DATA PROTECTION POLICY

In compliance with the EU General Data Protection Regulation, in force from 25 May 2018

Version 1 - May 23, 2018

*Multimatic Data Protection Policy

Introduction

The protection of personal data is important to Multimatic.

We collect and process information about individuals (personal data) for business purposes, including employment and HR administration, provision of our goods and services, marketing and business administration. This includes personal data relating to our employees, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure and the rights of individuals are respected. This Data Protection Policy (this Policy) explains our obligations in relation to personal data, how we keep it secure and what we expect from you when you are handling personal data in the course of your work.

If you routinely handle personal data, you will be given specific training and instructions regarding data protection procedures in relation to your particular function/department. This training and instructions will supplement your obligations as set out in this Policy.

This Policy applies from 25 May 2018, when the EU General Data Protection Regulation (GDPR) comes into force. It does not form part of your contract of employment or other contract to provide work or service for Multimatic, and does not give you any contractual rights. We may update this Policy at any time.

Who does this Policy apply to?

This Policy applies to all Multimatic employees, contractors, agency workers, consultants, interns, volunteers and other types of workers (together referred to as 'Employees' or 'you').

Who is responsible for data protection at Multimatic?

Multimatic is the "controller" for purposes of data protection law. This means that we are responsible for deciding how we hold and use personal data about you, including the way in which any personal data is processed. 'Processing' personal data means any activity that involves the use of personal data (e.g. obtaining, recording, holding, amending, retrieving, using, disclosing, sharing, erasing or destroying personal data). It also includes sending or transferring personal data to third parties.

We do not have an appointed Data Protection Officer, and are not obligated to appoint one.

* For the purpose of this Policy, "Multimatic" means each of Multimatic Ltd. (UK), Multimatic CFT Limited (UK), MTCE Limited (UK), Multimatic Marketing & Service Centre GmbH (Germany), Multimatic Engineering Prague s.r.o. (Czech Republic) and their respective divisions, branches and offices. To the extent any personal data is shared with the Multimatic Corporate Office (Multimatic Inc. (Canada)), reference to Multimatic will also include Multimatic Inc.

For purposes of overseeing, advising on, and administering compliance with this Policy and the relevant data protection law/regulations, we will identify a Data Protection Lead within each division or facility, as appropriate. Usually, the Data Protection Lead will be a member of the HR department and will be the first point of contact on issues relating to data protection.

This Policy also covers how the Multimatic Corporate Office (Multimatic Inc.) holds and uses any personal data about you that we share with them. The Multimatic Corporate Office is based in Canada, outside the European Economic Area (EEA), but it applies the same high standards to data protection compliance as the EEA. The European Commission has issued a decision confirming that Canada provides an equivalent level of protection to personal data.

All Employees at Multimatic have some responsibility for ensuring that personal data is kept secure and processed in a lawful manner. However, certain Employees will have particular responsibilities in relation to processing personal data and may receive specific instructions and training in respect thereof.

If you are in any doubt about how you should handle personal data, or if you have any concerns or questions in relation to the operation (or suspected breaches) of this Policy, please should seek advice from the HR manager/department for your respective division, branch or office, as set out below.

For Multimatic Ltd (including EU-Matic):-

Unit 40000
Herald Avenue
Coventry
CV5 6UB
email: euhr@multimatic.com

For Multimatic CFT Limited:-

Gateway 11 Business Park
Copper Smith Way
Wymondham, Norfolk
NR18 0WY
email: MCFTHR@cftech.co.uk

For MTCE Limited (including Multimatic Niche Vehicles Europe, Multimatic Niche Products, Selective Pre-Preg (SPP) and Multimatic Motorsports Europe): -

20 Fison Way
Thetford
IP24 1HJ
email: mtcehr@multimatic.com

For Multimatic Marketing & Service Center GmbH:-

Amsterdamerstrasse 192
50735 Köln
email: HR_MPSC@multimatic.com

For Multimatic Engineering Prague s.r.o.:-

Šafránkova 1243/3
Stodůlky, 155 00 Prague 5
Czech Republic
email: HR_MEP@multimatic.com

If you have any questions or concerns about how your personal data is being used by the Multimatic Corporate Office in Canada, please contact HR@multimatic.com.

Why is data protection compliance important?

Failure to comply with data protection law may expose Multimatic and, in some cases, individual Employees to serious legal liabilities. These can include criminal offences and fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from us in the courts if we breach their rights under data protection law. Breaches of data protection law can also lead to serious damage to our brand and reputation.

In addition to the legal liabilities, failure to comply with your obligations under this Policy could lead to disciplinary action, up to and including the termination of your employment.

What is personal data?

