



Data Privacy Policy

Current Version Number	2.0
Author	Ho Siang Yeow Chia Woon Fei
Reviewed By	Kho Kah Mun Chew Loon Huat
Review Date	12 September 2024
Approved By	Steven Wong
Approval Date	22 October 2024

Table of Contents

Overview.....	6
Scope.....	6
Glossary	6
Audiences of Document	6
General Principle	7
Notice and Choice Principle	7
Disclosure Principle.....	7
Security Principle.....	8
Retention Principle	8
Data Integrity Principle.....	9
Access Principle.....	9
Governance and Control Framework.....	9
Policy Maintenance	10
Awareness, Compliance and Breaches	10
Breach Reporting	10
Further Information	10

Document Change History

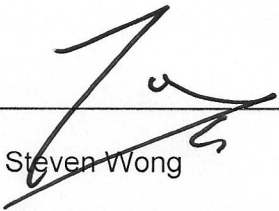
Version	Date	Updated By	Reviewed By	Approved By	Approval Date	Description
1.0	02/09/2013	Reza Sharifuddin	Chee Ping Wei	Chung Hon Cheong	02/09/2013	Document was created
1.1	28/07/2020	Ho Siang Yeow	Chew Loon Huat Kho Kah Mun	Si Tho Yoke Meng	28/07/2020	Update wordings in the policy
1.2	29/11/2023	Ho Siang Yeow	Chew Loon Huat Kho Kah Mun	Si Tho Yoke Meng	29/11/2023	Removed reference to GPIS 1 Update wordings in the policy
2.0	12/9/2024	Ho Siang Yeow Chia Woon Fei	Chew Loon Huat Kho Kah Mun	Steven Wong	22/10/2024	Review contents and renamed from e-Cover Privacy Policy to Data Privacy Policy

Revision History

Date	Reviewed By	Reason for Review	Review Result
28/07/2020	Ho Siang Yeow Chew Loon Huat Kho Kah Mun	Ad-hoc Review	Update the document as per revision in version 1.1
26/08/2021	Ho Siang Yeow Chew Loon Huat Kho Kah Mun	Annual Review	No changes
29/11/2023	Ho Siang Yeow Chew Loon Huat Kho Kah Mun	Review	Update the document as per revision in version 1.2
12/9/2024	Ho Siang Yeow Chia Woon Fei Chew Loon Huat Kho Kah Mun	Review	Update the document as per revision in version 2.0

Document Authorization

This document has been approved by



Name: Steven Wong

Designation: Executive Director

Data Privacy Policy

Overview The purpose of this policy is to provide guidance how Rexit handles Personal Information collected through business activities.

Scope

- This policy applies to existing and new projects, regardless of being software or hardware in nature.
- This Policy must be read together with applicable laws and regulations.
- Employees shall ensure that confidentiality of Personal Data is protected at all times, and that they process Personal Data in compliance with PDPA 2010.

Glossary Rexit – Rexit Berhad and all its subsidiaries.

Audiences of Document The intended audience of this document are as follows:

Audience	Application of the Document
Rexit Staff and Management	Rexit staff will use this document as a record of their roles, responsibilities and procedures. The management will use this document as a basis on checking on compliance to procedures and policies.
Regulatory Bodies	Regulatory bodies such as Bank Negara Malaysia will require documents such these and their regular execution in order to comply with information technology guidelines (GPIS 1).

Continued next page

Data Privacy Policy

Rexit recognizes the importance of protecting data privacy. Therefore, Rexit is committed to ensuring the security and confidentiality of the information provided by customers through the privacy practices outlined herein.

General Principle

- a) Under this principle, Data users are required to obtain written consent from the data subject before processing personal data.
- b) At the time of collecting Personal Data from a Data Subject, the Data Subject must be clearly informed about the core purpose of the data collection and whether or not that core purpose may be extended to other purposes.
- c) While the same requirements generally apply to both personal data and sensitive personal data, stricter rules often apply to sensitive personal data due to legal, regulatory, or internal regulations. Specifically, explicit consent is required for the processing of sensitive personal data.
- d) Personal Data must be collected only for specified, explicit and legitimate purpose(s).

Notice and Choice Principle

- a) Under this principle, personal data may be used and/or disclosed to third parties only with the consent of the data subjects, for the purposes for which it was collected, and in accordance with the privacy notice provided to the data subjects. Personal data must not be sold or disclosed to parties outside of Rexit without the express consent of the data subject or as required by law.
- b) Personal data cannot be transferred to third parties without the consent of the Data Subject. The Data Subject must also be informed about the purpose of the transmission, the identity of the recipient and the rights of the Data Subject.

Disclosure Principle

- a) Under this principle, Rexit must secure consent from the data subject for the disclosure of their data.
- b) Rexit will disclose personal information to third parties only under the following circumstances:
 - When required by Malaysian law
 - When mandated by legislation, regulation or a court order
 - To protect public interest, such as in the context of crime detection or police investigations
 - When authorized by the individual to whom the information pertains or by the relevant organization
- c) However, in order to ensure access to the full range of products and services, non-financial information may be shared with alliance partners, suppliers, and other related parties from time to time.

