

Personal Data Retention and Disposal policy

Version No : 2.0

Revision History

Version #	Revision Date	Description of Changes
1.0	1 st January 2022	Initial Version
2.0	9 th May 2023	Second Version

Document Control Summary of Changes

Version #	Revision Date	Author	Nature of Change
1.0	1 st March 2022	Arpaporn Suwannoi	Initial Draft
2.0	9 th May 2023	Arpaporn Suwannoi	Second Draft

Document Change Approvals

Name	Role	Approval Date
Ms. Lilly Ngamtrakulpanit	Managing Director, ManpowerGroup Thailand	26 th April 2022
Ms. Lilly Ngamtrakulpanit	Managing Director, ManpowerGroup Thailand	9 th May 2023

1. Background

The PDPA defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one 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.

The PDPA also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the PDPA, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organizational measures required by the PDPA to protect that data).

In addition, the PDPA includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- When the data subject withdraws their consent;
- When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
- When the personal data is processed unlawfully (i.e. in breach of the PDPA);
- When the personal data has to be erased to comply with a legal obligation; or
- Where the personal data is processed for the provision of information society services to a child.

This policy (the “Policy”) sets out the type(s) of personal data held by ManpowerGroup Thailand, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the PDPA, please refer to the ManpowerGroup Thailand’s Data Privacy Policy.

2. Aims and Objectives

The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that ManpowerGroup Thailand complies fully with its obligations and the rights of data subjects under the PDPA.

In addition to safeguarding the rights of data subjects under the PDPA, by ensuring that excessive amounts of data are not retained by ManpowerGroup Thailand, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

This Policy applies to all personal data held by ManpowerGroup Thailand by its employees/ temp associates and by third-party data processors processing personal data on ManpowerGroup Thailand’s behalf.

Version No: 2.0	Revision Date 9 th May 2023	Accessibility: Internal	Page 3 of 7
--------------------	---	-------------------------	-------------

4. Data Subject Rights and Data Integrity

All personal data held by ManpowerGroup Thailand is held in accordance with the requirements of the PDPA and data subjects' rights thereunder, as set out in ManpowerGroup Thailand's Data Protection Policy.

Data subjects are kept fully informed of their rights, of what personal data ManpowerGroup Thailand holds about them, how that personal data is used, and how long ManpowerGroup Thailand will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

Data subjects are given control over their personal data held by ManpowerGroup Thailand including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict ManpowerGroup Thailand's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling.

5. Technical and Organizational Data Security Measures

The following technical measures shall be in place by ManpowerGroup Thailand to protect the security of personal data.

- All emails containing personal data must be encrypted;
- All emails containing personal data must be marked "confidential";
- Personal data may only be transmitted over secure networks using appropriate security controls;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using approved postal delivery services;
- All personal data transferred physically should be transferred in a suitable storage container marked "confidential";
- No personal data may be shared informally and if access is required to any personal data of employee/ temp associate, such access should be formally requested from data privacy lead; Please refer to the Data Subjects Right Management Procedure for the same;
- All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of ManpowerGroup Thailand or not, without authorization;
- Personal data must be handled with care at all times and should not be left unattended or on view;
- Computers used to view personal data must always be locked before being left unattended;
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of ManpowerGroup Thailand where the party in question has agreed to comply fully with ManpowerGroup Thailand's Data Protection Policy and the PDPA requirements as highlighted in respective contracts;;
- All personal data stored electronically should be backed up as per ManpowerGroup Thailand backup policies. All backups should be encrypted;

- All electronic copies of personal data should be stored securely using passwords and encryption;
- All passwords used to protect personal data should be changed regularly and should must be secure;
- Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
- No software may be installed on any ManpowerGroup Thailand-owned computer or device without approval;
- Where personal data held by the ManpowerGroup Thailand is used for marketing purposes, it shall be the responsibility of Marketing Head to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

The following organizational measures are in place within ManpowerGroup Thailand to protect the security of personal data. Please refer to ManpowerGroup Thailand's Data Protection Policy for further details:

- All employees including temp associates and other parties working on behalf of ManpowerGroup Thailand shall be made fully aware of both their individual responsibilities and ManpowerGroup Thailand's responsibilities under the PDPA and under ManpowerGroup Thailand's Privacy Policy Manual;
- Only employees including temp associates and other parties working on behalf of ManpowerGroup Thailand that need access to, and use of, personal data in order to perform their work shall have access to personal data held by ManpowerGroup Thailand. The same shall be explicitly identified as a part of their contracts;
- All employees including temporary associates and other parties working on behalf of ManpowerGroup Thailand handling personal data will be appropriately trained to do so. Training shall be provided periodically and upon initiation of employment terms;
- All employees including temporary associates and other parties working on behalf of ManpowerGroup Thailand handling personal data will be appropriately supervised;
- All employees including temporary associates and other parties working on behalf of ManpowerGroup Thailand handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed by respective account managers and departmental leads;
- All employees including temporary associates and other parties working on behalf of ManpowerGroup Thailand handling personal data will be bound by contract to comply with PDPA and ManpowerGroup Thailand's Data Protection Policy;
- All agents, contractors, or other parties working on behalf of ManpowerGroup Thailand handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of ManpowerGroup Thailand arising out of the PDPA and ManpowerGroup Thailand's Data Protection Policy; Where any agent, contractor or other party working on behalf of ManpowerGroup Thailand handling personal data fails in their obligations under PDPA and/or ManpowerGroup Thailand's Data Privacy Policy, that party shall indemnify and hold harmless the ManpowerGroup Thailand against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out in this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

Version No: 2.0	Revision Date 9 th May 2023	Accessibility: Internal	Page 5 of 7
--------------------	---	-------------------------	-------------

- Personal data stored electronically (including any and all backups thereof) shall be deleted securely beyond recognition and/or reconstruction, including deleting from Trash folders, using IT department-approved utilities or equivalent solution(s);
- Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely beyond recognition and/or reconstruction, including deleting from Trash folders, using IT department-approved utilities or equivalent solution(s);
- Personal data stored in hardcopy form shall be shredded;
- Special category personal data stored in hardcopy form shall be shredded.
- The media that contains personal data or special category of personal data must be degaussed or wiped clean with an equivalent solution, if required, before disposal. Any final disposal must involve the physical destruction of the media.
- If a media previously used to store personal data or special categories of personal data is to be reused, it must first be reformatted to prevent recovery of any previously stored data.

7. Data Retention

As stated above, and as required by law, ManpowerGroup Thailand shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- The objectives and requirements of ManpowerGroup Thailand;
- The type of personal data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- ManpowerGroup Thailand's legal basis for collecting, holding, and processing that data; and
- The category or categories of data subject to whom the data relates.

While deciding the retention period for personal data, legal and regulatory requirements from ManpowerGroup Thailand legal time shall be considered as priority in the PII inventory. Further the contractual requirements shall also be considered for defining the retention of client related personal data. While storing the personal data specifically for PDPA subject, timeline as required by the data subject should also be considered.

The regulatory requirements for storage shall always supersede the storage requirements identified by contractual requirements/ legitimate interest for processing.

Please refer to **Annexure 1 [Data Retention Template]**, **Annexure 2 [Data Retention Template for Bullhorn]**, **Annexure 3 [Data Retention Template for RightTrack]** for the retention duration of various types of personal data stored within ManpowerGroup Thailand. The duration shall be reviewed regularly to remain relevant.

Retention period thus shall be communicated across to all forms of storage mechanism including electronic and hard copy formats.

Periodic audits shall be conducted by various business leads and DPO to ensure that personal data is not stored beyond the retention period.

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organizational measures to protect the rights and freedoms of data subjects, as required by the PDPA and shall be approved by the DPO.

Version No: 2.0	Revision Date 9 th May 2023	Accessibility: Internal	Page 6 of 7
--------------------	---	-------------------------	-------------

8. Roles and Responsibilities

The Data Protection Officer (“DPO”) shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, ManpowerGroup Thailand’s other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the PDPA and other applicable data protection legislation.

DPO shall be directly responsible for ensuring compliance with the above data retention periods throughout ManpowerGroup Thailand.

Any questions regarding this Policy, the retention of personal data, or any other aspect of PDPA compliance should be referred to the DPO.

Annexure 1 Thailand Data Retention Duration

Thailand Data Retention Template

Country	Name of App or Physical Record Facility	Responsible Department	Description	Retention Duration (Year)	Statutory or Company Recommended?	Duration measured from?	Statutory Citation (if any)
Thailand	Bullhorn	Operations	Records of candidate's profile (Recruitment System)	6	Company Recommended	From the date article is created	
Thailand	Tigersoft	HR	Staff Payroll System	10	Company Recommended	From the date that the data in no longer in used	
Thailand	Powerbase	Operations	Center Office (Records of associate , candidate's profile)	6	Company Recommended	From the date that the data in no longer in used	
Thailand	Power Vision	Payroll	Associate Payroll System	6	Statutory	From the year end (December) of each year	Section 14 of ACCOUNTING ACT, B.E. 2543 (2000)/ section 19, section 193/31 of The Thai Civil and Commercial Code
Thailand	Accpac	Finance	Finance & Accounting System	6	Statutory	From the year end (December) of each year	Section 14 of ACCOUNTING ACT, B.E. 2543 (2000)/ section 19, section 193/31 of The Thai Civil and Commercial Code