Personal data means any information about a living natural person that makes that person identifiable. We hold and use various types of personal data about you. This may include (but is not limited to):

- **identification information** (e.g. name, ID card, national identification/insurance numbers or equivalent (as applicable) and passport numbers, nationality, place and date of birth, gender, picture, IP address);
- **contact information** (e.g. postal address and e-mail address, phone numbers);
- **family situation** (e.g. marital status, number of children);
- **tax status** (e.g. tax ID, tax residence);
- **education and employment information** (e.g. places and dates of education, course taken, grades, degrees, designations; recruitment information, details of terms

of employment, performance information, disciplinary and grievance matters)

- **payroll and accounting data** (e.g. pay and benefit details, working hours)
- **security data** (e.g. door access, CCTV, use of computers and other technology)

Data protection law divides personal data into two categories: ordinary personal data and special category data. Any personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life or sexual orientation, or biometric or genetic data that is used to identify an individual is **special category data**. (The rest is **ordinary personal data**).

We hold and use certain sensitive data (special category data) about our Employees, including: sickness absence and medical information; details of time-off taken for family matters which could include information about physical or mental health conditions. Unless there is a legal obligation for us to do so, we currently do not collect or process personal data related to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, sexual life or sexual orientation, or biometric or genetic data. If our policies over these items should change in the future, the changes will comply with applicable data protection laws.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g. structured paper files and archives).

What does 'processing' personal data mean?

'Processing' personal data means any activity that involves the use of personal data (e.g. obtaining, recording, holding, amending, retrieving, using, disclosing, sharing, erasing or destroying personal data). It also includes sending or transferring personal data to third parties.

Data Protection Obligations

Multimatic is responsible for, and must be able to demonstrate compliance with, data protection law. It is, therefore, essential that Employees comply with data protection law and any other Multimatic policies, guidelines or instructions when processing personal data in the course of their employment.

We have set out below the key obligations under data protection law and details of how Employees can comply with these requirements.

1. Process personal data in a fair, lawful and transparent manner

Legal grounds for processing

Data protection law allows us to process personal data only where there are fair and legal grounds which justify using the information.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

- complying with a **legal obligation** (e.g. health and safety or tax laws);
- entering into or performing a **contract with the individual** (e.g. an Employee's employment contract, or a contract for services);
- acting in Multimatic's or a third party's **legitimate interests** (e.g. maintaining records of business activities, monitoring business productivity); or
- Obtaining the **consent** of the individual (e.g. for sending direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, Multimatic must effectively demonstrate that consent has been given.

Multimatic do **not** use consent as a legal ground for processing Employee data unless the specific data processing activities are genuinely optional.

In most cases, consent is also not required for other standard business activities involving use of customer or supplier data. Consent may, however, be needed for activities which are not required to manage the main business relationship, such as direct marketing activities.

Transparency

Data protection law also requires us to process personal data in a transparent manner, by providing individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. For example, we provide information about our processing of Employees' personal data in the Multimatic Employee Privacy Notice.

We will supplement these notices, where appropriate, with reminders or additional information when particular processing activities take place or when it becomes relevant for an individual, (e.g. when he or she signs up for a new service or event).

***What you need to do**:*

By processing personal data only in accordance with your proper job duties and Multimatic's instructions, ordinarily, you will be processing personal data fairly and lawfully.

The standard privacy notices and statements that we issue, for example, to Employees, customers and the public, should normally be sufficient to ensure that individuals have appropriate information about how you are handling their personal data in the course of your employment. However, you should consider whether reminders or additional information may be appropriate at the time specific processing activities take place. This is particularly important if you think that individuals may need further assistance to understand clearly how their data will be used as part of such activities.

Any new forms which collect personal data and any proposed consent wording must be approved in advance by the Data Protection Lead (identified for each Multimatic division, branch or office).

If you have any concerns about the legal grounds for processing personal data or if you are unsure whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), please check with the Data Protection Lead.

2. Take extra care when handling sensitive or special categories of personal data

Some categories of personal data are 'special' because they are particularly sensitive. These include information that reveals details of an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life or sexual orientation; or
- biometric or genetic data (if used to identify that individual)

Where special category personal data is concerned, data protection law requires us to have an additional legal ground to justify using this sensitive information (in addition to one of the legal grounds described in section 1). The appropriate additional legal ground will depend on the circumstances.

Additional legal grounds for processing special category data include the following:

- complying with a legal obligation/exercising a legal right in the field of employment*;
- assessing working capacity (based on expert medical opinion, and subject to obligations of confidentiality)*;

- carrying out equalities monitoring in relation to racial or ethnic origin, religious beliefs, health or sexual orientation*;
- exercising, establishing or defending legal claims*;
- preventing or detecting unlawful acts; or
- explicit consent of the individual. (In addition to the requirements for consent outlined in section 1 above, this requires an express statement from the individual that his or her special category data may be used for the intended purposes.)

** particularly relevant to processing Employee special category personal data*

Unless there is a legal obligation to do so, we currently do not collect or process special category personal data. If this policy should change in the future, any change will be made in compliance with applicable data protection laws.

