Exabytes Privacy Policy (Generative AI)

This Generative AI Data Privacy Policy (this "**Policy**") outlines how Exabytes collects, uses, protects, and manages personal data, including data processed through generative AI (gen AI) technologies. The policy ensures compliance with applicable data protection laws and regulations while maintaining transparency and trust with users. Below is a detailed explanation of each subtopic:

1. Purpose

The purpose of this Policy is to establish a clear framework for how Exabytes collects, processes, stores, and protects personal data including sensitive personal data (collectively referred to as "Personal Data"), particularly when processed through generative AI (GenAI) technologies. This policy ensures Exabytes adheres to all applicable data protection laws, such as Malaysia's Personal Data Protection Act 2010 ("PDPA"), and ISO 27001, while maintaining transparency and ethical responsibility in AI-driven data handling. It also aims to outline the measures taken to safeguard personal data and establish ethical guidelines for the responsible use of AI, ensuring fairness, accuracy, and non-discrimination in AI-powered decision-making.

By clearly defining these principles, Exabytes seeks to build trust with users by ensuring their data is used responsibly and securely. This policy also mitigates risks associated with AI-related data breaches, unauthorized access, or potential misuse of personal data in AI models. Through proper governance, oversight, and compliance measures, Exabytes ensures that GenAI technology aligns with legal and ethical standards while optimizing AI-driven services.

2. Scope

This Policy applies specifically to Personal Data, that is collected, processed, or stored by Exabytes for use in generative AI systems.. It includes data that is used in generative AI systems for various tasks, such as content generation, predictive analysis, personalized recommendations, and customer interactions. Exabytes ensures that AI-driven tools operate within strict privacy guidelines, preventing unauthorized usage or unethical exploitation of user data.

The scope covers all employees, contractors, vendors, and third-party partners who interact with AI-driven data processing systems. They are required to comply with Exabytes' AI privacy and security standards, ensuring that AI models and their outcomes respect user rights and confidentiality. Additionally, this policy governs all platforms, services, and products offered by Exabytes, including websites, applications, cloud-based services, and AI-integrated tools.

Furthermore, all data processing activities—whether conducted internally or via third-party AI vendors—must follow the guidelines outlined in this policy. Any third-party AI tools or services integrated with Exabytes' systems must undergo rigorous evaluation to confirm compliance with industry regulations and ethical AI principles. Exabytes retains oversight of how AI vendors handle user data and ensures that AI systems do not introduce unintended risks, biases, or breaches of privacy.

3. Proprietary Rights

3.1 Ownership of Personal Data

Users retain full ownership of their personal data, and Exabytes processes this data strictly in accordance with applicable laws and this policy. Exabytes does not assume ownership over any personal data provided by users unless explicitly agreed upon in writing. Users have the right to control, modify, or delete their data, ensuring that their personal information is not exploited for AI model training without consent.

3.2 Generative AI Outputs

Any content, insights, or reports generated by Exabytes' AI tools are considered the property of Exabytes unless otherwise specified in a formal written agreement between the parties. . AI-generated outputs, such as automated reports, analytics, or content recommendations, are managed under Exabytes' intellectual property rights. Users may have access to AI-generated insights, but the ownership of the AI's computational results remains with Exabytes to ensure consistency and integrity in business operations.

3.3 Third-Party Data Processing

Exabytes does not claim ownership of third-party data but may process it under the conditions specified by law and this policy. If external data sources are used for AI-driven processing, they must comply with strict security and privacy standards. Any data shared with third parties must undergo proper contractual agreements to ensure that AI-powered processing does not violate user rights or introduce ethical concerns.

3.4 Usage Rights and Intellectual Property

Exabytes is granted the right to process personal data solely for the purposes outlined in this policy or as required by law. Any additional data usage beyond the defined scope requires explicit consent from users. AI-generated insights, such as reports, analytics, or trend forecasting, are considered part of Exabytes' intellectual property, ensuring that business operations benefit from AI-driven intelligence while maintaining data security and ethical compliance.

