Table of contents

1. Company Overview, Purpose, Scope and Users

1.1. Company Overview

Peregrine Immigration Management Ltd was established in 2011 and is headquartered in Bristol. Peregrine was acquired by CIBT in September 2016.

Staff employed by CIBT or Peregrine support other CIBT group companies, as well as the legacy Peregrine business of developing and supplying global immigration management software to external licensees.

Peregrine currently has six direct employees, all of whom are based in the UK. Eight employees of other CIBT group companies, based in the UK, the US, South Africa and Brazil, also work on Peregrine business.

1.2. Purpose

Peregrine Immigration Management Ltd, hereinafter referred to as the "Company", strives to comply with applicable laws and regulations related to Personal Data protection in countries where Peregrine operates.

This Policy sets forth the basic principles by which Peregrine processes the personal data of customers, suppliers, website visitors, and other individuals, and indicates the responsibilities of its employees while processing personal data.

1.3. Scope

This Policy applies to the development, maintenance and provision of the **Immiguru** immigration knowledge database and the **Immigo** case management system for external licensees, and the Peregrine website and email newsletter subscription.

1.4. Users

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of Peregrine.

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Privacy and Electronic Communications Directive 2002/58/EC
- The Directive on Security of Network and Information Systems (NIS Directive - 2016/1148/EU)
- The UK Data Protection Act (1998), Schedule 1, Seventh Principle
- The UK Computer Misuse Act (1990)

- Employee Personal Data Protection Policy
- Personal Data Inventory Guidelines
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Guidelines
- Cross Border Personal Data Transfer Procedure
- Information Security Policy
- Computer Security Policy
- Business Continuity Plan
- Procedure for Document and Record Control
- Breach Notification Procedure

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation.

The GDPR applies to the processing of personal data in the context of the activities of Company entities (acting either as a controller or a processor) in the EU/EEA.

EU GDPR also applies to the processing of personal data of data subjects who are in the EU/EEA by a controller or processor not established in the EU/EEA, where the processing activities are related to:

- The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU/EEA; or
- The monitoring of their behaviour as far as their behaviour takes place within the EU/EEA.

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*."

4.1. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.2. Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3. Data Minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Peregrine must apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects concerned.

4.4. Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps 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 in a timely manner.

4.5. Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

4.6. Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, Peregrine must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

4.7. Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

5. Building Data Protection into Business Activities

To demonstrate compliance with the principles of data protection, an organisation should build data protection into its business activities.

Personal data processing activities must only be undertaken when explicitly authorised by the Managing Director.

Peregrine must decide whether to perform a Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

5.1. Notification to Data Subjects

If Peregrine is collected personal data from data subjects, at the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, Peregrine will properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and Peregrine's security measures to protect personal data.

This information is provided through the Personal Data Protection Notice.

The **Information Security Manager** is responsible for creating and maintaining a Personal Data Protection Notice.

External licensees of Immigo (data controllers) are responsible for notifying data subjects whose data they transfer and store using Immigo.

5.2. Consent basis for processing

Whenever Peregrine is a data controller and personal data processing is on the basis of the data subject's consent, Peregrine will retain a record of such consent. Peregrine will provide those data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

5.2.1. Cookies

Immiguru and Immigo users actively click "Accept" or "Don't accept" buttons to give or withhold their consent to the use of cookies to help their computer remember when they are logged in, and to ensure that requests to Immiguru are coming from that computer.

5.2.2. Contact us

By including personal data, including name and email address, when using our "Contact us" form, website users consent to Peregrine contacting them by email in response to their queries and comments.

5.2.3. News alert subscribers

By entering their email address into the box on Peregrine's News page and clicking the "Subscribe" button, users consent to Peregrine storing the email address and sending them immigration news alerts, company news and product updates.

5.2.4. Minors

Where collection of personal data relates to a child under the age of 16, Peregrine must ensure that parental consent is given prior to the collection using the Parental Consent Form.

5.2.5. Change of purpose

Personal data must only be processed for the purpose for which they were originally collected. In the event that Peregrine wants to process collected personal data for another purpose, Peregrine must seek the consent of its data subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s).

5.3. Contract basis for processing

Contact details of Immiguru/Immigo client and supplier users in the Immiguru database are collected and stored and otherwise processed in order to fulfil client (licensee) and partner contracts.

Immigo clients' applicant and corporate data stored in the Immigo database is collected and stored and otherwise processed in order to fulfil client (licensee) contracts.

5.4. Collection

Peregrine must strive to collect the least amount of personal data possible. If personal data is collected from a third party, the Managing Director of Peregrine shall seek to ensure that the personal data is collected lawfully.

Now and in the future, the **Information Security Manager** must ensure that collection methods are compliant with relevant law, good practices and industry standards.

5.5. Processing Location and Security

Peregrine is certified to the ISO 27001 Information Security Standard.

Personal data is processed in the United Kingdom (in the European Union). Hosting and storage of personal data takes place on secure, virtual servers in outsourced data centres, which are located in the United Kingdom (in the European Union) and are managed by multiple hosting providers.

The hosting providers and datacentres are either ISO 27001 or SOC 2 compliant, and GDPR compliant, and maintain strict security protocols. The choice of hosting provider and agreement is reviewed regularly to ensure that they meet the Information Security and Personal Data Protection Objectives.

5.6. Retention

Under the UK Data Protection Act, we are required to keep documents for not longer than is necessary for the management of user accounts. After this period, personal data will be irreversibly destroyed.

