



Data Protection and Information Security Policy

Introduction

This Practice is committed to protecting the privacy and security of personal data and information entrusted to us by our clients. This Data Protection and Information Security Policy outlines the measures we take to ensure the confidentiality, integrity, and availability of personal data and information in our care.

Scope

This policy applies to all personal data and information processed by this Practice, including data and information processed on behalf of our clients. It covers all aspects of information security and data protection, including data collection, storage, processing, transmission, and disposal.

Compliance with Data Protection and Privacy Laws

This Practice complies with all applicable data protection and privacy laws and regulations, including the General Data Protection Regulation (EU-GDPR), the Data Protection Act 2018, and any other applicable laws or regulations in the countries where we operate.

Collection and Use of Personal Data and Information

This Practice collects and uses personal data and information only for the purposes for which it was collected and in accordance with applicable laws and regulations. We collect personal data and information from our clients, their customers, and other sources only when necessary and with the consent of the individuals concerned.

Data and Information Security

This Practice implements appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data and information in our care. We implement measures such as encryption, access controls, firewalls, and monitoring

to protect against unauthorised access, disclosure, or use of personal data and information.

Data and Information Retention and Disposal

This Practice retains personal data and information only for as long as necessary to fulfil the purposes for which it was collected or as required by applicable laws and regulations. We securely dispose of personal data and information when it is no longer needed, in accordance with our retention and disposal policies.

Data Subject Rights

This Practice respects the rights of data subjects under applicable data protection laws and regulations, including the right to access, rectify, erase, restrict processing, object to processing, and data portability. We provide data subjects with mechanisms to exercise these rights and respond to their requests in a timely and appropriate manner.

Third-Party Service Providers

This Practice engages third-party service providers only when necessary and in accordance with applicable laws and regulations. We ensure that these service providers comply with the same data protection and information security standards as [Company] and enter into appropriate contracts to ensure the protection of personal data and information.

Training and Education

This Practice provides regular training and education to all employees, contractors, and third-party service providers on the importance of data protection and information security and the requirements of this policy. This training covers topics such as the handling and storage of personal data and information, data subject rights, and the identification of potential security threats.

Enforcement and Consequences of Breach

Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including termination of employment or contractual obligations. This Practice reserves the right to take legal action to protect personal data and information and to seek damages for any harm caused by a breach of data protection or information security.

Review and Update

This policy will be reviewed and updated on a regular basis to ensure that it continues to meet this Practice's needs and complies with any changes in applicable laws and regulations.

New update from DCME 27.3.23