***What you need to do**:*

If you are handling special category personal data in the course of your employment, you need to take extra care. In particular, you must ensure that:

- any processing activities are strictly in accordance with your proper job duties and Multimatic's instructions;
- there are appropriate legal grounds for processing the data (both the basic grounds under section 1 and the additional grounds under this section 2) which have been assessed for your specific activities;
- individuals have received adequate information about how their data is being handled. In some cases, an existing privacy notice may need to be supplemented with more specific information regarding the special category data (e.g. when Multimatic is managing sickness absence and/or making adjustments to job duties for Employees with disabilities or serious illness, we may provide additional privacy notices to supplement the Employee Privacy Notice);
- you apply additional security and confidentiality measures, taking into account the fact that the loss or misuse of special category data may be greater than with other types of data. See also section 7 below; and
- if you are relying on consent as a legal ground for processing, you obtain the prior approval of the consent wording from the Data Protection Lead.

If you routinely handle special category data as part of your job duties, Multimatic will ordinarily put in place procedures which ensure that your processing activities satisfy the requirements above.

However, if alternative circumstances apply (e.g. you are involved in a new project or are updating an existing system which involves new processing of special category data), please contact the Data Protection Lead to ensure that the correct compliance procedures are followed.

Similarly, if you have any concerns over the legal grounds that apply when you are processing special category data, please contact the Data Protection Lead.

3. Only process personal data for specified, explicit and legitimate purposes

Multimatic will only process personal data in accordance with our legitimate purposes to carry out our business operations and to administer employment and other business relationships.

What you need to do:

You must only use the personal data that you process in the course of your duties for Multimatic's legitimate and authorized purposes. You must not process personal data for any purpose which is unrelated to your proper job duties.

Processing personal data for any unauthorized purposes could result in a breach of data protection law (e.g. using the company contacts database to find out a colleague's home address for private, non-work related purposes). This may have potentially damaging consequences for all concerned, including disciplinary action.

If you need to process personal data for a different purpose than that for which it was originally collected, you must check whether the individuals have been informed. If not, you should consider whether the additional purpose is both legitimate in the context of Multimatic's business activities and compatible with the original purpose.

If in doubt, contact the Data Protection Lead before processing the data for the additional purpose.

4. Make sure that personal data is adequate, relevant and limited to what is necessary for your legitimate purposes

Data protection law requires us to ensure that, when we process personal data, it is adequate, relevant to our purposes and limited to what is necessary for those purposes (also known as 'data minimization'). In other words, we can ask for the information we need for our legitimate business purposes, but we won't ask for more information than we need to carry out our business operations.

5. Keep personal data accurate and (where necessary) up-to-date

Multimatic must take steps to ensure that personal data is accurate and (where necessary) kept up-to-date. For example, we request that Employees provide us with any change in contact details/address or other personal information for HR and payroll purposes.

***What you need to do**:*

When you process individuals' personal data in the course of your employment, you must make reasonable efforts to be accurate and, where necessary, keep the relevant information updated.

When collecting personal data, try to confirm its accuracy at the outset. If you discover any inaccuracies in the personal data that you are handling, these need to be corrected or deleted without delay.

Personal data should be held in as few places as possible, to avoid the risk that duplicate copies are not updated and become out of sync. You should not create additional copies of personal data, but should work from and update a single, secure copy (in accordance with standard Multimatic procedures on retention and storage of records).

6. Keep personal data for no longer than is necessary for the identified purposes

Records containing personal data should only be kept for as long as they are needed for the identified purposes. Multimatic has data retention, storage and deletion policies and internal processes/guidelines regarding various types of company records and information, including records and information that contain personal data.

We take appropriate steps to retain personal data only for so long as is necessary, taking into account the following criteria:

- the amount, nature and sensitivity of the personal data;
- the risk of harm from unauthorized use or disclosure;
- the purpose for which we process the personal data, and how long we need the particular data to achieve this purpose;
- how long the personal data is likely to remain accurate and up-to-date;
- how long the personal data might be relevant to possible future legal claims; and
- applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

***What you need to do**:*

Familiarize yourself with our retention policies, processes and guidelines that are relevant to your job. Ensure that, where it falls within your responsibility, you remove or delete all information that is no longer required to be retained.

If you are not sure what retention guidelines/instructions apply in your role, or how to apply them to a particular type of personal data, please contact the Data Protection Lead for guidance.

7. Take appropriate steps to keep personal data secure

Keeping personal data safe and complying with Multimatic's procedures to protect the confidentiality, integrity and security of personal data is a key responsibility for all Employees.

Multimatic's computer systems, electronic communications systems and software platforms containing personal data have appropriate security measures in place. These security measures consist of a combination of physical, technological and organizational controls, including:

- building security
- information limited to authorized users and subject to password protections
- regular updates of system passwords, controlled by password enforcer software
- confidentiality obligations of Employees
- appropriate firewall, anti-virus and network protections in place, together with regular software updates
- procedures for secure disposals of records and equipment, backups and disaster recovery
- remote working limitations
- protocols on use of technology and data storage
- asset registers

***What you need to do**:*

To assist in maintaining data security and protecting the confidentiality and integrity of the personal data you handle in course of your employment, you must comply with this Policy and Multimatic's instructions regarding the processing and security of personal data.

