Data Protection Policy – Pat's Coaches Limited

Who are we?

Pat's Coaches Limited [the Company] needs to collect and process relevant information about individuals; these can include employees, customers, suppliers, business contacts and other people the Company has a relationship with or may need to contact. This policy advises how we handle and store this information in compliance with the company's data protection standards and the General Data Protection Regulation 2016/679 (the "GDPR", also referred to in this policy as the law). The Company is registered as a data controller (contact details below) with the Information Commissioner's Office under registration reference: *ZA330368*.

The data controller decides how your personal data is processed and for what purposes. This Data Protection Policy ensures the Company:

- Complies with data protection law and follow good practice;
- Protects the rights of employees, customers and partners;
- Is open about how it stores and processes individual's data;
- Protects itself from the risks of a data breach.

What is Personal Data?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation 2016/679 (the "GDPR"). The GDPR replaces the existing DPA (Data Protection Act) regulations with effect from 25th May 2018 and has been adopted by the Company with immediate effect.

Data Protection Law

The GDPR is underpinned by 6 important principles stating that data must be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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

Who does this policy apply to?

- All branches of the Company (existing and future);
- All employees and volunteers of the Company;
- All contractors, suppliers and other people working on behalf of the Company.

It applies to all data that the Company holds relating to identifiable individuals as documented within this policy.

Data Protection Risks

This policy helps to protect the Company and the rights of individuals from data security risks, including:

- **Breaches of confidentiality:** For instance, information being given out inappropriately;
- **Inappropriate use of data:** For instance, data should only be used for the purpose(s) it was collected for;
- **Reputational damage:** For instance, the Company would suffer if hackers gained access to sensitive data.

Responsibilities

Everyone who works for or with the Company has some responsibility for ensuring data is collected, stored and handled appropriately. Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The **directors** of the Company are ultimately responsible for ensuring that legal obligations are met;
- The **compliance officer**, also acting as the **data protection officer, Kate Bartle,** is responsible for:
    - Keeping directors updated about data protection responsibilities, risks and issues;
    - Reviewing all internal HR and data protection procedures and related policies, in line with an agreed schedule;
    - Conducting Data Privacy Impact Assessments (DPIAs) as required for assessing new projects and changes to existing projects through implementation of new technology or software;
    - Conducting internal audits of processing activities;
    - Maintaining relevant documentation on processing activities, purposes, data sharing and retention;
    - Ensuring that where data processors are used a relevant written contract has been put in place in compliance with the GDPR;
    - Ensuring that Privacy by Design is a key consideration of all new projects, technology and software being implemented by the Company;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Dealing with requests from individuals, also known as *Subject Access Requests*, in line with their rights to:
        - Be informed;
        - Access;
        - Rectification;
        - Erasure (where applicable* – *see the Privacy Notice for more information*);
        - Restrict processing (where applicable*);
        - Data portability;
        - Objection (where applicable*); or
        - In relation to automated decision making and profiling.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
    - Approving any data protection statements attached to communications such as emails and letters;
    - Addressing any data protection queries from journalists or media outlets like papers;
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles;
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
    - Performing regular checks and scans to ensure security hardware and software is functioning properly;
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it in order to carry out their work responsibilities** and only in line with those specific responsibilities;
- Data **should not be shared informally**. When access to confidential information is required, employees are to make the request via their line manager;
- The Company will provide training to all employees to help them understand their responsibilities when handling data;
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below;
- In all areas where data is stored electronically, **strong passwords must be used** and they should never be shared;
- Personal data **is not to be disclosed** to unauthorised people, either within the Company or externally;
- Data is to be **regularly reviewed and updated** if it is found to be out of date. If the data is no longer required, it should be deleted and disposed of in accordance with policies regarding retention and disposal;
- Employees **should request help** from their line manager or the data protection officer if they are unsure of any aspect relating to data protection;
- The CCTV system is to be operated by designated management only and release of footage is subject to requests made by local authorities – e.g. the Police – or through Subject Access Requests only.

Data Storage

These rules describe where and how data should be stored safely. Any questions regarding this should be directed to the compliance officer.