3.5 User-Generated Content and AI Processing

Users grant Exabytes a limited license to process their data through AI-driven tools, ensuring compliance with all privacy regulations. AI tools are programmed to prioritize data protection and fairness, ensuring that users' privacy and rights are respected at all times. If AI models generate personalized content based on user interactions, the system ensures that these outputs do not infringe upon users' data rights or introduce security vulnerabilities.

4. Responsibilities

4.1 Management Responsibilities

The management team is responsible for overseeing the implementation and enforcement of this policy, ensuring that all AI-driven data processing activities align with regulatory and ethical standards. This includes allocating sufficient resources for data protection measures, AI risk assessments, and compliance audits. Regular evaluations of AI models must be conducted to prevent biases, security vulnerabilities, or unintended privacy risks.

Management must also ensure that this policy remains up to date with changes in legal requirements, technological advancements, and industry best practices. Any updates to AI systems or data processing methodologies must be documented and communicated to all relevant stakeholders. Additionally, management is responsible for fostering a culture of AI ethics, ensuring that AI deployments align with principles of fairness, accountability, and transparency.

4.2 Employee Responsibilities

All employees must complete mandatory data protection and AI ethics training to ensure they understand the principles of responsible AI use. Employees handling personal data must maintain strict confidentiality and follow security protocols to prevent unauthorized access or misuse of data in AI models. Any employee who suspects a data breach or an AI system malfunction that may impact user privacy must immediately report it to the designated Data Protection Officer (DPO).

Employees are required to use AI-generated data and insights strictly for authorized purposes. AI-driven automation should not replace human oversight in decision-making processes where ethical concerns, legal compliance, or individual rights are at stake. Employees must also ensure that AI outputs are validated for accuracy and do not produce misleading or harmful content.

4.3 Third-Party Vendor Responsibilities

Any third-party vendors providing AI tools or data processing services must adhere to Exabytes' privacy and security standards. Vendors must sign legally binding agreements that ensure compliance with Exabytes' data protection policies and applicable regulations. Additionally, vendors must conduct their own audits and risk assessments to ensure their AI technologies do not introduce security vulnerabilities or ethical concerns.

If a third-party AI vendor experiences a data breach or non-compliance issue, they must immediately notify Exabytes to ensure swift remediation efforts. Vendors must also provide evidence of compliance with data protection laws upon request, ensuring that Exabytes maintains full control and visibility over AI-related data processing activities.

4.4 Data Protection Officer (DPO) Responsibilities

The DPO is responsible for monitoring compliance with data protection laws, conducting risk assessments, and ensuring that AI-driven data processing aligns with privacy standards. The DPO serves as the primary point of contact for all data protection inquiries, issues, or incidents related to AI technologies.

Regular audits and AI system evaluations must be conducted to identify potential risks, biases, or unintended consequences of generative AI outputs. The DPO must also ensure that AI systems operate ethically by reviewing AI training datasets, monitoring AI-generated content, and implementing corrective measures when necessary. Additionally, the DPO is responsible for ensuring that AI systems remain transparent and explainable to users.

5. Data Collection and Usage

5.1 Types of Data Collected

- Personally Identifiable Information (PII)

  Exabytes collects personal information such as name, email address, phone number, and government-issued identification numbers. This data may be used for identity verification, customer support, or AI-powered personalization features. All PII is processed securely and is not used for AI training unless explicit consent is obtained from the user.

- Financial Information

  Exabytes processes financial data, including payment details, billing addresses, and transaction history, to facilitate secure transactions and prevent fraud. AI-powered fraud detection systems may analyze transaction patterns to identify suspicious activity while ensuring that user financial data remains protected.

- Technical Data

  Exabytes collects technical data such as IP addresses, device information, browser types, and cookie data to enhance system security and performance. AI-driven cybersecurity tools may use this data to detect anomalies, prevent cyber threats, and improve user authentication mechanisms.

- Behavioral Data

Behavioral data, including website interactions, search history, and user preferences, is collected to improve AI-driven personalization and recommendation systems. This data helps optimize content delivery, marketing campaigns, and user engagement while ensuring compliance with privacy laws.