In particular, you are required to:

- save, store and communicate personal data only within and using authorized Multimatic information and communications systems
- when storing or sending data on company computer systems, ensure that the data is encrypted and password protected, and remains locked when you are away from computer
- not store or send personal data on flash drives, personal devices or using personal communications facilities
- lock hard copy files containing personal data in a secure cabinet
- never leave a laptop (or other device) or any hard copies of documents containing personal data in a public place
- take care when viewing personal data in hard copy or on-screen that such information is not viewed by anyone who does not have the right to that information (especially if viewing the personal data in a public place)
- ensure that information containing personal data is disposed of securely and permanently, using confidential waste disposal or shredding when necessary
- alert the Data Protection Lead to any personal data breaches immediately and in accordance with Multimatic's Data Breach Reporting Policy
- ensure that any sharing or disclosure of personal data is permitted by appropriate legal grounds and, where necessary, with safeguards in place

8. Take extra care when sharing or disclosing personal data

The sharing or disclosure of personal data (for example, to third party service providers) is a type of processing, and therefore all the principles described in this Policy need to be applied.

Internal data sharing

Personal data is only shared internally within Multimatic (including the Multimatic Corporate Office) on a 'need to know' basis.

External data sharing

We only share personal data with third parties where we have a legitimate purpose and an appropriate legal ground under data protection law which permits us to do so. Commonly, this includes situations where we are legally obliged to provide the information (e.g. for tax purposes) or where necessary to perform our contractual duties to individuals.

We may appoint third party service providers (known as processors) who will handle information on our behalf, for example to provide payroll, data storage or other technology services.

Multimatic remains responsible for ensuring that our processors comply with data protection law and this Policy in their handling of personal data. We assess and apply data protection and information security measures prior to, and during, the appointment of a processor. The extent of these measures will vary depending on the nature of the activities, but will include appropriate risk assessments and reviews, as well as contractual obligations.

Details of the recipients or categories of recipients of personal data (including processors and other third parties) should be set out in privacy notices as described in section 1 above.

***What you need to do**:*

You may only share or disclose personal data with an Employee, agent or representative of Multimatic, if the recipient has a job-related need to know the information.

You may only disclose personal data to service providers or other third parties where:

- there is a legitimate purpose and an appropriate legal ground for doing so (e.g. in order to provide a service such as payroll or if we are legally obligated to do so)
- the individuals whose personal data is being shared have been properly informed (e.g. in an appropriate privacy notice)
- Multimatic has checked that the service provider or other third party has adequate security and data protection measures in place, to protect the personal data concerned
- the service provider or other third party has signed a written contract that contains the provisions required by data protection law (unless the Data Protection Lead has specifically determined that this is not required in the context)
- the transfer complies with any overseas transfer restrictions, if applicable

Routine disclosures of personal data to established recipients (e.g. payroll providers or group entities), which form a normal and regular part of your job duties, will ordinarily satisfy the above requirements. You should always ensure you comply with particular Multimatic instructions that apply. However, if you are in any doubt as to whether you can share personal data with anyone else, first contact the Data Protection Lead.

9. Do not transfer personal data to another country unless there are appropriate safeguards in place

An out of country transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise used in, a different country. European Union data protection law restricts, in particular, transfers of personal data to countries outside of the European Economic Area (EEA – i.e. the European Union plus Norway, Liechtenstein and Iceland), to ensure that the level of personal data protection is not compromised.

Multimatic assess the risks of any transfer of personal data outside of the EEA (taking into account the principles in this Policy, as well as the restrictions on transfers outside the EEA) and puts in place additional safeguards where required.

We currently transfer some of your personal data to the following country outside the EEA: Canad**a.** There is an adequacy decision by the European Commission in respect of Canada. This means that Canada is deemed to provide an adequate level of protection for your personal data.

What you need to do:

If you are required to transfer personal data outside of the EEA in the course of your employment, adequate safeguards need to be in place. Where these transfers are a normal and regular part of your job duties, Multimatic's current safeguards provide the required levels of data protection.

However, if you are transferring personal data outside the EEA in unique circumstances (e.g. for a new type of processing or to countries other than Canada), you should contact the Data Protection Lead for further guidance before going processing the transfer.

10. Report any data protection breaches without delay

Multimatic takes any data protection breaches very seriously. Breaches can include, or result from: lost or mislaid equipment or data; use of inaccurate or excessive data; failure to address an individual's rights; accidental sending of data to the wrong person; unauthorised access to, use of or disclosure of data; deliberate attacks on Multimatic's systems; theft of records; and any equivalent breaches by Multimatic's service providers.

Where there has been a breach of security leading to the accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access to personal data, Multimatic will take immediate steps to identify, assess and address the breach, including containing the risks, remedying the breach and notifying appropriate parties (see below). Multimatic has a Data Breach Reporting Policy which sets outs its procedures for identifying, assessing and addressing personal data security breaches.

If Multimatic discovers that there has been a personal data security breach that poses a risk to the rights of individuals, we will report the breach to the relevant supervisory authority within 72 hours of discovery.

