TPS Services

Practical TPS solutions for businesses

DATA PROTECTION OUR POLICY

TEL: 0343 005 9576

TPS Services

Telephone: 0343 005 9576

Fax: 0844 774 8411

www.tpsservices.co.uk

TPS Checker

Telephone: 0343 005 9576

Fax: 0844 774 8411

www.tpschecker.co.uk

I Want That Ltd

Kemp House, 152-160 City Road

London, EC1V 2NX

Data Protection Policy

Introduction

TPS Services is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act"). Staff will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, partners or other entities who have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, TPS Services has to collect, hold and use information about people to whom it provides services.

This personal information must be handled and dealt with properly, however it is collected, held, recorded or used (whether it be on paper, in computer records or recorded by any other means) and there are safeguards within the Act to ensure this.

TPS Services regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly and all staff are required to adhere to this policy to ensure its effectiveness.

To this end the company fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act 2018.

Who to contact

Name	Vince Costa-Barnett - Director
Company	TPS Services (IWT)
Address	Kemp House 152-160 City Road London EC1V 2NX
Telephone	0343 005 9576

The principles of data protection

The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive information

TPS Services will, through appropriate management and the use of strict criteria and controls:-

- Observe fully the conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

  These include:
  - The right to be informed that processing is being undertaken;
  - The right of access to one's personal information within the statutory 40 days;
  - The right to prevent processing in certain circumstances;

- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, TPS Services will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
- The basic principle be undertaken that access should only be granted to any element of data where it is absolutely necessary for the purpose of the function being performed i.e. no individual or company should have access to more information than they need for the specific purpose.

All staff are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within the company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically and restricted IP access;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other entities of the company must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the company and that individual, company, partner or firm;
- Allow data protection audits by the company of data held on its behalf (if requested);
- Indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the company.

Issues applying directly to the transmission and storage of Client data

All data uploaded by our clients will be stored for a specified period of time, which be default is 60 days. Clients can select either 30 days or 45 days as alternatives. In some cases clients can select that we store no data at all.

At the expiration of that time, client's files are deleted from our system.

Clients may log in and delete files at any other time of their choosing, for example straight after screening has been completed and their results downloaded.

All data is transmitted over secure internet connections using SSL encryption.

I Want That Ltd t/a TPS Services is a fully licenced TPS, CTPS and FPS holder and ultimately regulated by the Information Commissioners Office (ICO).

Exchanging data with a third party company will always be a concern for businesses and TPS Services appreciates that, but we can assure our clients that if their data was not safe with us then we would not be able to operate.

Implementation

The company has appointed a Compliance Manager. This person will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Compliance Manager. The Compliance Manager will also have overall responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the company, with the Data Protection Act.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. TPS Services is registered as such.

The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end the designated officer will be responsible for notifying and updating the Compliance Manager of the processing of personal data.

The Compliance Manager will review the Data Protection Register annually.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes should be brought to the attention of the Compliance Manager immediately.