

MARCOM

Client, Customer & Service Users - Privacy Notice

MARCOM is an ICT, Defence & Technology Company which is committed to ensuring that the Personal Data of our Clients, Customers & Service Users is processed fairly and lawfully, is accurate, is kept securely and is retained for no longer than is necessary.

The guidelines that we follow are contained in our “Data Protection Policy” which is available on request to Clients.

As an ICT Contractor we are extremely conscious of the very high levels of Customer & Client Data, including “sensitive information”, that we have access to or manage on your behalf. All members of our team who can access your data, have qualified as MoD Security Officers and the Technical Director has completed training at GCHQ and the MoD Cyber Essentials Training Course. Ensuring the safety and integrity of your data and helping you minimise risk is integral to what we do.

This “Privacy Notice” sets out what data we collect or access, how we process it and who we may share it with and why.

It also explains your rights with respect to the Personal Data that we may collect from you; that is data that identifies you as an individual or from which you may be identified.

Why do we need this Privacy Notice & Data Protection Policy?

On the 25th May 2018 the General Data Protection Regulation (GDPR) will come into force and the current Data Protection Act (DPA) 1998 will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

This new regulation is intended to better protect individuals by ensuring that Companies, Public Authorities, Charities etc. look after your data properly and within clear guidelines. You may see the term “Data Subject”, this refers to someone whose information or data is held by an organisation.

Who are we?

MARCOM Defence

MARCOM Defence, 3A Chapel St, Chichester, West Sussex, PO19 1BU trading as “MARCOM *Defence*”, “MARCOM *Computing*” & “MARCOM *Technologies*”, for simplicity the Company will be referred to as “MARCOM” in the remainder of this document.

Who in the Company is responsible for ensuring that we meet our obligations for data protection?

The responsible person is called the “**Data Controller**” (DC) and is registered with the “**Information Commissioner’s Office**” (ICO) – the ICO is the Regulator in the UK for Data Protection. Our Registration No. is Z9534825, you can check our details on the ICO’s website: <https://ico.org.uk/esdwebpages/search> and enter our postcode or company name.

The Data Controller is Miss J Schofield and she can be contacted as follows:

By Email: jennifer@marcomdef.co.uk

Or in writing to:

The Data Controller, MARCOM *Defence*, 3A Chapel St, Chichester, West Sussex, PO19 1BU.

Why do we need to hold and process your personal data?

To meet our contractual obligations as an ICT Contractor we may have access to your systems and the data contained therein as follows:

- By remote access.
- By physically visiting your site(s), home or business whether attended or unattended (as a key holder).
- By hosting your data on our Servers or in our Cloud Services.
- Through managing your ICT infrastructure.
- By managing data and access on your behalf on Third Party platforms.
- During maintenance of your equipment and devices in our workshops or on site.
- In providing WEEE services to you or your organisation.
- By managing email services on your behalf.
- When your Organisation has outsourced Data Protection Officer (DPO) services to MARCOM.
- When we provide data monitoring services to your Organisation.
- When you are using equipment supplied by us that we have designed, modified or programmed to harvest data as part of our contractual arrangements.
- When assisting Customers, Clients and their Staff to resolve technical issues.
- When providing data back-up services.

We very much value our relationship with our Customers and Clients, many of whom are referrals and regular users of our services, we would like from time-to-time to keep you in touch with developments in the ICT world and advise you of any special offers that we have. To do this we like to keep your contact details to stay in touch, normally by Email but occasionally by telephone. **However, we will not do this without seeking your express consent.**

MARCOM may also process personal data if at least one of the following applies:

- In order to protect the vital interests of an individual.
- There is explicit consent.
- For financial transactions relating to MARCOM's Services.
- For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- For reasons of public interest in the area of public health
- For reasons of substantial public interest, based on law, which is proportionate in the circumstances and which provides measures to safeguard the fundamental rights and the interests of the Data Subject.
- To ensure compliance with the legal restrictions placed on the use of our systems and platforms.

What sort of personal information could we be collecting about you and processing?

The categories of information that we collect, process and hold may include:

- Personal information (such as name, address, phone number(s), email address(es)).
- Credit or Debit Card information.
- Date of Birth.
- Log-in Details and Passwords for Accounts.
- Details of other Service Suppliers such as ISPs.
- Client referral information.
- IP Addresses.
- Equipment MAC Codes.
- Data usage and URL's visited.
- Website Registration information.
- Location & Positional information.
- Back-up Data created when providing support services – retained until Client satisfied with restored data integrity.

Some Clients & Customers voluntarily provide sensitive medical information to us to permit the supply of specialist or adapted equipment or software; this information is kept securely and only shared with key Staff and its use is restricted to:

- Assisting those with disabilities or difficulties to enjoy a better quality of life.
- Ensuring the suitability of the services that we provide.

- Enabling the provision of additional assistance where necessary.
- Protecting vulnerable individuals.

Where we supply and install CCTV for a Client or Customer we do not access stored information for any purpose other than the assistance of crime investigation. Passwords are always changed from the manufacturer's default to reduce the potential for hacking or unauthorised viewing. We advise clients on the need for signage alerting Customers to the presence of such equipment in public areas.

Do we pass or share your personal information with anyone else?

We will not give your information or personal details to anyone outside MARCOM other than those listed below without your consent, unless we are required by the law to do so.

We routinely share limited information (only when required by our contract with you) with the following, who are controlled by specific Data Processing Agreements (DPAs) which limits the extent to which they may use and process your data to the purposes that we have agreed:

- Exa networks
- ISPs
- Nominet

How long will we retain your data?

Some data such as records of financial transactions will be kept for seven years for audit and tax purposes, other data is held no longer than deemed necessary.

At MARCOM our principle is not to retain any data or personal information for longer than is necessary in relation to the purposes for which it was collected. We will always be driven by best practice to ensure that Information will be held in accordance with the latest guidelines.

What are my rights regarding the data you hold about me?

Under GDPR (the new regulation) you have significantly enhanced rights which include:

1. Being informed of data processing (which is covered by this Privacy Notice).
2. Accessing information (also known as a Subject Access Request (SAR)) that we hold on you. In some circumstances there can be a charge for this.
3. Having inaccuracies corrected promptly.
4. Having information that we hold about you erased except where there is a statutory or legal requirement for us to collect process or hold it.
5. Restricting processing of your data except where there is a contractual, statutory or legal requirement to process it.
6. Data portability where relevant.
7. Intervention in respect of automated decision making (automated decision making is used only to a limited extent by MARCOM primarily in Network monitoring and to the extent only that IP addresses, MAC Codes & Device Names / Types may be captured).
8. Withdrawing consent (see below)
9. Complaining to the Information Commissioner's Office (ICO) (See below)

Can I stop you holding and processing my data?

Withdrawal of Consent

The lawful basis upon which MARCOM processes personal data is that it is necessary in order to comply with our legal and contractual obligations.

Where MARCOM processes personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

To exercise any of these rights you must in the first instance contact the Data Controller (DC) in writing or by email at the addresses on Page 1.

If you are unhappy with the way your request has been handled, you may wish to ask for a review of the DCs decision by challenging it in writing within 28 days.

Complaints to the ICO

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally the ICO cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Should you have any queries regarding our Data Protection Policies or Procedures please do not hesitate to contact us.