If a personal data breach is likely to result in a high risk to the rights of individuals, we will inform the affected individuals about the breach and provide them with information about its likely consequences and the mitigation measures we have taken.

We also keep an internal record of all personal data breaches, regardless of their effect and regardless of whether they were reported to any supervisory authority.

***What you need to do**:*

If you become aware of any breach (or suspected breach) of this Policy (including, specifically, a security breach), you must report it to the Data Protection Lead immediately, and take any other required steps in accordance with our Data Breach Reporting Policy.

11. Do not use profiling or automated decision-making unless you are authorized to do so

Profiling, or automated decision-making, occurs where an individual's personal data is processed and evaluated by automated means, resulting in an important decision being taken in relation to that individual. This manner or processing/evaluation poses potential risks for individuals where a decision is based, in whole or in part, on that profiling or other automated processing.

One example of automated decision-making would be using an online psychometric test to automatically reject job applicants who do not meet a minimum pass mark without any human oversight, such as a review of the test results by a recruiting manager.

Data protection law prohibits decision-making based solely on profiling or other automated processing, except in very limited circumstances. In addition, where profiling or other automated decision-making *is* permitted, safeguards must be put in place, including giving individuals the opportunity to express their point of view and challenge the decision. Multimatic currently do not use profiling or other automated decision-making. In future, if any profiling or other automated decision-making is considered by Multimatic in relation to specified categories of personal data, an assessment will be undertaken for compliance with data protection law requirements and appropriate safeguards will be implemented on a case-by-case basis.

What you need to do:

If you conduct profiling or other automated decision-making in the course of your job responsibilities, you must consult with the Data Protection Lead and seek guidance on any applicable safeguards that must be implemented.

If you are proposing to undertake any new automated decision-making or profiling activities in the course of your employment, please contact the Data Protection Lead who will advise you whether these activities are permitted and the safeguards required to be put in place.

12. Integrate data protection into operations

Data protection law requires Multimatic to build data protection considerations and security measures into all of our operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals. This involves taking into account various factors including:

- the risks (and their likelihood and severity) posed by the processing on the rights and freedoms of individuals;
- technological capabilities;
- the cost of implementation; and
- the nature, scope, context and purposes of the processing of personal data.

We also seek to assess data protection risks regularly throughout the lifecycle of any project or activity which involves the use of personal data.

What you need to do:

If you are involved in the design or implementation of a new project or activity that involves processing personal data, you must give due consideration to all principles of data protection set out in this Policy.

You should assist the Data Protection Lead with regular reviews of projects or activities to ensure data protection risks continue to be addressed.

A useful tool for assessing data protection and privacy considerations is a Data Protection Impact Assessment or 'DPIA'. A DPIA will consider the necessity and proportionality of a processing operation, and assesses the risks to individuals and the measures that can be put in place to mitigate those risks. A DPIA must be carried out if a data processing operation is likely to give rise to a high risk to individual rights and freedoms.

If you are involved in the design or implementation of a new project that involves processing personal data, you must check whether it is necessary to conduct a DPIA or similar risk or compliance assessment by contacting the Data Protection Lead.

The Data Protection Lead will also be able to advise you on how we expect you to conduct, or otherwise contribute to, a DPIA or similar risk assessment.

Individual Rights and Requests

Under data protection law, individuals have certain legal rights when it comes to how we handle their personal data. For example, individuals have the following rights:

- **The right to make a subject access request.** This enables individuals to receive certain information about how we use their personal data, as well as to receive a copy of it and to check that we are lawfully processing it.
- **The right to request that we correct incomplete or inaccurate personal data** that we hold about them.
- **The right to request that we delete or remove personal data** that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below).
- **The right to object to our processing of their personal data** where we are relying on our legitimate interest (or the legitimate interest of a third party) or where we cannot show a compelling reason to continue the processing.

- **The right to request that we restrict our processing of their personal data**. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.

- **The right to withdraw any consent** which they have given.

- **The right to request that we transfer their personal data** to themselves or to another party, in a structured format. This right applies in respect of data that have been provided which is necessary for the performance of a contract or which they have consented to us using.

- **The right to challenge a decision based solely on profiling/automated processing**, to obtain human intervention, and to express their point of view.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one month timeframe.

Individuals also have rights to complain to the relevant supervisory authority on data protection laws, and to take action in court to enforce their rights and seek compensation for, damages suffered from, any breaches.

***What you need to do**:*

If you receive a request from an individual seeking to exercise a right in relation to his or her personal data, or making an inquiry or complaint about our use of such personal data, you must forward the request, inquiry or complaint to the Data Protection Lead immediately. The request, inquiry or complaints needs to be dealt with appropriately and within the applicable time limits, in accordance with this Policy and other Multimatic procedures. Your assistance may be requested to address and respond to the request, inquiry or complaint.

Record Keeping

In order to comply, and demonstrate our compliance, with data protection law, we keep various records of our data processing activities. These include a Record of Processing which must contain, as a minimum: the purpose of the processing; the categories of the data subjects and personal data; the categories of the recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data.

***What you need to do**:*

You must also comply with our applicable processes/guidelines and any specific instructions you are given concerning the keeping of records about our processing of personal data.

