

# Midcam Engineering Ltd.

## DATA PROTECTION POLICY

### Purpose and Background

Midcam Engineering Ltd holds information about employees and other people involved with our activities. The Company has a responsibility to look after this information properly, and to comply with the Data Protection Act. The UK Act will be replaced by the EU General Data Protection Regulation (GDPR) from 25<sup>th</sup> May 2018. It is likely that the GDPR will continue to form the basis of our Data Protection legislation, even once the UK has left the EU, so it is fully taken into account in this policy.

### Scope

This policy applies to information relating to identifiable individuals which is held by Midcam Engineering Ltd

### Our legal basis for using people's data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, even deleting it – will have an acceptable legal basis. There are six of these:

Consent from the individual (or someone authorised to consent on their behalf).

Where it is *necessary* in connection with a contract between our Company and the individual.

Where it is *necessary* because of a legal obligation.

Where it is *necessary* in an emergency, to protect an individual's 'vital interests'.

Where it involves the exercise of a public function – i.e. most activities of most government, local government and other public bodies.

Where it is *necessary* in our legitimate interests, as long as these are not outweighed by the interests of the individual.

Where we are basing our processing on consent we will be able to 'demonstrate' that we hold consent. This means having a record of who gave consent, when they gave it, how they gave it (e.g. on the website, on a form, verbally) and what they actually consented to.

In the case of legitimate interests we will do a balancing test, and be confident that our legitimate interests in using the data in a particular way are not over-riden by the interests of the individual.

### Data Protection Principles

Data Protection compliance is based largely on a set of Principles.

The six GDPR Principles say that:

Whatever you do with people's information has to be fair and legal. This includes making sure that they know what you are doing with the information about them.

When you obtain information you must be clear why you are obtaining it, and must then use it only for the original purpose(s).

You must hold the right information for your purposes: it must be adequate, relevant and limited to what is necessary.

Your information must be accurate and, where necessary, up to date.

You must not hold information longer than necessary.

You must have appropriate security to prevent your information being lost, damaged, or getting into the wrong hands.

Our policy sections below reflect each of these principles in a bit more detail.

Continued....

## **Transparency & purposes (first and second Principles)**

We will make key information available to people at the time we collect information from them. This includes:

the identity and contact details of our Company and the person who is responsible for Data Protection;  
the purposes we intend to use the data for and our 'legal basis' for this (see above);  
what we regard as our 'legitimate interests', if this is our basis for processing;  
any specific recipients of the data or categories of recipients.

Other information will be made available where relevant. This includes:

the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

details of the individual's rights, such as to request a copy of all the data held;

the right to withdraw consent if that is the legal basis for processing (but not retrospectively);

whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

In both cases, we will only tell people things they won't already know. When an employee joins our Company they know that we will keep a record about them and their activities with us.

Any **direct marketing** that we may want to carry out (see below), or any additional purpose(s) that we might use the data for – publicity, perhaps. ('Data' can include photos, videos, CCTV, audio recordings, etc, not just written records.)

## **Direct marketing**

One explicit right that people have is to stop us sending them marketing material (by post, phone, email or text) if they don't want it.

When we collect information from people that might be used for marketing we will say so at the time and ask them if they are happy to hear from us. The wording will be along the lines of: "We would like to keep you up to date with information about opportunities and events within Midcam Engineering Ltd. Please tick here to indicate which method(s) you are happy for us to use: Mail o, Phone o, Email o, Text o"

These rules are only for marketing. They do not stop us from contacting people in whatever is the most convenient way to give them information about things such as purchase orders, or for other administrative purposes.

## **Data quality, record keeping and retention (third, fourth and fifth principles)**

Our activities will be more effective and appropriate if we have good quality records about the people we are working for and with. GDPR insists on this. We will ensure we have the information we need, but no more (it must be adequate, relevant and limited to what is necessary) and it will be as accurate as we can make it and – where necessary – kept as up to date as possible. We will not keep it longer than necessary.

We will remind our staff that the individual concerned has the right to see all the information recorded about them by the Company. While Data Protection concerns should never prevent us from recording the information we believe we need (especially in cases relating to serious misbehaviour). This can be a useful discipline in deciding what to record and how to record it.

Our Company will also have a clear policy on how long to keep information. We will draw up a retention schedule, taking each type of record we hold and specifying how long we normally keep it, and our justification for this. We will set up a process for ensuring that data is deleted or destroyed routinely at the appropriate time.

You have the right to request see the personal information we hold on you and that we rectify or delete the personal data or restrict the processing of your personal data, if you think they are inaccurate. Furthermore, you have the right to object against the processing based on our legitimate interests as a legal basis. We are required to assess and act on your request. Please contact us at [sales@midcamengineering.co.uk](mailto:sales@midcamengineering.co.uk).

Additionally, you also have the right to data portability if it should become relevant. You have a right to lodge a complaint with your local supervisory authority.

Continued...

## **Security (sixth principle)**

We will take good care of the information we hold, whether on computer or on paper, and make sure that we have provided guidance and training to our staff so that they treat the information appropriately.

In particular we will think about the risks when data is 'in transit' – either on portable devices or when it is being sent out. For example:

If people are using their personal phone, laptop, camera or other device for our Company's purposes there will be clear expectations of how they should be secured.

When sending information, particularly by email, we will take steps to prevent confidential information being sent to the wrong person. For example, by using password-protected documents and sending the password in a separate email.

We will also take care not to disclose people's email addresses or other information inappropriately by carelessly copying in a large number of people or forwarding an email that has been copied widely.

Information on paper will not be left lying around, and will only be taken out of a secure location when this is really necessary.

Where information is processed for us externally we will expect the external organisation to be able to give us satisfactory guarantees about the security measures they take.

## **Responsibilities**

Responsibility for compliance with Data Protection lies with the organisation, not with any specific individual. The Directors will be responsible to keep up to date with any developments, to check that we are complying and have the evidence to prove it, to give advice to staff and to handle any issues such as a data breach or a Subject Access Request. The Directors may designate someone to be the lead person.

We will notify the Directors in the event of a serious issue eg a data breach.

When we work in collaboration with other organisations we will sort out clearly (and in writing) who is responsible for what, in order that there are no Data Protection gaps.

If we engage external suppliers to handle data for us in any way, our contract will set out their responsibilities to handle data in a way that will not cause us to be in breach.

Any queries regarding this policy can be made in writing to:

Midcam Engineering Ltd. Unit 4, Redbrook Business Park, Wilthorpe Road, Barnsley S75 1JN

Document created 04/05/18