GDPR Compliance Policy

Author:	David Finney	Date:	May 2018
Revision:	1	Reviewed:	September 2018
Review Date:	October 2019		

Contents

Introduction

TTC Group is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting.* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, address, email address, driving history/background (including licence details), financial and pay details, education and skills,*

	marital status, relevant medical information, nationality, job title, and CV.
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is The Information Commissioners Office (ICO)

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Data Protection. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our data protection officer (DPO), David Finney has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

David Finney
david.finney@ttc-uk.com
01952 607190

The principles

TTC Group comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Accountability and transparency

We ensure accountability and transparency in all our use of personal data. We show how we comply with each Principle by keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This is kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we demonstrate compliance and we are responsible for understanding our particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

Our procedures

Fair and lawful processing

We process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we do not process personal data unless the individual whose details we are processing has consented to this happening or that we have a contractual or legal obligation to process.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs processing data

TTC Group is classified as a data controller and a data processor. We maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

TTC Group Ltd – **ZA272769**
TTC 2000 Ltd – **ZA020741**
Cycle Experience Ltd – **ZA166005**

As a data processor, we comply with our contractual obligations and act only on the documented instructions of the data controller. As a data processor, we:

- Do not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If there is any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

We establish a lawful basis for processing data and ensure that any data we are responsible for managing has a written lawful basis approved by the DPO. The lawful basis for each of our data assets is documented in order to provide clarity and transparency. At least one of the following conditions applies wherever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**

Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

When making an assessment of the lawful basis, we first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We do not rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This is done via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent clearly identifies what the relevant data is, why it is being processed and to whom it will be disclosed.

Responsibilities

Our responsibilities and objectives

- Analyse and document and classify the type of personal data we hold
- Check procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implement and review procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Fully understand our data protection obligations
- Check that any data processing activities we deal with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause a breach of data protection laws
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Role of the Data Protection Officer

- Keeping the board updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members and those included in this policy
- Answer questions on data protection from staff, board members and other stakeholders
- Respond to individuals such as clients and employees who wish to know which data is being held on them by us
- Check and approve third parties that handle the company's data any contracts or agreement regarding data processing
- Make arrangements to deal with Subject Access Requests
- Report to the ICO when required

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If we believe that information is inaccurate we will make every effort to correct this information with the approval of the data subject or data controller.

Data security

All data is stored securely and in accordance with the ISO 27001 framework to which TTC is certified.

Where other organisations process personal data as a service on our behalf, the relevant due diligence is undertaken to ensure that suitable security is in place relevant to the processing and if any additional, specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it
- Printed data is securely disposed of when it is no longer needed. For more information see - **Data Disposal Policy.**
- Data stored on a computer is protected by strong passwords that are changed regularly. We encourage all staff to use complex passwords which are audited regularly. For further information see – **Password Policy**
- Data stored on portable media must be encrypted or password protected and locked away securely when not being used
- The IT Director must approve any cloud-based storage system used to store data
- Servers containing personal data are kept in a secure location, with access significantly limited
- Data is regularly backed up in line with the company's backup procedures

- Data is not stored directly on mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data are approved and protected by security software
- All possible technical measures within reasonable practicality are put in place to keep data secure

Data retention

We retain personal data for no longer than is necessary. What is necessary will depends on the circumstances of data asset or data subject, taking into account the reasons that the personal data was obtained, and the purpose for processing and whether any legal or contractual obligations are to be me. For further information see – **Data Retention Policy.**

Transferring data

TTC Group will always transfer sensitive data wherever possible using a secure method of transfer, this method will be communicated and arranged with the transferee. We recommend that individuals or third parties use a suitably secure method of transfer when sending data to us. The responsibility of data whilst in transit lies with the sender.

Transferring data internationally

TTC Group do not currently transfer any data outside of the European Economic Area (EEA). Should there be a requirement for TTC to do so, it will only be done subject to a lawfully binding agreement between the parties involved.

