

PeopleIN Limited and its subsidiaries (**PeopleIN, Us or We**) are committed to protecting and securing the privacy and confidentiality of our stakeholder's Personal Information.

For the purposes of this policy, relevant stakeholders include:

- PeopleIN employees;
- prospective PeopleIN employees;
- host employers/clients;
- service providers;
- business associates; and
- visitors, which includes visitors to our website.

When handling Personal Information we comply with the Australian Privacy Principles (**APPs**) contained in the *Privacy Act 1988* (Cth) (**the Privacy Act**). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at www.aoic.gov.au.

What is Personal Information and why do we collect it?

"Personal Information" is information or an opinion about an identifiable individual, or an individual who is reasonably identifiable.

The types of Personal Information we collect may depend on the reason for collection and different Personal Information will be required depending on the stakeholder.

We collect your Personal Information for the primary purpose of operating our business and providing our services. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure.

The types of personal information we collect will include names, addresses, email addresses, phone numbers and other information necessary for operating our business and providing our services, including for associated administrative and legal purposes. In addition we may collect personal information relating to employment which includes, but is not limited to, tax file number details, bank account details, superannuation details, reference details, emergency contact details, visa details, qualifications/training details, limited health information.

This Personal Information is obtained in many ways including by completing form(s), by telephone, by email, from your website, from media and publications, from other publicly available sources, and from other third parties.

We collect personal information that is necessary for the purpose of operating our business and providing our services to you, including:

- confirming your identity;
- confirming accuracy of information provided to us;
- providing services to you;
- transferring monies or paying benefits;
- verifying your identity;

- letting you know about our other services; and
- managing our relationship with you.

If you are a service provider, we collect Personal Information that is necessary for the purpose of operating our business and providing our services, as well as receiving products or services from you and conducting due diligence on you and your products or services.

If you do not provide us with the information we require, we may terminate our relationship with you if we believe it will jeopardise our ability to provide a complete, accurate and comprehensive service.

Third Parties

Where reasonable and practicable to do so, we will collect your Personal Information directly from you when you correspond or register details with us, enter into arrangements with us or provide feedback to us. However, in some circumstances we may be provided with information by third parties (such as host employers).

Disclosure of Personal Information

We may disclose your personal information to companies within our corporate group, our bank or financial institution, insurers and to other third party contractors to facilitate the delivery of our services or improve the quality of our services to you, including to carry out maintenance, repairs and development of our computer software and hardware.

We may also disclose your personal information to third parties, such as host employers, service providers engaged to undertake functions or activities on our behalf (e.g. processing payment information, managing databases, marketing, researching and advertising), advisors, lawyers, accountants and to law enforcement agencies or to government bodies.

We take steps to ensure that our service providers are obliged to protect the privacy and security of personal information and use it only for the purpose for which it is disclosed.

We may also disclose your personal information to acquirers (or potential acquirers) of all or any part of our business, or in order to run the business or part of the business acquired.

We may also use or disclose any of your personal information for other purposes and/or to other persons as required or permitted by law.

Security of Personal Information

Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification or disclosure. This includes physical security (e.g. limited access to hard-copy documents) and computer/network security (passwords, firewalls).

We may use cloud storage to store the personal information we hold about you, and the cloud storage may be located outside Australia.

It is generally unlikely that we will disclose your personal information overseas. However, any overseas disclosure does not affect our commitment to safeguarding your personal information and we will take reasonable steps to ensure any overseas recipient complies with the APPs.

Where we may be disclosing your personal information overseas, we will seek your consent, or inform you and ensure that appropriate contractual measures are in place requiring the overseas entity to protect your personal information in accordance with our obligations under Australian privacy law.

Cookies

To improve your experience on our website, we may use 'cookies'. A cookie is a small text file that our website may place on your computer as a tool to remember your preferences. In many cases, the tools used on our website record information in a way that does not identify you as an individual. In other cases, information may be personal information in which case this Privacy Policy will apply.

You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of our website.

Access to your Personal Information

You may request access to the personal information we hold about you by contacting us in writing at Level 6, 540 Wickham Street, Fortitude Valley QLD 4006. Fees will not be charged for requesting access to your Personal Information but you may be charged a reasonable fee for providing access to your personal information.

There may be circumstances where we are unable to give you access to the information that you have requested. If this is the case we will inform you and explain the reasons why.