- Employee Data

  Employee-related data such as employment history, salary details, and performance records may be processed for HR analytics and talent management purposes. AI-driven HR tools may analyze this data to identify workforce trends and improve hiring decisions while maintaining data confidentiality.

- Purposes of Data Collection

  Exabytes collects and processes personal data to enhance AI-driven services, including customer support automation, content generation, and predictive analytics. AI models are designed to improve operational efficiency while ensuring that user data is handled responsibly.

  Additionally, data is used to improve fraud detection, security monitoring, and compliance reporting. Exabytes ensures that AI systems do not make decisions that negatively impact users without human oversight, and all AI-generated insights are regularly reviewed for accuracy and fairness.

5.2 Generative AI (GenAI) Usage

- AI-Driven Customer Support

  Generative AI-powered chatbots and virtual assistants use customer data to provide automated yet personalized support. These AI systems analyze past interactions and context to improve response accuracy, ensuring that customer inquiries are resolved efficiently while safeguarding personal data.

- AI-Generated Content

  Exabytes’ AI tools generate marketing materials, reports, and automated insights based on data-driven analysis. All AI-generated content undergoes human review to ensure that it is accurate, unbiased, and aligned with ethical guidelines.

- Data Analysis and Insights

  AI models analyze large datasets to generate business insights, trend forecasts, and risk assessments. These insights help decision-makers optimize business operations while ensuring that personal data is anonymized when necessary.

- Automation and Efficiency

AI-driven automation streamlines repetitive tasks such as document processing, data classification, and compliance monitoring. Exabytes ensures that automation does not replace human oversight in critical decision-making areas, preserving transparency and accountability.

5.3 Legal Basis for Processing

- Consent

  Explicit, informed consent from the data subject is required for AI-related data processing activities, including but not limited to personalized recommendations, targeted advertising, and the use of personal data in AI training datasets.. Where personal data is obtained from third-party sources, the disclosing party shall provide written assurance that the data subject has granted valid consent for such processing purposes in accordance with applicable data protection laws. Data subjects reserve the right to withdraw their consent at any time, and such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. Requests for withdrawal of consent may be submitted via email or through Exabytes' designated support channels.

  In the event that the data subject/user fails to provide the mandatory personal data required, Exabytes shall be unable to register, authenticate, or deliver the requested services. As a result, access to certain functionalities, digital platforms, or customer support services may be restricted or unavailable.

- Contractual Necessity

  AI-powered data processing may be necessary to fulfil contractual obligations, such as automated billing, order processing, or fraud prevention mechanisms. AI-driven operations must align with legal agreements between Exabytes and its customers.

- Legal Obligation

  Certain AI-driven data processing activities may be required to comply with legal and regulatory requirements, such as financial audits, cybersecurity monitoring, and compliance reporting. AI-generated compliance reports must remain transparent and verifiable.

- Legitimate Interest

  Exabytes may process data using AI for legitimate business interests, provided that such processing does not override individual rights. AI-driven analytics, security monitoring, and operational efficiency improvements fall under this category, but measures must be taken to prevent discriminatory or unethical AI outcomes.

6. Data Security and Protection

6.1 Encryption

Exabytes implements end-to-end encryption to safeguard personal data during both transmission and storage. AI-driven systems that process user data are integrated with encryption protocols such as AES-256 and TLS 1.2/1.3 to prevent unauthorized access. Additionally, encrypted datasets are used for AI training when necessary, ensuring that sensitive information remains protected even in AI-driven analytics.

6.2 Access Controls

Role-based access controls (RBAC) are enforced to ensure that only authorized personnel can access sensitive AI-processed data. AI models handling personal information are restricted to specific departments, such as compliance or security teams, with strict logging of all access attempts. Multi-factor authentication (MFA) and least-privilege principles are applied to prevent unauthorized interactions with AI-powered systems.

6.3 Firewalls and Intrusion Detection

Advanced cybersecurity measures, including firewalls, AI-powered threat detection, and intrusion prevention systems, are used to monitor network traffic and detect anomalies. AI-enhanced security tools continuously analyze patterns of malicious activities and block threats in real time. These AI-driven security mechanisms ensure that both structured and unstructured data are protected from cyberattacks.