If you are processing personal data in the course of your employment and you collect any new types of personal data or undertake any new types of processing activities, either through the introduction of new systems or technology or by amending existing ones, please inform the Data Protection Lead so that we are able to keep our records up-to-date.

Training

We require all Employees to undergo some basic training to enable them to comply with data protection law and this Policy. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, we provide training as part of our induction process for new Employees and operate an ongoing training programme to make sure that Employees' knowledge and understanding of what is necessary for compliance in the context of their employment duties and responsibilities is up-to-date. Attendance at training sessions is generally mandatory and will be recorded.

Departures from this Policy

There are some very limited exemptions from data protection law, which may permit departure from aspects of this Policy in certain circumstances.

You will be given specific instructions if any exemptions are relevant to your functions and responsibilities.

If you think you should be able to depart from this Policy in any circumstances, you must contact the Data Protection Lead before taking any action.

Contact for Questions and Information

If you have any questions relating to this Policy or are need additional information about how you should handle personal data, please contact the following:-

For Multimatic Ltd (including EU-Matic):-

Unit 40000
Herald Avenue
Coventry
CV5 6UB
email: euhr@multimatic.com

For Multimatic CFT Limited:-

Gateway 11 Business Park
Copper Smith Way
Wymondham, Norfolk
NR18 0WY
email: MCFTHR@cftech.co.uk

For MTCE Limited (including Multimatic Niche Vehicles Europe, Multimatic Niche Products, Selective Pre-Preg (SPP) and Multimatic Motorsports Europe): -

20 Fison Way
Thetford
IP24 1HJ
email: mtcehr@multimatic.com

For Multimatic Marketing & Service Center GmbH:-

Amsterdamerstrasse 192
50735 Köln
email: HR_MPSC@multimatic.com

For Multimatic Engineering Prague s.r.o.:-

Šafránkova 1243/3
Stodůlky, 155 00 Prague 5
Czech Republic
email: HR_MEP@multimatic.com

If you have any questions or concerns about how your personal data is being used by the Multimatic Corporate Office in Canada, please contact HR@multimatic.com.

APPENDIX

This Appendix provides more detail about the type of personal data Multimatic holds in relation to Employees, what we use it for, our legal grounds for doing so, who we share it with and how long we keep it.

The specific types of data about Employees that we will hold, use and share will depend on each Employee's role, the terms of employment, individual circumstances and the conditions affecting Multimatic from time to time. For example, if an Employee does not have a work computer or use any other technical device, we will not hold any computer or device usage records; if an Employee does not work for us in a full-time capacity, we will not hold records about rights or benefits that the Employee is not entitled to; if an Employee has not yet taken a day off sick, we will not currently hold any sickness absence records; and we are only likely to share information about the Employee with professional advisers in particular circumstances.

Note also that the first two Tables below divide items of personal data into relatively broad categories (under the headings "Type of ordinary personal data held by us" or "Type of special category personal data held by us"). Where multiple purposes and/or legal grounds for our use of a given "type" of personal data are identified, this does not necessarily mean that *all* of the purposes and/or legal grounds are applicable to *all* items of personal data falling within that "type" of personal data.

More information on ordinary personal data

Type of ordinary personal data held by us	What we use it for	Legal ground	Guideline retention period
Biographical details (including name, title, contact details, date of birth, gender, emergency contacts, photograph)	Administration of the contract, emergency contact details so we can look after your welfare in an emergency, gender for gender pay gap reporting, equal opportunities monitoring, tax/insurance compliance, and pension administration, photograph for identification and on intranet/web to help colleagues/customers/ HR to perform identification.	Legal obligation; Performance of the contract; In our legitimate interest to hold emergency contact details in order to inform a person nominated by you in an emergency situation. In our legitimate interest to use photographs to help colleagues/ customers/ security perform identification	During employment and up to 6 years after employment ends Emergency contacts, photograph: during employment and up to 6 months after employment ends

Recruitment information (including correspondence/ references/ right to work checks and related documents)	Administration of the contract, and to check and demonstrate that you have the legal right to work in the relevant jurisdiction	Legal obligation; Performance of the contract; In our legitimate interest to maintain relevant and appropriate records of recruitment for business management and administration of employment	During employment and up to 6 months after employment ends (Right to work checks - two years after employment ends)
Employment details (including start date, contractual terms, location, job title, career history with Multimatic)	Administration of the contract; Managing our relationship with you on an ongoing basis; Details about roles/experience, etc. May be used in communications with customers and potential customers.	Legal obligation; Performance of the contract; In our legitimate interest to manage our ongoing relationship and to promote our goods/services to customers and potential customers	During employment and up to 6 years after employment ends
Payroll, tax, national identification/insurance details or equivalent (as applicable) and bank details	Paying you, deducting tax and relevant national insurance or equivalent deductions (as applicable), keeping appropriate records	Legal obligation; Performance of the contract	Payroll/tax/national identification/ insurance or equivalent (as applicable): Six years from the end of the financial year in which payments are made Bank details: During employment and up to 6 months after employment ends
Working hours and arrangements	Paying you correctly; Complying with legal requirements regarding working time; Managing attendance, day-to-day operational management and dealing with requests to alter hours	Legal obligation; Performance of the contract; In our legitimate interest to manage working hours/ arrangements to ensure effective business operations	During employment and up to 6 months after employment ends
Pay and benefits including pensions (as applicable) and expenses, as well as information necessary for administration	Providing you with agreed pay, benefits and expenses; making decisions about future compensation; tracking and reviewing pay, benefits, expenses;	Legal obligation; Performance of contract; In our legitimate interest to analyse pay, benefits and	During employment and up to 6 years after employment ends

