PILATESPT LTD DATA PROTECTION POLICY

Introduction

Purpose

PilatesPT Ltd is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out PilatesPT Ltd's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees [workers, contractors, volunteers, interns, apprentices] and former employees, referred to as HR-related personal data. [This policy does not apply to the personal data of clients or other personal data processed for business purposes.]

PilatesPT Ltd has appointed Stuart Gordon, Company Co-Director as the person with responsibility for data protection compliance within PilatesPT Ltd. He can be contacted at stuart@pilatespt.co.uk. Questions about this policy, or requests for further information, should be directed to him.

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.

Data protection principles

PilatesPT Ltd processes HR-related personal data in accordance with the following data protection principles:

- PilatesPT Ltd processes personal data lawfully, fairly and in a transparent manner.
- PilatesPT Ltd collects personal data only for specified, explicit and legitimate purposes.
- PilatesPT Ltd processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- PilatesPT Ltd keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- PilatesPT Ltd keeps personal data only for the period necessary for processing.

- PilatesPT Ltd adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

PilatesPT Ltd 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.

Where PilatesPT Ltd processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

PilatesPT Ltd will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the [employment, worker, contractor or volunteer relationship, or apprenticeship or internship] is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which PilatesPT Ltd holds HR-related personal data are contained in its privacy notices to individuals.

PilatesPT Ltd keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, PilatesPT Ltd will tell him/her:

- 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 PilatesPT Ltd has failed to comply with his/her data protection rights; and
- whether or not PilatesPT Ltd carries out automated decision-making and the logic involved in any such decision-making.

PilatesPT Ltd 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.

[If the individual wants additional copies, PilatesPT Ltd will charge a fee, which will be based on the administrative cost to PilatesPT Ltd of providing the additional copies.]

To make a subject access request, the individual should send the request to stuart@pilatespt.co.uk. In some cases, PilatesPT Ltd may need to ask for proof of identification before the request can be processed. PilatesPT Ltd will inform the individual if it needs to verify his/her identity and the documents it requires.

PilatesPT Ltd will normally respond to a request within a period of one month from the date it is received. In some cases, such as where PilatesPT Ltd processes large amounts of the individual's data, it may respond within three months of the date the request is received. PilatesPT Ltd will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, PilatesPT Ltd is not obliged to comply with it. Alternatively, PilatesPT Ltd can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which PilatesPT Ltd has already responded. If an individual submits a request that is unfounded or excessive, PilatesPT Ltd will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require PilatesPT Ltd 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 PilatesPT Ltd 's legitimate grounds for processing data (where PilatesPT Ltd 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 PilatesPT Ltd''s legitimate grounds for processing data.

To ask PilatesPT Ltd to take any of these steps, the individual should send the request to stuart@pilatespt.co.uk.

Data security

PilatesPT Ltd takes the security of HR-related personal data seriously. PilatesPT Ltd has internal policies and controls in place to protect personal data against loss,

accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Systems Restrictions

All systems are only accessible by Hollie Gordon (Director) and Stuart Gordon (Director) of PilatesPT Ltd, with password access.

Data Security Policy

All Data is only accessible by Hollie Gordon (Director) and Stuart Gordon (Director) of PilatesPT Ltd, with password access.

Where PilatesPT Ltd engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical measures to ensure the security of data.

Impact assessments

Some of the processing that PilatesPT Ltd carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, PilatesPT Ltd will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.]

Data breaches

If PilatesPT Ltd discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. PilatesPT Ltd will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.]

International data transfers

[PilatesPT Ltd will not transfer HR-related personal data to countries outside the EEA]

Individual responsibilities

Individuals are responsible for helping PilatesPT Ltd keep their personal data up to date. Individuals should let PilatesPT Ltd know if data provided to PilatesPT Ltd changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals [and of our customers and clients] in the course of their [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, PilatesPT Ltd relies on individuals to help meet its data protection obligations to staff [and to customers and clients].

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside PilatesPT Ltd) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from PilatesPT Ltd's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

[Further details about PilatesPT Ltd's security procedures can be found in its data security policy.]

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under PilatesPT Ltd'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.

Training

PilatesPT Ltd will provide training to all individuals about their data protection responsibilities as part of the induction process [and at regular intervals thereafter].

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.