Maintaining the Quality of your Personal Information

It is an important to us that your Personal Information is up to date. We will take reasonable steps to make sure that your Personal Information is accurate, complete and up to date.

You have a right to ask us to correct any information we hold about you if you believe it is inaccurate, incomplete, out of date, irrelevant or is misleading. If we do not agree with the corrections you have supplied and refuse to correct the Personal Information, we are required to give you a written notice to that effect and a statement if requested.

Privacy Policy Complaints and Enquiries

If you have any queries or complaints about our Privacy Policy please contact us at: 07 3238 0800.

If we have not responded to you within a reasonable time frame, or if you are not satisfied with the manner in which the company has handled a complaint, a further complaint can be submitted to The Office of the Australian Information Commissioner.

Related legislation

Privacy Act 1988 (Cth)

Related Documents

- Disciplinary Policy
- Data Privacy Procedure

Policy Review

This policy will be reviewed at least annually (or more frequently if necessary due to technical or other business policy requirements). The Company reserves the right to suspend, modify, or withdraw this Policy at any time. The Employee is responsible for regularly reviewing its terms.

Data Privacy PROCEDURE

PURPOSE: To protect our candidate, client and corporate data, PeopleIN have established an approval process that applies to all company staff and which shall be followed whenever candidate, client or corporate data is being requested or released outside a Business Unit or the Group.

What requires approval?

Approval will be required under this policy for the extraction or release of any of the following:

- Data that contains sensitive Personal Identifiable Information (for example: driver's license, passport details, date of birth, health or credit information, tax file number, employee records or sensitive information; and
- Where the data is being shared between business units/entities within the Group, or externally from the organisation; or
- If the data is going to be used for some form of communications or marketing campaign thereby requiring consent checks; or
- Where the data is being provided to a third-party that is not recognised by a regulator or legal authority as the appropriate and necessary recipient of that information under law.

Notwithstanding the above, under this policy no prior approval is required for the following use cases:

- Operational and transactional data that is used while performing ordinary business processes and functions, for the stated purposes under which it was collected, using approved business systems and security procedures.
- Data approved for project use and transmitted in a previously approved and appropriately secure manner between formally contracted parties specific to the purposes of that project.
- Deidentified and/or abstracted data for which transmission to another party is neither in breach of the Privacy Act 1988, the Australian Privacy Principle (APP) guidelines or PeopleIN internal or contractual confidentiality requirements.
- Data that is provided to an entity, body corporate or persons recognised by a regulator or legal authority as the appropriate and necessary recipient of that information under law.

Who can approve release of data under this policy?

Within PeopleIN, there are two roles appointed to ensure the security, integrity, governance and standards for appropriate use and representation of client, candidate and company data. These roles are the **Data Custodian** and **Senior Data Custodian**.

In the first instance, where extraction or release of client, candidate or company data must be approved, engage with your Business Unit leader (BUL). Your BUL will then seek the appropriate approval from the PeopleIN **Data Custodian**.

Role of the Data Custodian

The Data Custodian within PeopleIN is the **Head of ICT Operations**. In their role of Data Custodian, they are responsible for:

- Reviewing and approving/declining any requests to extract datasets from any company business systems.
- Coordination of requests, including managing the structure, security and sharing protocols for that data, as per the approval process and where appropriate.

Doc # Revision: PRO_0042_A

Page 1 of 2

Doc Owner: GOD

This is a Controlled Document as are all on PeopleINtranet Online. Electronic and printed copies are not controlled, will not be updated and must be checked against PeopleINtranet Online prior to use.

Approved: GOD – 29.08.2024

PeopleiN

Data Privacy PROCEDURE

- Escalating data extract requests to the **Senior Data Custodian** where the requirement involves sharing any data extract externally from the organisation.

Role of the Senior Data Custodian

The Senior Data Custodian must be a **GLT member** and, in conjunction with a second nominated GLT member, is responsible for reviewing and approving/declining requests to extract data that is intended to be shared outside the Group. The current Senior Data Custodian is the **Group Operations Director**.

Related Documents

Privacy Policy

Procedure Review

This process will be reviewed at least annually (or more frequently if necessary due to technical or other business requirements). The Company reserves the right to suspend, modify, or withdraw this process at any time. The Employee is responsible for regularly reviewing its terms.