MECsafe Limited

Data Protection Policy

Revision 1
May 2018

Contents

Context and overview

Key details

* **Policy prepared by:** Oliver Stanser
* **Next review date:** May 25th 2019

Introduction

MECsafe Limited are strongly committed to protecting privacy. This Privacy Policy tells you how we use the personal information that we gather from you, or that you provide to us.

MECsafe Limited needs to gather and use certain information about individuals.
These can include clients and delegates, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures MECsafe Limited:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations — including MECsafe Limited— must collect, handle and store personal information. This will be superseded by the GDPR (General Data Protection Regulation) on 25th May 2018.

These rules apply to personal and/or sensitive personal data, regardless of whether the data is stored electronically or on paper.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR states that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

People, risks and responsibilities

Policy scope

This policy applies to:

1. All staff of MECsafe Limited
2. All contractors, suppliers and other people working on behalf of MECsafe Limited

It applies to all data that the company holds relating to identifiable individuals. The personal data that we may hold includes:

- Names of individuals
- Postal (work) addresses
- Email addresses
- Telephone numbers
- National Insurance Numbers
- Qualifications
- …plus any other information relating to individuals that may be required for them to undertake training with us, such as dietary requirements.

Data protection risks

This policy helps to protect MECsafe Limited from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to personal data.

Responsibilities

Everyone who works for or with MECsafe Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Every employee who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The people listed below have key areas of responsibility:

The Managing Director, Oliver Stanser, is ultimately responsible for ensuring that MECsafe Limited meets its legal obligations.

The Managing Director is responsible for:

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data MECsafe Limited holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- MECsafe Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines in this document.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- If emails are accessed via a device such as a smartphone or tablet, the device should be protected by a passcode and have up to date Malware/Antivirus installed.
- All employees are issued with a copy of our Data Protection Policy which must be read and acknowledged as part of their induction process.

Data

Data Storage

These rules describe how and where data should be safely stored.

Electronic Data –
MECsafe Limited store all data on a secure server protected by a watchguard T30 (firewall / router).

Paper Data

When data is stored on paper, it is kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out.

Staff members must ensure that:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (such as a USB stick or memory card), these should be kept locked away securely when not being used, and the files on these sticks should be encrypted.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be in a secure location, away from general office space.
- Data should be backed up frequently.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- If paper copies of documents containing personal data are to be taken off-site, the documents must be stored in a locked briefcase and not left unattended.

Data Use

MECsafe Limited need to collect a certain amount of personal data in order to provide services to clients. It is necessary to share some of this information with external organisations who are providing these services with MECsafe Limited or on our behalf.

However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Sharing

In order to provide a service, MECsafe Limited needs to share certain personal information with third parties. This information can include:

- Name
- Job title
- Place of work
- Email address
- Telephone number
- Qualifications
- Dietary requirements

Data sharing agreements are either in place, or in the process of being implemented with all of our third party suppliers. This ensures that they work to the same strict guidelines with regards to protecting personal data as MECsafe Limited.

All information that is passed onto third parties is done so electronically. This is done via encrypted email.

Data accuracy

The law requires MECsafe Limited to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Managing Directors responsibility to ensure email marketing databases are updated with the 'Constant Contact', 'unsubscribe' data prior to each email campaign.

Data Breach

MECsafe Limited holds very little information which could place individuals at risk in the event of a data breach. However, should there be a breach, the people involved will be informed urgently along with notification of any potential risk. In the event of a serious breach which could result in fraud being committed, or if the publication of the data could cause extreme distress or embarrassment, this would be reported to the Information Commissioner's Office (ICO) in accordance with the law.

Data Retention

For delegates who undertake training with MECsafe Limited, this data will be retained indefinitely for statistical purposes and for operational reasons, for example if we need to evidence training for a delegate's continuing professional development. The data will be retained under 'legitimate interest' and delegates will be informed of this. However at the time of booking the delegate will have the option to ensure this data is destroyed in a timely way, for example after a qualification or certification has been issued.

If a delegate requests that their data is to be destroyed, this will be added to our 'destroyed data log' sheet. This log will contain the delegate name, the date and method that the request was made, and the date that we actually deleted their information from all sources.

Consent

Obtaining consent and customer information

MECsafe Limited will ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

All of our communications contain statements advising customers why we need their information, and what we will do with it.

In order to be GDPR compliant, all of MECsafe Limited's forms will contain a simplified version of our privacy notice to offer clarity to our delegates. These forms include:

- Booking forms
- Post-course questionnaires
- Pre-coursework
- Exam registration forms

MECsafe Limited also has a comprehensive Privacy Policy, setting out how data relating to individuals is used by the company. This privacy statement forms appendix 1 of this document.

Subject access requests

All individuals who are the subject of personal data held by MECsafe Limited are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at info@mecsafe.co.uk

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosure

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, MECsafe Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

Any questions relating to the content of this document should be addressed to:

Oliver Stanser
Managing Director
MECsafe Limited
Unit 9
Snape Lane
Harworth
DN11 8SP

Appendix 1

MECsafe Limited

Privacy Policy

Revision 1

May 2018

MECsafe Limited considers data protection and security seriously and fully complies with the United Kingdom Data Protection Act of 1998.