	making decisions about compensation; auditing and reporting on company financial position	expenses and make decisions about appropriate compensation on an individual and company level	
Performance and career progression (including appraisals, performance management, target/objective setting, consideration of new duties/roles)	Ensuring you perform in accordance you're your employment contract and to the standards we require; considering future duties/roles; setting performance-related objectives; determining eligibility for performance/ discretionary bonuses (if applicable)	Performance of the contract; In our legitimate interest to manage performance and duties/roles to ensure effective business operations and set appropriate levels of remuneration	During employment and up to 6 months after employment ends
Qualifications (including educational, vocational, driving licences where appropriate) and training	Ensuring you are appropriately qualified and trained for current or potential positions	Legal obligation; Performance of the contract; In our legitimate interest to ensure that you have appropriate qualifications and training for current or potential future positions	During employment and up to 6 months after employment ends
Holidays and other time-off	Managing statutory and non-statutory holiday and other time-off	Legal obligation; Performance of contract; In our legitimate interest to ensure holidays are taken at times compatible with our business requirements and that any consequent operational adjustments are made	During employment and up to 6 years after employment ends

Disciplinary, conduct and grievance matters	Investigating and dealing with disciplinary, conduct and grievance matters	Legal obligation; Performance of the contract; In our legitimate interest to deal effectively with disciplinary, conduct or grievance matters; Public interest in detecting or preventing unlawful acts	During employment in accordance with our disciplinary and grievance policies, and up to 6 months after employment ends
Health and safety	Conducting risk assessments; establishing safety measures to mitigate identified risks; providing a safe and healthy working environment; keeping required records	Legal obligation; In our legitimate interest to ensure you are able to perform your duties in a safe and healthy environment for the efficient operation of the business	Decided on a case-by-case basis in accordance with the criteria set out in this Policy, and taking into account any legal requirement to retain particular records
Changing terms of employment or termination of employment	Administration of the contract; making changes to the terms of employment to fit business requirements; managing our relationship with you on an ongoing basis including during notice; promotions, role changes and other career progression; termination of the working relationship whether instigated by us or by you; managing post–employment issues	Legal obligation; Performance of the contract; In our legitimate interest to manage, alter and, where relevant, to terminate the contractual relationship or respond to resignations and to deal effectively with post-employment issues	During employment and up to 6 years after employment ends
CCTV footage	Primarily for security purposes, although we may also use CCTV footage when investigating allegations of misconduct by employees or other wrongful behavior	Legal obligation; Performance of the contract; In our legitimate interest to deal effectively with allegations of misconduct and to maintain the	One year (12 months) from date information is captured

		security of our premises	
Information about Employee's use of business equipment, technology and systems, including our computers/ telephones/mobile phones/ software/ applications/ social media/[door entry systems/clocking in and out systems/time recording/performance output monitoring	Maintaining the operation, security and integrity of our business communications systems (e.g. protection from hackers, malware, etc.); providing IT and communications systems support; preventing excessive personal use; recording communications with customers for quality control and training purposes; keeping premises secure; managing time; recording rate of work/efficiency of work	Performance of the contract; In our legitimate interest to maintain operational security and integrity of communications systems, prevent excessive use of business resources for personal purposes, and monitor and maintain quality of communications with customers; record time worked and rate/efficiency of work	One year (12 months) from date information is captured
Personal data produced by Employee and others in the course of carrying out job (e.g. job-related emails, minutes of meetings, written reports, business social media presence etc.)	Performance of job duties by you and your colleagues; carrying on the business of the company; monitoring your business social media presence to ensure expected standards are complied with	Performance of the contract; In our legitimate interest to carry out the company business	Decided on a case-by-case basis in accordance with the criteria set out in this Policy
Personal data, which may include any of the types of data set out in this Appendix, that is relevant to our strategic decision making processes, to planning business operations, actual and potential legal claims, corporate reporting and business risk analysis	To enable us to carry out the company business, analyse current business performance, plan for the future, present information in reports to relevant audiences such as shareholders, protect the company from legal claims, seek professional advice as and when required in	Legal obligation; Performance of the contract; In our legitimate interest to carry out the company business, including taking strategic decisions in the interest of the business, communicating about the	Decided on a case-by-case basis in accordance with the criteria set out in this Policy

	the course of running our business	business with relevant audiences and seeking professional advice where appropriate	

