HeadHunters
HQ

Personal Data Protection Policy

Updated and Effective as of 11 November 2025

1 Introduction

In its everyday business operations HeadHunters HQ makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps HeadHunters HQ is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to HeadHunters HQ systems.

2 Personal Data Protection Policy

2.1 The Personal Data Protection

The Personal Data Protection Act 2012 (PDPA) is one of the most significant pieces of legislation affecting the way that HeadHunters HQ carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the PDPA, which is designed to protect the personal data of individuals in Singapore. It is HeadHunters HQ's policy to ensure that our compliance with the PDPA and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

There are some terms which are used throughout the Data Protection Provisions and which bear particular meanings for the purposes of the PDPA. Some of these terms are defined in Part I of the PDPA (specifically, in Section 2(1)). However, the most fundamental definitions with respect to this policy are as follows:

a) “**Individuals"** refers to natural persons who are alive and can be identified either from the data itself or from the data in conjunction with other information that is in, or is likely to come into, the possession of the organisation.

b) "**Personal data**" refers to data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

c) "**Organisations**" refers to any entity or individual, including a data intermediary, that processes personal data in Singapore.

d) "**Collection"** refers to the act of obtaining personal data from any source, including third parties. "Use" refers to the handling of personal data within an organisation. "Disclosure" refers to the provision of personal data to third parties outside the organisation.

e) "**Purposes**" refers to the reasons for which personal data is collected, used, or disclosed. Organisations must have a valid reason for collecting, using, or disclosing personal data, and must inform individuals of these purposes.

f) "**Reasonable**" refers to a standard of behaviour that is appropriate and justifiable given the circumstances. The PDPA requires organisations to take reasonable steps to ensure that personal data is accurate and up-to-date, and to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks. What is considered "reasonable" will depend on factors such as the sensitivity of the data, the potential harm that could result from a breach, and the resources available to the organisation.

2.3 Principles relating to the processing of personal data

There are several fundamental principles upon which the PDPA is based. These principles are as follows:

a) Consent: Organisations must obtain an individual's consent before collecting, using or disclosing his or her personal data unless an exception applies.

b) Purpose limitation: Organisations must collect, use, or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances and that the individual has been informed of.

c) Notification: Organisations must inform individuals of the purposes for which their personal data is being collected, used or disclosed.

d) Access and correction: Individuals have the right to access and correct their personal data held by an organisation.

e) Accuracy: Organisations must make reasonable efforts to ensure that the personal data collected is accurate and complete.

f) Protection: Organisations must protect personal data in their possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.

g) Retention limitation: Organisations must cease retention of personal data when the purpose for which it was collected is no longer being served unless the retention is necessary for legal or business purposes.

h) Transfer limitation: Organisations must ensure that personal data transferred to third parties is protected by comparable data protection standards.

i) Openness: Organisations must be open about their personal data management policies and practices.

j) Accountability: Organisations must be accountable for complying with the PDPA and take appropriate measures to ensure that they are in compliance. These principles are designed to ensure that personal data is processed in a fair, transparent, and responsible manner, and that individuals have control over their personal data

HeadHunters HQ must ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.4 Rights of the individual

The data subject also has rights under the PDPA. These consist of:

- The right to access
- The right to correction
- The right to withdraw consent
- The right to request cessation of use or disclosure
- The right to request deletion
- The right to limit use or disclosure
- The right to data portability
- The right to object
- The right to be informed of the consequences of not providing personal data

These rights are designed to give individuals greater control over their personal data and to ensure that their personal data is being processed fairly and transparently by HeadHunters HQ.

Each of these rights must be supported by appropriate procedures within HeadHunters HQ that allow the required action to be taken within a reasonable time, taking into account the complexity and volume of the request, and to provide an explanation if the request cannot be fulfilled.

DATA SUBJECT REQUEST	TIMESCALE
The right to access	One month
The right to correction	One month
The right to withdraw consent	Without undue delay
The right to request cessation of use or disclosure	Without undue delay
The right to request deletion	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
The right to be informed of the consequences of not providing personal data	When data is collected

Table 1: Timescales for data subject requests

The Personal Data Protection Commission (PDPC) in Singapore recommends that organisations respond to data subject requests within 30 days, but acknowledges that this may not be feasible in all cases.

Regardless of the timeframe, HeadHunters HQ should prioritise data subject requests and respond to them as promptly as possible to ensure compliance with the PDPA's principles and regulations, and to maintain the trust of their customers or clients

2.5 Consent

According to the PDPA, an individual's consent must be obtained before collecting, using, or disclosing their personal data, unless the collection, use, or disclosure is exempted or permitted under the law. The consent must be obtained in an appropriate manner, which means that the individual must be informed of the purposes for which their personal data will be collected, used, or disclosed, and any other relevant information that would enable them to make an informed decision.

Unless it is necessary for a reason allowable in the PDPA, consent must be obtained from a data subject to collect and process their data. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights regarding their data explained. This information must be provided in an accessible form, written in clear language and free of charge.

HeadHunters HQ also ensures that the consent obtained is valid and can be demonstrated, and that individuals have the right to withdraw their consent at any time, subject to any legal or contractual restrictions. The record of the consent obtained, including when and how it was obtained will be kept by HeadHunters HQ.

If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

2.6 Privacy by Design

HeadHunters HQ has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues.

HeadHunters HQ considers privacy and data protection issues throughout the entire lifecycle of personal data, from the initial collection to the eventual disposal of the data. This includes implementing technical and organisational measures such as privacy impact assessment, to safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

2.7 Transfer of personal data

Transfers of personal data outside of Singapore must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the PDPA.

Individuals' consent must be obtained before transferring their personal data outside of Singapore, except in certain situations where the transfer is necessary for a legitimate purpose and where adequate protection of the personal data is ensured.

HeadHunters HQ implements reasonable security arrangements to protect personal data during the transfer process, including during transmission and storage. This includes taking steps to ensure that the personal data is encrypted, using secure communication channels, and implementing measures to detect and prevent unauthorised access or interception.

It may be necessary for specific contractual terms to be used to cover international transfers. Where possible, these should be based on standard contractual clauses (SCCs) made available by the relevant authority.

2.8 Data Protection Officer

Under the PDPA, organizations are required to appoint a Data Protection Officer (DPO) if they are a public authority, perform large-scale monitoring, or process sensitive data on a large scale. The DPO must possess the necessary expertise and may be an in-house employee or an external service provider. HeadHunters HQ has appointed Donavan Er as our DPO; he can be reached at dpo@headhuntershq.com.

2.9 Breach notification

It is HeadHunters HQ's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the PDPA, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority like Personal Data Protection Commission (PDPC) will be notified as soon as practicable after HeadHunters HQ becomes aware of the breach. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

The notification to PDPC may includes:

a) A description of the breach, including the date and time of the breach, the type of personal data affected, and the number of individuals affected.

b) The steps that the organisation has taken or intends to take to mitigate the harm caused by the breach.

c) Contact information for a person who can provide further information about the breach.

d) Any other information that the PDPC may require.

2.10 Addressing compliance to the PDPA

The following actions are undertaken to ensure that HeadHunters HQ complies at all times with the accountability principle of the PDPA:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing

- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to countries other than Singapore including details of controls in place
- Personal data retention schedules
- Relevant technical and organisational controls in place