MECsafe Limited are strongly committed to protecting privacy. This Privacy Policy tells you how we use the personal information that we gather from you, or that you provide to us.

Information We Collect

In order to provide you with our services, we need to collect some personal information from you. This is collected in a number of ways:

- through forms on our website
- if you make an enquiry or booking for one of our training courses via telephone, or email
- via a referral from your line manager or a nominated person within your organisation
- when you communicate with us for any reason, including by email, postal mail or telephone.

If your or your nominated representative provide information to us, MECsafe Limited consider this to be confirmation of your consent to us, in order that we may use that information to provide a service to you.

Use of Cookies

We use cookies to enable you to navigate more easily around our website and to gather analytics information. We use Google analytics within our websites to monitor how our visitors use it and how they found it. This is done so that we can see total (not individual) statistics on which content users access most frequently. The cookies also tell us if you have visited the site before and how many individual users our website has. This does not constitute personal data as we cannot identify individuals
– the data is used for statistical purposes only.

This information helps us to make our website more engaging and allows us to tailor our content to suit our audience.

Occasionally we may have links to other relevant websites and/or social media on our website. These services may leave cookies on your computer when you use them, especially if you are already logged in to their service. MECsafe Limited cannot access these cookies nor control their use. Similarly, these 3rd party services cannot access MECsafe Limited's session or analytics cookies.

If you do not wish to accept cookies, you can set your own cookie preferences on your computer.

Use of Your Information

The information that we collect and store about you is used only to help us provide services to you and to enable us to communicate about subjects of legitimate interest with you.

Storing Your Personal Data

The personal information you provided to us is stored electronically on our server and CRM and on paper copies at the MECsafe Limited head office.

Paper files containing personal information are kept securely in a locked filing cabinet and/or locked archive area at MECsafe Limited head office. Only authorised personnel are entitled to access these files.

We will store this data indefinitely for statistical purposes and to inform you of any relevant updates or courses which relate to your continuing professional development (CPD).

If you do not want us to store this data for these reasons, please tell us.

Please note that the transmission of information via the internet (including email) is not completely secure and therefore, although we try our best to protect the personal information you provide to us, we cannot guarantee the security of data sent to us electronically and the transmission of such data is therefore entirely at your own risk.

Disclosing Your Information

We may need to disclose your personal information to:

- any third party we contract to act on our behalf, including contractors who are providing a training course on our behalf
- professional organisations who are responsible for issuing an accreditation for your completed training
- partners with whom we work to provide services
- any law enforcement agency, court, regulator, government authority or other third party where it is necessary to comply with a legal or regulatory obligation, or otherwise to protect our rights or the rights of any third party
- we will never supply your data to any third party organisation for marketing purposes.

When we do share your information with other parties, we will do so in a manner which complies with the GDPR. This means we will:

- have data sharing agreements in place with all third parties, and ensure that they have mechanisms in place to comply with GDPR and keep your data safe
- Only share information which is relevant to the service we are providing, for example we would not share dietary requirements unless it is a training event where lunch is provided.

Third Party Links

You might find links to third party websites on our website or within the documentation we provide to you.

If you access other websites using the links provided, the operators of these sites may collect information from you which will be used by them in accordance with their own privacy policies which you should review.

We cannot accept any responsibility or liability for their policies as we have no control over them.

Social Networking

The website allows you to share or follow information about us such as blogs and special offers using third party social networking (ie "share this", "like" or "follow" buttons).

We offer this as part of our marketing strategy to generate interest in MECsafe Limited. Sharing personal or non-personal information with a social network may result in that information being collected by the social network provider and being made visible to the public, including through Internet search engines.

Please note that we do not endorse any social networking platforms, nor do we control their policies or practices.

You should always read the privacy policy of any social network through which you share information carefully in order to understand their specific privacy and the way they use your information. It is advisable to set your own preferences on how your information can be viewed on social networks.

Internet-based Transfers

The internet is of course a global digital environment, therefore, using the Internet to collect and process personal information may involve transmitting this personal information on an international basis. If you browse our website and enter into any electronic communication with us, you acknowledge that we process personal information in this way. However, we will endeavour to protect all personal information collected through our website in order to comply with strict data protection standards.

Access to Information

Should you wish to access or update the personal information that we hold about you, please contact us using the contact details below.

Contacting Us

Please get in touch if you have any queries, comments or requests about this privacy policy. You can call us on 01302 775900 or email info@mecsafe.co.uk

Your Consent

By using our website or services, you consent to the collection and use of information as outlined in within this document.

Changes to the Privacy Policy

We may change this Privacy Policy from time to time by updating this document. The online version is available at: www.mecsafe.co.uk

Please come back and check this page occasionally to ensure that you are happy with any changes.