Paper Storage

- Data stored on paper, including that which is normally stored electronically but has been printed out, should be kept in a secure place where it cannot be seen or accessed by unauthorised people;
- When not required, the paper or files should be kept in a locked drawer or filing cabinet;
- All employees should ensure paper and printouts are not left where unauthorised people can see them, like on a printer or desk;
- Data printouts should be shredded and disposed of securely when no longer required.

Electronic Storage

- All electronically stored data must be protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- If data is stored on removable media (including CDs, DVDs, USB/Pen drives, external hard-drives), these should be kept locked away securely when not being used;
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service;
- Servers containing personal data should be sited in a secure location, away from general office space;
- Data should be backed up frequently. Those backups should be tested regularly;
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones unless done so with express permission, and where permission has been granted, only for the purposes of fulfilling the role of the employee and use for which the data has been collected. These devices must follow the same guidelines with regards to password protection and only the minimum data essential to the task should be stored;
- All servers and computers containing data should be protected by an approved security software and a firewall.

Data use

Personal data is of no value to the Company unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

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

Data accuracy

The law requires the Company, and all employees on its behalf, to take all reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort the Company will put into ensuring its accuracy.

- Data is to be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Employees should take every opportunity to ensure data is updated. For instance, by confirming a customer's details during calls or relating to data held about employees, ensuring all employees are aware of their responsibility to provide accurate details and advise of changes in a timely manner;
- Data should be updated as inaccuracies are discovered;
- It is the compliance officer's responsibility to ensure marketing databases, where held, are checked against industry suppression files every six months.

Subject Access Requests

All individuals who are the subject of personal data stored and processed by the Company are entitled to:

- Be informed of what information the Company holds about them, the purpose for which they hold it and how it is processed;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed how the Company is meeting data protection obligations.

A Subject Access Request is the process an individual uses to make a request for their information. Subject Access Requests can be made using the following methods:

- Individuals (non-employees):
    - Requests can be made by sending an e-mail addressed to compliance@patscoaches.co.uk;
    - Requests can also be made in writing FAO Compliance Officer, Pat's Coaches Ltd, Derwen House, Southsea Road, Southsea, Wrexham, LL11 6PP
- Employees
    - Requests can be made by sending an e-mail addressed to compliance@patscoaches.co.uk;
    - Requests can also be made in writing FAO Compliance Officer, handed in to the office or by post using the above details;
    - Finally, requests can be made using the supplied Subject Access Request Form.

Under GDPR, individuals cannot be charged for a Subject Access Request, **unless**, requests made are manifestly unfounded or excessive, particularly if it is repetitive (although refusal to respond is acceptable under GDPR in these circumstances).

Requests made electronically will be responded to also using electronic format.

All requests will be responded to without delay but at least within one calendar month of receipt of the request. This period can be extended by a further two months for complex or numerous requests, however, where the period has cause to be extended, the individual will be informed and provided with an explanation.

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

Disclosing data for other reasons

In certain circumstances the GDPR allows the Company to disclose personal data to law enforcement agencies without the consent of the individual. Under these circumstances, the Company will disclose the requested data, however, the data controller will ensure that the request is legitimate, seeking assistance from the directors and from the Company's legal advisers where necessary.

Providing information

Pat's Coaches Ltd 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 these ends, the Company has a Privacy Notice, setting out how data relating to the individuals is used by the company. This notice is available both on request and also on the Company's website at the following link: patscoaches.co.uk/privacynotice.pdf.

Contact Details

To exercise all relevant rights, or submit queries / complaints relating to the processing of your personal data please in the first instance contact the Compliance Officer at compliance@patscoaches.co.uk or in writing to Pat's Coaches Ltd, Derwen House, Southsea Road, Southsea, Wrexham, LL11 6PP

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

NOTE: *Where consent is requested for the processing of personal data, consent will be required to be provided for each request on an individual basis at point of collection. Provision of consent will be recorded and managed on an ongoing basis within the Employee Record. Employees have the right to withdraw consent at any time – requests are to be made in writing. The Employee will be notified in writing with confirmation that the requested details have been amended / removed and that the Employee Record has been updated to indicate withdrawal of consent.*