Data Protection Policy

1. Introduction

RaceTech (referred to as "the **Company**" or "**RaceTech**" in this policy) needs to gather and use certain information and data about individuals. These individuals can include RaceTech employees, workers, directors, officers, contractors, business contacts, customers and suppliers with whom the Company has a relationship or may need to contact in order for RaceTech to carry on its work operations and business purposes.

This policy describes how personal data should be collected, handled, stored and processed to meet the Company's data protection standards and to comply with the law.

This policy does not have contractual effect and does not form part of any individual's contract of employment or contract for services.

2. Why this policy exists

This data protection policy aims to ensure that RaceTech:

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

It also aims to ensure that all RaceTech Staff comply with data protection law and follow good practice.

3. Definitions

"Personal data" is any information that relates to an individual who can be identified from that information.

"**Processing"** is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special Categories of Personal Data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal Records Data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4. Data Protection Law

The Data Protection Act (the "DPA"), and the General Data Protection Regulation (the "GDPR") describe how organisations, including RaceTech, must collect, handle, use and store personal data. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

Data protection legislation is underpinned by important principles:

- personal data must be processed lawfully, fairly and in a transparent manner;
- personal data should only be collected for specified, explicit and legitimate purposes;

- the Company must process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- the Company must keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- the Company must keep personal data only for the period necessary for processing; and
- the Company must adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Racecourse Technical Services Limited (with registered company number 00422837) is the "data controller" under data protection legislation in respect of personal data of RaceTech Staff.

RaceTech will endeavour to implement appropriate and effective technical and organisation measures to ensure compliance with the data protection principles.

RaceTech tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

5. Data Protection Officer

RaceTech has appointed the Company Secretary as its Data Protection Officer ("DPO"). The DPO's role is to inform and advise the Company on its data protection obligations.

6. Policy scope

This policy applies to:

- all staff of RaceTech (including employees, workers, officers and directors engaged at RaceTech's Head Office, in any RaceTech transport location or any other RaceTech location); and
- all contractors and other people working for or on behalf of RaceTech (together referred to as "**RaceTech Staff**" in this policy)

This policy applies to all personal data that the Company holds relating to identifiable individuals. This could include:

- Names
- Postal addresses
- Email addresses
- Telephone numbers
- Next of kin details
- Bank account details
- National insurance numbers
- Medical information
- Appraisal information
- Other information held on an individual's personnel file and in HR systems

The Company may also process Special Categories of Personal Data or Criminal Records Data to perform obligations or to exercise rights in employment law.

7. Data protection risks

The Company takes security of personal data seriously, and has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, inadvertent disclosure and improper access. This policy helps to protect the Company from data security risks, including breaches of confidentiality (for instance, information being given out inappropriately and/or in breach of confidentiality duties).

8. Responsibilities

All RaceTech Staff have responsibility for ensuring data is collected, stored, processed and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

RaceTech Staff may have access to the personal data of other individuals and of our customers and clients in the course of their employment or engagement. Where this is the case, RaceTech relies on RaceTech Staff to help meet its data protection obligations to staff and to customers and clients.

The below people have some particular areas of responsibility:

• The **RaceTech Board** is ultimately responsible for ensuring that the Company meets its data protection obligations.

• The **Data Protection Officer** is responsible for:

- Keeping the Board informed and updated about data protection responsibilities, risks and actual or potential issues;
- Reviewing, updating and ensuring the accuracy of all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and providing advice for the people covered by this policy;
- Handling and overseeing responses to data protection questions from the people covered by this policy;
- Dealing with and overseeing the Company's response to data subject access requests (see below); and
- Checking and approving any contracts or agreements with third parties that may involve the processing of personal data on behalf of the Company to ensure that appropriate technical and operational measures are in place to ensure the security of data.

• The **IT Support Engineer** is responsible for:

- Ensuring all systems, services and equipment used for storing personal data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Company is considering using to store or process personal data, for instance, cloud computing services to ensure they meet acceptable standards.

• The **Head of PR & Marketing** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with other RaceTech Staff (including the DPO) to ensure marketing initiatives abide by data protection principles and the Company's policies and procedures.

9. General RaceTech Staff Guidelines

- The only people able to access data covered by this policy should be those **who need to do so for their work** and are authorised to do so.
- Data **should not be shared informally**. When access to confidential information is required, the appropriate RaceTech Staff member should request it from their line manager.
- RaceTech Staff should keep all data **secure**, by taking sensible precautions, following the Company's policies and following the guidelines below.
- **Strong passwords** must be used on all devices, computers and systems and they should never be shared.
- Personal data **must not be disclosed** to unauthorised people, either within the Company or externally.

- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted or disposed of in line with Company policies and procedures including any data retention policy in place from time to time.
- Personal data (and devices/folders etc. containing personal data) **should not be removed** from RaceTech premises without adopting appropriate security measures (e.g. encryption and password protection) to secure the data and the device;
- RaceTech Staff **should request help** from their line manager or the DPO if they are unsure about any aspect of data protection.
- RaceTech Staff are responsible for helping the Company keep **their personal data** up to date. RaceTech Staff should let the Company know if their data needs to be updated.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under RaceTech's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

The Company **will provide training** to all RaceTech Staff to help them understand their responsibilities when handling data.