- Email addresses stored in our servers by us for immigration news and service update notifications will be kept by us until such time that the data subject notifies us that they no longer wish to receive this information.
- Personal contact details emailed to us via our "Contact us" form will be kept until the related query is resolved.
- Contact details of Immiguru/Immigo users, supplier and company contacts in the Immiguru database in our servers will be kept by us until the termination of the relevant supplier or client contract.
- Immigo clients' applicant data stored in the Immigo database will be kept by us for as long as the service agreement between Peregrine and the client (external licensee) is in effect.
- Server logs of website visitors' URLs are maintained for one year.

Peregrine must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Peregrine is certified to the ISO 27001 Information Security Standard.

Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. The Information Security Manager is responsible for compliance with the requirements listed in this section.

5.7. Disposal

The Company and its employees should, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. Overall responsibility for the destruction of data falls to the Information Security Manager.

Once the decision is made to dispose of the data, it should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Information Security Manager subcontracts for this purpose. Any applicable general provisions under relevant

data protection laws and the Company's General Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the Information Security Policy.

The Information Security Manager shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

5.8. Disclosure to Third Parties

If Peregrine were to use a third-party supplier to process personal data on its behalf, the Information Security Manager would have to ensure that this processor would provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor GDPR Compliance Questionnaire must be used.

Peregrine must contractually require such a supplier to provide the same level of data protection. The supplier must only process personal data to carry out its contractual obligations towards Peregrine or upon the instructions of Peregrine and not for any other purposes. When Peregrine processes personal data jointly with an independent third party, Peregrine must explicitly specify its respective responsibilities and those of the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

5.9. Cross-border Transfer of Personal Data

The GDPR applies to the processing of personal data in the context of the activities of Company entities (acting either as a controller or a processor) in the EU/EEA.

EU GDPR also applies to the processing of personal data of data subjects who are in the EU/EEA by a controller or processor not established in the EU/EEA, where the processing activities are related to:

- The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU/EEA; or
- The monitoring of their behaviour as far as their behaviour takes place within the EU/EEA.

The EU GDPR allows for personal data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection.

Thus Peregrine, in the absence of European Commission adequacy decision, may transfer personal data:

- for which it is the data controller outside non-EU states by using of standard contractual clauses as listed in Annex 1 and Annex 2 to this document
- for which it is not the data controller subject to instruction from the relevant data controller.

CIBT **DPO** will be responsible for monitoring the official European Commission website (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm) as well as other communication channels to quickly identify any new versions of the standard contractual clauses and update Annex 1 and Annex 2 of the procedure.

5.10. Rights of Access by Data Subjects

When requested by a data subject or relevant data controller to correct, amend or destroy personal data records, Peregrine must ensure that these requests are handled within a reasonable time frame. Peregrine must also record the requests and keep a log of these.

Peregrine will provide data subjects for which it is the data controller with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism is further detailed in the Data Subject Access Request Procedure.

5.11. Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. The Managing Director is responsible for ensuring that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

5.12. Right to be Forgotten

Upon request, data subjects for which Peregrine is the data controller have the right to obtain from Peregrine the erasure of their personal data. Peregrine must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

- As a controller, upon request from clients (licensees) and suppliers, website users and newsletter subscribers, Peregrine will erase their personal data obtained on the basis of consent or contract. As a consequence, Peregrine may no longer be able to respond to queries, provide email news alerts, or provide access to our software products for those clients (licensees) and suppliers, website users and newsletter subscribers.
- As a processor, upon request from its clients (licensees), Peregrine will assist them to erase the personal data they have stored in Peregrine databases.

5.13. Data Breach Response

When Peregrine learns of a suspected or actual personal data breach, the Data Breach Response Team – Peregrine's Managing Director (**MD**), Chief Technical Officer (**CTO**) and Information Security Manager (**ISM**) and the CIBT Data Protection Officer (**DPO**) - must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the *Data Breach Response and Notification Procedure*. Where there is any risk to the rights and freedoms of data subjects, the data controller must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

Once a breach of personal data controlled by Peregrine is reported, Peregrine must implement the following:

- Validate/triage the personal data breach
- Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded
- Identify remediation requirements and track resolution
- Perform the Data Protection Impact Assessment on the affected processing activity.
- Record the data breach into the Data Breach Register.
- Report findings to the top management
- Coordinate with appropriate authorities as needed
- Coordinate internal and external communications
- Ensure that impacted data subjects, data controllers and supervisory authorities are properly notified, if necessary

6. Organization and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with Peregrine and has access to personal data processed by Peregrine.

The key areas of responsibilities for processing personal data lie with the Data Protection Triumvirate – Peregrine's Managing Director (**MD**), Chief Technical Officer (**CTO**) and Information Security Manager (**ISM**):

Peregrine MD makes decisions about and approves Peregrine's general strategies on personal data protection.

Peregrine ISM is responsible for managing the personal data protection program and for the development and promotion of end-to-end personal data protection policies.

Peregrine ISM, together with **CIBT DPO,** monitors and analyses personal data laws and changes to regulations, develops compliance requirements.

Peregrine CTO is responsible for:

- 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.

Peregrine ISM, 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 like newspapers.
- Where necessary, working with the Data Protection Officer to ensure marketing initiatives abide by data protection principles.

Peregrine ISM is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing Personal data protection expertise and awareness training for employees working with personal data.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

Peregrine ISM is responsible for passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department must ensure that Peregrine reserves a right to audit suppliers.

7. Audit and Accountability

Peregrine ISM is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

8. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which Peregrine operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail. Managing records kept on the basis of this document

9. Validity and document management

This document is valid as of 30/04/18

The owner of this document is the **Information Security Manager**, who must check and, if necessary, update the document at least once a year.