Continued next page

Data Privacy Policy

Security Principle

- a) Under this principle, Rexit must ensure that the location where personal data is stored is equipped to prevent any loss, misuse, modification, unauthorized or accidental access, disclosure, alteration, or destruction.
- b) Rexit must ensure that security measures are integrated into all equipment used to store personal data.
- c) It is essential that Rexit's personnel with access to personal data possess high reliability, competency, and integrity.
- d) Any transfer of the personal data are to be done in a secured manner.
- e) The security measures that Rexit should implement include, but are not limited to the following:
 - Access to IT servers is restricted in a secured location and limited to authorized employees only.
 - Access to personal data within Rexit shall be restricted to authorized employees on a 'need to know' basis.
 - A backup procedure is in place for computer-held data, including offsite backups.
 - All reasonable measures have been taken to ensure that staff are informed of Rexit's security measures and comply with them.
 - All waste papers, printouts, etc. to be disposed of carefully.
 - Passwords must be changed regularly.
 - Users must log out of the website when it is no longer in use or before leaving their computer unattended

Retention Principle

- a) In retaining personal data, Rexit must determine the duration required to fulfil the purpose for which the data was collected, in accordance with applicable laws.
- b) Rexit must outline the processes for retaining personal data. Data will be removed once it is no longer needed for its original purpose or for legal and business reasons.
- c) Rexit must have a policy on destruction or deletion of personal data and to specify the method of destroying or deleting the personal data which is in its possession or control.

Continued next page

Data Privacy Policy

Data Integrity Principle

- Personal Data collected should be relevant to the purposes for which it is to be used and (to extent necessary for those purposes) should be accurate, complete and kept up-to-date.
- Personal Data must be relevant and not excessive in relation to its intended purposes.
- Personal data must be recorded accurately and completely.
- A comprehensive examination or inspection of the requirements for keeping personal data up to date must be conducted. Rexit must implement appropriate procedures, including periodic reviews and audits, to ensure that all data is maintained accurately and up to date.

Access Principle

- a) Personal data must be kept up-to-date. A Data Subject has the right to access their personal data held by a Data User and to correct any inaccuracies, incompleteness, misleading information, or outdated data, except where access or correction is restricted by applicable laws.
- b) If personal data is provided by a third party, the Data Subject should be given an opportunity to review and, if necessary, correct the data. If the data is provided verbally to Rexit, it must be presented back to the Data Subject for review and correction if needed.
- c) Annotations to a Data Subject's documents should include only information that is provided by the Data Subject. Only accurate, objective and substantiated annotations can be added to a Data Subject documents.

Governance and Control Framework

- The CEO is ultimately responsible for ensuring that Rexit establishes policies and procedures for the collection and/or use of Personal Data which meet not only the requirements of the Rexit Data Privacy Policy but also all relevant legal, regulatory and contractual requirements.
- The DPO is the initial contact person for any data privacy issues. The DPO represent the second line of defence in the data privacy control framework and support the senior and business management in developing and implementing adequate procedures, safeguards and controls to ensure that the business meets all of its data privacy obligations.

Continued next page

Data Privacy Policy

Policy Maintenance

- This policy will be reviewed for accuracy and completeness on periodic basis and as and when required by Compliance department. Any amendments made to this policy further to this review process will be submitted to Senior Management for recommendation, and Audit & Risk Management Committee for endorsement, and obtain approval from the Board.
- Once approved, any amendments to this policy will be communicated to all employees.

Awareness, Compliance and Breaches

- All employees shall be properly informed of the Data Privacy Principles when processing personal data.
- Training will be provided at least once annually. Employees will be informed when training sessions are scheduled. Employees are responsible for attending training sessions as outlined in Rexit's training plan. Employees are expected to stay up to date with the data protection laws and regulations.

Breach Reporting

- A "Data Privacy Breach" refers to any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For example, a Data Privacy Breach would occur if Personal Data belonging to employees was disseminated to external parties without authorisation, e.g. stolen, lost or mistakenly disclosed.
- When a Data Privacy Breach occurs or when employees become aware of a Data Privacy Breach, the issue must immediately be reported to the DPO. The incident will be managed and monitored in accordance with the Rexit Incident Response Guideline.
- Employees should be aware that breaches of this Policy, or failure to act within the spirit of the Policy, will be viewed seriously by Rexit, and may result in disciplinary action, as outlined in Rexit Disciplinary Action Procedure.

Further Information

For further information about any aspect of this Policy, please contact Data Privacy Officer.

Data Privacy Officer
Rexit Software Sdn Bhd
42, Jalan BM 1/2, Taman Bukit Mayang Emas,
47301 Petaling Jaya, Selangor.
Telephone: +603-78031131
Email: dpo@rexit.com

End