Rights of individuals

Individuals have rights to their data which must respected and complied with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Privacy Notices are in place which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- We keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Individuals are able to access their personal data and supplementary information.
- Individuals are made aware of the lawfulness of the processing activities

3. Right to rectification

- Personal data of the individual is rectified or amended if requested by the data subject if it is inaccurate or incomplete.
- This is done without delay, and no later than one month. This can be extended to two months with permission from the DPO and in approval of the data subject.

4. Right to erasure

- We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We will retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- Upon request we will provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We will provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy notices

A privacy notice is supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice will be provided within a reasonable period of having obtained the data, which will mean within one month.

If the data is being used to communicate with the individual, then the privacy notice will be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice will be supplied prior to the data being disclosed.

What is included in our Privacy Notice

Our Privacy Notices are concise, transparent, intelligible and easily accessible. They are provided free of charge and are written in clear and plain language, particularly if aimed at children.

The following information is included in privacy notices to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- Whether the data is shared with a third party and for what reason
- Detailed information of any transfers to third countries and safeguards in place
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The process for a data subject to make a Subject Access Request

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How we deal with subject access requests

We will provide a data subject with a copy of their information upon request, free of charge. This will occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system. If this is not available the transfer of data will be done by a method which is agreed by the data subject.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual will be informed within one month. Approval must be obtained from the DPO before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data,

we can request the individual specify the information they are requesting. This can only be done with permission from the DPO.

Once a subject access request has been made, we will not change or amend any of the data that has been requested. Doing so is a criminal offence.

For further information see – **Subject Access Request Policy**

Data portability requests

We will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We will provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This will be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month.

Right to erasure (right to be forgotten)

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data. If the individual asks, we will inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We will cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We will always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We will offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We will only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we will:

- Give individuals detailed information about the automated processing.
- Advise that they are able to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third parties

Using third party controllers and processors

As a data controller and data processor, we have written contracts in place with third party data controllers and data processors that we use. The contracts contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected. We request completion of a Data Protection Agreement for third parties who process our data. Due diligence is completed for processors who carry out high risk activities as part of their service and we request that they complete a Third Party Data Security Questionnaire prior to the commencement of a service. This questionnaire is reviewed by the DPO, IT Director and supplier relationship managed prior to approval.

As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects. If appropriate, based on the service provision and sensitivity of the data, a Data Processing Agreement will be put in place between the data controller and the data processor.

Data Processing Agreements and Contracts

Our Data Processing Agreements and contracts comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our Data Processing Agreements and contracts include terms that specify:

- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Arrangements for data disposal or return upon termination of the agreement/contract
- Availability to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on the GDPR.

Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Regular audits of our data protection processes and information security management system will be carried out in accordance with our ISO 9001 & 27001 accreditations.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. TTC Group will keep this policy under review and amend or change it as required. Notification will be given to the DPO of any breaches of this policy. Compliance with this policy will be in full and at all times.

Training

All employees of TTC Group will receive adequate training on provisions of data protection law specific for their role. Further training will be given as requested or if there is a move in role or responsibilities.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as we have become aware of a breach. TTC Group has a legal obligation to report any data breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

For further information please see – **Data Protection Reporting Policy**

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts the individual, the data controller and the data processing organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Failure to comply with this policy or with the terms set out in our contract and/or Data Processing Agreement may lead to termination of that service.

If there are any questions or concerns about anything in this policy, do not hesitate to contact the TTC Group DPO.

Supporting policies

The GDPR Compliance Policy is supported by the following company policies that are available upon request:

CCTV Policy
Computer Security Policy
Data Classification Policy
Data Disposal Policy
Data Protection Policy
Email & Communications Policy
Encryption Policy
Homeworker Protocol Policy
Information Security Policy
Information Sharing Policy
Internet Usage Policy
Managing Data Protection Policy – Third Party Enquiries
Mobile Device Policy
Non-Police Vetting Policy
Password Policy
Quality Policy
Virus Detection Procedure