organisations situated in countries without adequate protections.

4.3.5. Processed in line with the data subjects' rights.

4.3.6. An inventory is maintained of the personal information categories for the purposes of exercising or performing any right or obligation which is conferred or imposed by law or (including permissible exemptions allowable by DPA) on Clipfine through contract.

4.3.7. In connection with any legal proceedings or for the purpose of obtaining legal advice.

4.3.8. For the administration of justice, for the exercise of functions conferred by statute, or for the exercise of any function of the Crown.

4.3.9. Data for the purpose of monitoring equality is carried out with appropriate safeguards for the rights and freedoms of data subjects and that information is accurate, and where necessary kept secure and up to date.

4.3.10. Respectful of individual data subjects' rights in relation to their personal information, including their right to access information held on written request to the "Data Controller" at Clipfine Head Office; and

4.3.11. Where CCTV recording is in place, the replaying and reviewing of data for the purposes of identifying an individual is a "Licensable Activity" and shall only be undertaken by a licensed security professional holding a current CCTV SIA licence.

4.3.12. Clipfine Group of companies are registered with the ICO.

4.3.13. CCTV cameras may be installed in your work area such as building perimeter, access and egress points, stair cases and office areas. If this is the case, the cameras are installed for security reasons only and are never installed in private areas such as toilets facilities and changing rooms.

4.3.14. CCTV footage can be obtained by completing the company subject access request process

5. Communication and Consent

5.1. This policy is communicated to all existing and potential employees and "other" individuals who provide information for the purposes of access control to be used as part of the premises site emergency plan.

5.2. Personal data of employees, prospective employees and subcontractors and the employees of our Clients subcontractors is used as part of Clipfine's security, safety, and welfare access control systems.

5.3. Explicit consent is obtained from all individuals providing personal data for specified use which includes clear purpose and methods of how the processing and storage stated at the time of information request.

5.4. Clipfine will not transfer data outside the European Economic Community unless it has been confirmed that it can be adequately protected, and explicit permission has been obtained from the Data Subject.

5.5. Data provided by individuals, Clipfine employees, employees and visitors of Clients and employees of Subcontractors regarding their qualification and competence is used for validity checks of expiry dates for CSCS and related scheme cards including SIA Licenses. Where personal data is collected for the Principal Contractor for the management of access permits; all such "personal data" in hard copy and or electronic form will be held securely under lock and key, and as applicable password protected computer systems. Any person requesting sight of such information must have written authority from the authorised "Data Processor"; for clarity this will be the Clipfine Contract Manager. Upon completion of the Contract the hard copy data will be securely shredded by the Data Controller, who in most cases is the Principal Contractor of the site.

6. Security

6.1. We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

6.2. Security procedures include:

6.2.1. Entry controls. Any stranger seen in entry-controlled areas will be reported.

6.2.2. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

6.2.3. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

6.2.4. Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

6.3. All Security Officers processing personal data on behalf of Clipfine have been security screened and vetted in accordance with BS7858.

7. Disclosure and Sharing of Personal Information

7.1. We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

7.2. We may also disclose personal data we hold to third parties:

7.2.1. In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

7.2.2. If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

7.2.3. If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8. Dealing with Subject Access Requests

8.1. Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately.

8.2. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

8.2.1. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

8.2.2. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

8.2.3. Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

This policy applies to all employees of Clipfine Limited.

Date: November 2020

Signed: 

T. MacCarron
Chairman

Clipfine Limited

30 John Street
London
WC1N 2AT

Tel 0845 6128811
info@clipfine.com
www.clipfine.com