10. Data Storage

This section sets out how and where data should be safely stored. Questions about storing data safely can be directed to the IT Support Engineer or Data Protection Officer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot access it.

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- RaceTech Staff should make sure paper and printouts are **not left where unauthorised people could access them** (for example, like on a printer).
- **Data printouts should be shredded** and disposed of securely when no longer required.

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

When data is **stored electronically**, it must be protected from unauthorised access and distribution, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between RaceTech Staff members.
- If data is **stored on removable media** (like a CD, DVD or memory stick), these should be encrypted and kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to a cloud computing service if **approved by the DPO or IT Support Engineer**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently** and those backups tested regularly, in line with the Company's procedures.
- Data should **never be saved locally** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall** as advised by the IT Manager**.**

11. Data Use

When personal data is accessed and used, it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, RaceTech Staff should ensure **the screens of their computers are always locked** when left unattended.

- Personal data **should not be shared informally**. Caution should be exercised when sending personal data by email, as this form of communication is not secure.

- Data **must be encrypted before being transferred electronically**. The IT Support Engineer can explain how to encrypt data in order send data to authorised external contacts.

- Personal data should **never be transferred outside of the European Economic Area**.

- RaceTech Staff **should not save local copies of personal data to their own computers**. Always access and update the central copy of any data.

12. Data Accuracy

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

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

- Data should be held in **as few places as necessary**. RaceTech Staff should not create any unnecessary additional data sets.

- RaceTech Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's or supplier's details when they call.

- The Company will aim to make it **easy for data subjects to update the information** RaceTech holds about them (for instance, via a secure section of the Company's website or HR systems (as appropriate)).

- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

13. Subject Access Requests

All individuals who are the subject of personal data are entitled to make a subject access request. If an individual makes a subject access request, RaceTech will tell them:

- whether or not his/her data is processed and if so why,
- the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks RaceTech has failed to comply with his/her data protection rights; and
- whether or not RaceTech carries out automated decision-making and the logic involved in any such decision-making.

RaceTech will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

RaceTech will verify the identity of anyone making a subject access request before providing any information.

RaceTech will aim to provide the relevant data within one month. In some cases, (including where RaceTech processes a large amount of the individual's data) RaceTech may respond within three months. RaceTech will inform the individual within one month if this is the case.

If a subject access request is manifestly unfounded or excessive, RaceTech is not obliged to comply with it or may charge a fee based on the administrative cost of responding.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at **sar@racetech.co.uk.**

RaceTech may supply a standard request form, although individuals do not have to use this.

14. Other individual rights

Individuals have a number of other rights in relation to their personal data. They can require RaceTech to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override RaceTech's legitimate grounds for processing data (where RaceTech relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override RaceTech's legitimate grounds for processing data.

To ask RaceTech to take any of these steps, the individual should send the request to **sar@racetech.co.uk.**

15. Disclosing Data for Other Reasons

In certain circumstances, the DPA and the GDPR allow personal data to be disclosed without the consent of the data subject, for example to law enforcement agencies. Under these circumstances, RaceTech may disclose personal data if required. However, RaceTech will ensure the request is legitimate and the disclosure appropriate. The person responsible will seek assistance from the Board, the DPO and from the Company's legal advisers where necessary.

16. Impact assessments

Where processing by the Company may result in a high risk to an individual's rights and freedoms, RaceTech will carry out a data protection impact assessment to determine whether the processing is necessary and proportionate. RaceTech will consider the purposes for which the activity is carried out, the risks for individuals and what can be done to mitigate those risks.

17. Breaches

The Company has procedures in place to deal with any suspected personal data breaches (i.e. any acts or omissions that compromise the security, confidentiality, integrity or availability of personal data or the safeguards put in place to protect it, which would include the loss, unauthorised access, unauthorised disclosure or unauthorised acquisition of personal data).

RaceTech will notify individuals or any applicable regulator where legally required to do so.

Any individuals who suspect a personal data breach should immediately inform their line manager, the IT Support Engineer, the Head of PR & Marketing or the DPO as appropriate.

18. Providing Information

The Company aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To this end, the Company has a privacy notice, setting out how data relating to RaceTech Staff is used by the Company.

RaceTech regards the lawful and correct treatment of personal information as very important to successful working and to maintaining the confidence of those with whom we deal.

RaceTech aims to ensure that personal data is treated lawfully and correctly.

19. Monitoring and Review

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the DPA and the GDPR.

This policy is subject to any applicable data protection laws and regulations.

In case of any queries or questions in relation to this policy please contact RaceTech's Data Protection Officer:

Bob Ivey
People & Culture Director and Company Secretary
Email: bivey@racetech.co.uk
Telephone: 0208 947 3333 xtn 257