More information about special category data

Type of special category data held by us	What we use it for	Legal ground	Special category legal ground	Guideline retention period
Sickness absence and medical information (including records relating to absence and its management, information about any medical condition and doctor's reports and notes)	Payment of sick pay (if applicable); providing health insurance and/or managing absence and ensuring appropriate cover; considering how health issues may affect your ability to do your job and considering adjustments, which may involve us seeking medical advice on this; compliance with health and safety requirements	Legal obligation; Performance of the contract; In our legitimate interest to manage Employees with health conditions, maintain a safe and healthy working environment and to manage sickness absence of our workforce and ensure appropriate cover	Legal obligation/right in relation to employment. Assessment of working capacity. In exceptional circumstances, to protect your or someone else's interests, where consent cannot be given	Decided on a case-by-case basis in accordance with the criteria set out in this Policy
Time off taken for family related reasons (which could include information about an Employee's health)	Facilitating the taking of time off for family related matters; managing absences and ensuring appropriate cover	Legal obligation; Performance of the contract; In our legitimate interest to manage absences and ensure appropriate cover	Legal obligation/right in relation to employment Assessment of working capacity	During employment and up to 6 months after employment ends
Equal opportunities and diversity	To monitor equality of opportunity and diversity in our organization; comply with company policies	In our legitimate interest to understand how our organization is doing with regard to diversity and equal opportunities	Public interest in monitoring equal opportunities within the workforce	During employment and up to 6 months after employment ends

Criminal convictions/ offences	When you are working for us, if a criminal conviction comes to light, to investigate and assess the impact, if any, on your continued employment (see Disciplinary policy)	Legal obligations; Performance of the contract; In our legitimate interest to determine whether to employ individuals with criminal convictions in particular roles	You have manifestly made the information public; Establishing, exercising or defending legal claims; Public interest in detecting or preventing unlawful acts	Decided on a case-by-case basis in accordance with the criteria set out in this Policy

Information on retention periods for specific category data can be found in the Multimatic Employee Data Retention Guide document**.**

More information about how we share personal data

Who we share your personal data with	**What data we share**	**Why we share it**	**Legal ground**
Multimatic Corporate Office (Multimatic Inc.) in Canada	Any of your personal data that is relevant	To make business decisions connected with your career, pay and benefits, such as inclusion in the group-wide profit share plan and/or bonus arrangements; Part of the group-wide policies for monitoring individual performance; To manage the company's and the group's business; To monitor company performance; To provide system maintenance, support and hosting of data	Legal obligation; Performance of the contract; In our legitimate interest to manage the business and your performance
Third party service providers: e.g. pension/	Pay, national insurance or equivalent	To enable the service provider to carry out payroll	Performance of contract; In our legitimate

insurance providers, including (as applicable) life insurance, income protection, company vehicle insurance, etc.	identification details, bank details, health and sickness information, drivers licence information	functions, insurance provisions, /IT services; To provide and administer pension/insurance and other benefits (as applicable)	interest to engage appropriate service providers to manage payroll/IT, etc.
Our legal and other professional advisers appointed from time to time	Any of your personal data that is relevant	To obtain legal or other professional advice about matters related to you or in the course of dealing with legal disputes with you or other Employees; to obtain advice on business management and planning, including accounting advice; to independently audit our accounts	Legal obligation; Performance of contract; In our legitimate interest to seek professional advice to clarify our rights/obligations and appropriately defend ourselves from potential claims; to manage the business and its finances. In relation to special category data – legal obligation/right in relation to employment; defending legal claims
Occupational health professionals/medical professionals	Details of your sickness absences, information we already have about your health/medical conditions as relevant	To seek a medical report about you in accordance with our sickness and absence policies; to carry out assessments required by health and safety legislation	Legal obligation; In our legitimate interest to manage sickness, absence and health issues arising in our workforce In relation to special category data – Legal obligation/ right in relation to employment; assessment of working capacity
Tax authorities, Health and Safety authorities	Pay, tax and national identification/ insurance details or	To comply with regulatory and legal obligations	Legal obligation. In relation to special category data – Legal obligation/right in

	equivalent (as applicable); Accident and absence info; name; address; date of birth		relation to employment or social security; defending legal claims
Potential purchasers/new service providers	Any of your personal data that is relevant	To provide relevant information to prospective purchasers or new service providers	Legal obligation; In our legitimate interest to consider/proceed with a transfer/sale of the business or engagement of new service providers
Customers, supplier, potential customers or suppliers, shareholders and other interested parties	Any of your personal data that is relevant, including business contact details, information about your duties/roles and experience	Inclusion in corporate reports, for use in business communications, to obtain security clearance to work on customers' or suppliers' premises, etc.	Legal obligation; In our legitimate interest to communicate about the business and our Employees to appropriate audiences, which include customers, suppliers potential customers and suppliers, shareholders and other interested parties
Third parties at your request	Employment details as relevant	At your request, to provide a reference to a potential new employer/details of your employment to a mortgage company or other credit agency	In our legitimate interest to action your reasonable requests to provide personal data to third parties