marantec
engineered for you

Marantec UK Privacy Policy

Data Protection Policy

marantec
engineered for you

Data Protection Policy

Marantec UK Privacy Policy

1. Introduction
Marantec UK (the Company) processes the personal data of living individuals such as its staff, customers and suppliers. This processing is regulated by the General Data Protection Regulation (GDPR). The UK's regulator for the GDPR is the Information Commissioner's Office (ICO). Marantec UK is registered as a Data Controller with the ICO and is responsible for compliance with the GDPR.

1.1 Key Definitions
The GDPR contains a number of key definitions which are referenced in this policy such as 'personal data', 'processing' and 'Data Controller'. Those definitions are set out in Annex A.

1.2 Purpose and Objectives of Policy
This policy sets out Marantec UK's commitment to comply with the the General Data Protection Regulation ('the GDPR').

1.3 Scope and Status of the Policy
This policy applies to all staff who use or process any personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for Marantec UK's purposes. Further, the policy applies to all personal data or special category data held in any form whether manual paper records or electronic records.

2. Roles and Responsibilities

Board of Directors
The Board of Directors is responsible for approval of the Policy and for strategic level implementation of the policy and oversight of compliance with the policy.

Privacy Officer

Marantec UK's Privacy Officer is primarily responsible for advising on and assessing the Company's compliance with the GDPR and making recommendations to improve practice in this area. Further, the Privacy Officer acts as the primary point of contact for GDPR matters and for providing advice, support and guidance in relation to day-to-day data protection matters.

All staff
All staff, including permanent staff, contractors and temporary workers must comply with this Policy and the GDPR whenever processing personal data held by the Company or on behalf of the Company.

Contractors and Consultants

Third parties such as consultants, contractors or agents, undertaking work on behalf of the Company involving personal data, must adhere to the Company's Data Protection Policy and comply with the GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy and GDPR.

3. Compliance with the GDPR

3.1 Awareness & Capability

The Company will implement, and monitor completion of mandatory Data Protection training for all staff. The content of that training will be reviewed annually.

3.2 Privacy By Design

The Company will implement a Privacy By Design Approach to processing personal data through integrating Privacy Impact Assessments into business processes and projects.

3.3 Security
The Company will protect the security of personal data by maintaining, and monitoring compliance with the Company's Information Security Policy and Information Classification Scheme.

3.4 Record Keeping & Retention
The Company will maintain a Records Retention and Disposal Schedule setting the periods for which records containing personal data are to be retained.

3.5 External Contractors and International Transfers

The Company will enter into legally binding contracts with external bodies where those bodies are engaged to process personal data on our behalf. The Company will implement adequacy arrangements where transferring any personal data outside of the European Union.

3.6 Other Third Party Access
The Company will only disclose personal data to third parties such as the police, central government, pension and insurance providers where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

3.7 Internal Sharing
The Company will seek to ensure that personal data is only shared across different departments where those areas have a business need for accessing that data.

4 Data Subjects Rights
The Company will comply with requests from an individual to exercise their rights under the GDPR. All individuals have the right to be informed what information the Company holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to submit a Subject Access Request should complete the form available on the website. Under GDPR, individuals also have the following rights in relation to their personal data:

- The right to request their personal data is rectified if inaccurate

- The right to request erasure of their personal data

- The right to request that the processing of their personal data is restricted

- The right of portability in relation to their personal data

- Rights related to automated decision making or profiling

Individuals who wish to exercise the above rights should contact the Company's Privacy Officer via legal@linkcontrols.co.uk. Individuals should submit their request in writing and specify exactly what personal data and/or processing they are referring to and which right they wish to exercise. If you are seeking access to your personal data (i.e. making a 'Subject Access Request') then you may find it helpful to complete the Company's Subject Access Request Form and send this to the Privacy Officer.

Any staff member who receives a Subject Access Request or a request from an individual to exercise the above rights under GDPR should forward them to the Privacy Officer immediately. All staff are responsible for cooperating with the Privacy Officer to ensure that the Company can comply with an individual's request under the GDPR within the statutory timescales.

5. Own Personal Data

All staff are responsible for checking that information they provide to the Company in connection with their employment is accurate and up to date. Any changes to personal data provided (e.g. change of address) must be promptly notified, in writing, to the Company. The Company cannot be held responsible for errors unless the member of staff has properly informed the Company about them.

6. Personal Data Breaches

The Company will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether;

- The breach should or must be reported to the ICO

- Data subjects should or must be made aware of the breach

- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspects an actual or potential personal data breach has occurred must immediately notify the Privacy Officer. All staff are responsible for fully engaging and cooperating with the Privacy Officer in relation to their investigation of a personal data breach.

7. Compliance

Compliance with this Policy and the GDPR is the responsibility of all members of staff. Employees must comply with the rules and procedures made by the Company. Any breach of the policy by a member of staff may result in disciplinary action. Any breach of the GDPR by the Company may result in a substantial fine or actions imposed upon the Company by the ICO.

8. Further Information

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Privacy Officer: legal@linkcontrols.co.uk. Any individual who considers that the Policy has not been followed in respect of personal data about themselves should also raise the matter with the Company's Privacy Officer. Further information about the GDPR can be found on the Information Commissioner's Office (ICO website). Further guidance for staff can be obtained by contacting the Privacy Officer.

APPENDIX A

KEY DEFINITIONS

1. 'Personal Data' means data which relate to a living individual who can be identified from those data or 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 IP addresses and 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.

2. 'Special category data' which means any personal data information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.

3. 'Processing' means any operations or set of operations which is performed on personal data whether or not by automated means such as collection, use, disclosure or storage of personal data etc.

4. 'Data Controller' means the organisation which, either alone or jointly with another organisation, determines the manner and purpose of the processing of personal data. The Data Controller is responsible for compliance with the GDPR.

5. 'Data Processor' means an organisation (such as a contractor) which processes personal data on behalf of a Data Controller.

6. 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.