People Technologies Ltd.

Privacy and Data Protection Policy

July 2021

Purpose of this document

In line with the UK Data Protection Act 2018 and with the principles set out under the General Data protection Regulation (EU) 2016/679, this document sets out the company policy for managing the privacy and security of personal data processed by the company on behalf of clients and in developing the business interests of the company.

Contact details of the company

People Technologies Ltd.
123 Molesey Park Road
East Molesey
KT8 0JX
Surrey
UK

Inquiries regarding this policy should be sent to Eugene Burke, Technical Director, via eugene@peotech.co.uk.

What this document covers

This document covers:

- What personal identifiable information (PII) the company may process to fulfil its contractual obligations and to conduct its business.
- What safeguards the company employs to ensure that the processing and management of PII data is secure.
- What the company will do if it detects or is alerted to a breach of data security.
- Who in the company is responsible for overseeing this policy.

Why we process personal data

The company's business is the supply of psychometric tests for the assessment and selection of personnel as aviation pilots and air traffic controllers.

In line with legitimate interest guidance provided by the UK Information Commissioner's Office (ICO), there are four reasons why the company processes and holds personal data to enable the company to meet its business objectives:

To conduct our business:

1. Data is received and held by the company to respond to inquiries from potential clients and to manage contracts with established clients.
2. Data is received and held by the company in relation to suppliers and subcontractors who provide services to enable the company to function.

To supply products and services to our clients and to develop and maintain our products and services:

3. To meet the company's contractual obligations to its clients in the use of its products and services.

4. To conduct ongoing research and development to ensure that the company's products and services are of a high quality and meet professional standards.

These are all allowable and lawful reasons for the company to process, hold and manage personal data.

The types of personal data that we hold

To conduct our business:

- The details of organisations inquiring about the company's products and services as well as existing clients using the company's products and services.

- The details of contacts in that organisation which may include the person's name, their position in the organisation and their contact details including email address, telephone number and postal address.

- Legal documents and communications relating to the sale and ongoing supply of products and services to the company's clients.

- Documents and communications with suppliers who support the company in meeting its business objectives.

To supply products and services to our clients and to develop and maintain our products and services:

- The company may process data on candidates who have sat the company's tests and that data may include their scores on those tests, the date they sat the tests, the candidate's name, date of birth or age at the time of testing and their gender.

- The company may also receive and process data on a candidate's success in pilot or air traffic control training.

- Personal data on candidates sitting the company's tests may be necessary for matching and collating data on candidates and for statistical analysis to identify trends and relationships in that data.

How we process and store personal data

To conduct our business:

- All inquiries are treated as confidential and are only replied to via the company email @peotech.co.uk.

- All inquiries and contractual information are recorded and stored on secure company laptops that require password access and that are monitored by security and antivirus software.

- Paper copies of contractual, financial and legal information may be stored in paper form in secure and lockable storage.

- All records that are no longer required by the company to conduct its business are destroyed by either deleting from digital media or by using a shredder for paper copies.

- The company does maintain records to provide historical information regarding contracts, for the purpose of contract renewals and for clients who may have previously ceased to use the company's products and services but wish to re-establish a relationship with the company.

- Should a client, past or present, contact the company to request that information held on them or for them is deleted, the company will respond by confirming the reason for the request and delete that information unless that deletion will materially affect the company's ability to conduct its business. All such inquiries should be directed to Eugene Burke via eugene@peotech.co.uk.

- Note that the company assumes the responsibility of data controller in managing the security of the data gathered to conduct its business.

  A data controller is defined by the UK Information Commissioner's Office (ICO) as those who exercise overall control of the purpose and means of the processing of personal data.

  As a data controller, the company has registered with the ICO as a Tier 1 (micro) organisation under the registration number ZB121597.

To supply products and services to our clients and to develop and maintain our products and services:

- In the use of the company's products, the responsibility for gaining candidate consent for the recording of PII data is the client's responsibility in line with local legal and professional guidelines. However, the company has a responsibility to actively advise clients to alert candidates of the reasons why personal data is being collected and their rights regarding that data.

- The company's products (tests) are hosted on test administration software owned and supplied by a vendor that is independent of the company. That software has a number of security protocols and safeguards to ensure that personal data and test scores are stored securely and are only accessed by relevant client personnel. Inquiries regarding these security protocols and safeguards should be directed to Eugene Burke via eugene@peotech.co.uk. The inquirer may then be referred to the software vendor if required to satisfy the inquiry.

- The company does, from time to time, receive data from the test administration software in order to:

  - Review the performance of clients' candidates on the tests and to ensure that norms and benchmarks are fit for use.

  - Conduct analyses to monitor the psychometric performance of the tests.

  - To compare different candidate groups scores.

  - To validate the tests against training outcomes.

- To conduct benchmarking analyses to assist clients in identifying actions to improve their attraction, selection and training of their candidates.

- In receiving and processing data to service clients and while the company is acting in the interests of another party, the client, the company is likely to be classified as either a data controller or as a joint data controller.

  How these responsibilities are shared is complicated by the fact that the client may be located outside the UK and subject to different data protection laws and regulations to those in the UK.

  That said, the general principles of good data protection practice are acknowledged globally and compliance with UK law should ensure that the company is following effective procedures to safeguard both itself and the interests of the client.

  A separate document, Data Management and Processing Guideline, provides details of the principles and the procedures to be followed in the processing of data received by the company. That document describes:

  - How candidate data should be transferred to ensure security.

  - How PII data may be used to enable data processing to be performed and what should happen to PII data once that processing has been completed.

  - Anonymisation of candidate data for longer-term storage and retrieval.

  - Where candidate data should be stored and access to that data managed.

  A copy of the company's Data Management and Processing Guideline may be obtained by contacting Eugene Burke via eugene@peotech.co.uk.

What we need to do in the event of a breach of security

In the event of a breach and to record details of a breach:

- Assess the severity of the breach:

  - What data were involved?
  - Could this data reveal the identity of a person to whom the data belongs (a "data subject")?
  - When did the breach occur?
  - Where did the breach occur? Was it via a client's site or systems; during data transfer and, if so, via what medium (e.g. email, data transfer software); through the company's equipment or actions?

- Determine what actions are required to contain and/or remedy the breach:

  - Contact any service providers and/or subcontractors responsible for the equipment and/or software involved.
  - Agree a response plan and a timeline including service providers and/or subcontractors if relevant for containing the breach and recovering any lost or deleted data if possible.
  - Assess whether passwords and access to systems need to be changed and, if so, a timeline to make those changes.

        - Contact any affected clients, suppliers and/or subcontractors to alert them to the breach, the severity of the breach and what actions the company is taking to respond to the breach. They should be informed that they have the right to register a complaint with the ICO if they are not satisfied with how the company has handled the breach. Details of how a complaint can be made to the ICO are available via https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

- Contact the ICO:

    - If a data breach is significant and the impact on individuals may be severe, the company is required to report that data breach to the ICO within 72 hours of becoming aware of the breach.
    - Information on how to contact the ICO in the event of a breach can be found via https://ico.org.uk/for-organisations/report-a-breach/
    - This site also provides various tools and guidance to assess whether a breach is sufficiently severe to warrant contacting the ICO

Version control of this document

This is shown by the date of this document and later versions will be indexed by a date subsequent to the current document's date. The date shown on this document is the date of the current version.

Person responsible for this document

Eugene Burke, Director, People Technologies Ltd.