6.4 Regular Audits and Compliance Checks

Exabytes conducts regular security audits and compliance assessments, typically on an annual basis, or more frequently if necessary, to ensure AI-driven systems comply with industry standards such as PDPA and ISO 27001. These audits involve reviewing AI model performance, data usage logs, and security measures to identify vulnerabilities or ethical concerns. Any identified risks are promptly addressed through corrective action plans.

6.5 Incident Response Plan

A structured incident response plan is in place to address data breaches or AI-related security incidents swiftly. In the event of unauthorized access or data leakage, an AI-powered alerting system notifies security teams for immediate action. Exabytes follows a strict protocol that includes forensic investigation, impact analysis, and user notification in compliance with regulatory requirements.

6.6 Generative AI (GenAI) Security Measures

A) Anonymized and Synthetic Data for AI Training

To minimize privacy risks, Exabytes ensures that AI training models use anonymized or synthetic datasets rather than directly processing user PII. Where real data is required, strict de-identification techniques are applied to protect individuals' identities.

B) Restricted AI Model Access

Access to AI models and their training datasets is limited to authorized data scientists and engineers. AI models handling sensitive data undergo security reviews to prevent leakage, bias, or unethical usage.

C) Compliance Monitoring of AI Outputs

AI-generated content, decisions, and insights are regularly reviewed for compliance with privacy, security, and ethical standards. Automated monitoring tools scan AI-generated outputs for potential biases, inaccuracies, or regulatory violations, ensuring that AI remains a responsible tool within Exabytes.

7. Data Retention and Deletion

7.1 Retention Period

Exabytes retains personal data only for as long as necessary to fulfill the purpose for which it was collected or as required by law. AI-driven systems follow strict retention policies that automatically purge or anonymize outdated personal data. Retention timelines vary based on data categories, ensuring compliance with regulatory requirements while minimizing unnecessary data storage.

7.2 Secure Data Deletion and Anonymization

Once personal data is no longer needed, it is securely deleted or anonymized to prevent re-identification. AI-powered data deletion mechanisms ensure that data is wiped from all storage locations, including backups, while maintaining compliance with secure deletion protocols such as NIST 800-88 guidelines (Guidelines for Media Sanitisation). Users may also request the deletion of their data, subject to legal obligations.

7.3 Archiving for Statistical and Historical Analysis

Certain AI-analyzed datasets may be archived for historical or statistical research purposes, provided they are anonymized. These archives contribute to AI model improvements, trend analysis, and security research without compromising individual privacy.

7.4 Generative AI (GenAI) Data Retention Guidelines

Data used to train AI models is retained only for as long as necessary and is securely deleted after the training process is complete. Any AI-generated content containing sensitive data undergoes strict verification to ensure it meets privacy and ethical guidelines before being stored or shared.

8. Third-Party Data Sharing and Vendors

8.1 Third-Party Vendor Compliance

Exabytes partners with third-party vendors for AI development, cloud storage, and data processing. These vendors must comply with Exabytes' strict data protection policies and sign legally binding data processing agreements (DPAs). Regular audits ensure vendors maintain security and privacy standards, preventing unauthorized use of AI-processed data.

8.2 Legal Requirements for Data Sharing

Exabytes may be required to share personal data with regulatory authorities or legal bodies to comply with laws and regulations. Any AI-driven data sharing follows legal frameworks such as PDPA, ensuring users are informed about disclosures when applicable. AI-generated reports provided to regulators undergo privacy checks to remove unnecessary personal identifiers.

8.3 Business Transfers and AI Vendor Oversight

In the event of mergers, acquisitions, or business restructuring, AI-powered systems and related users' data (including Personal Data) may be transferred to new entities, including those located outside Malaysia. Such transfers will be conducted in compliance with applicable data protection laws and with stringent measures in place to ensure that AI-stored users' data (including Personal Data) remains protected.. Additionally, AI vendors are prohibited from using Exabytes' data for their own purposes including any processing or transfer of data outside of Malaysia, except as explicitly defined agreements with Exabytes. Data subject/user will be informed of any cross-border transfers of their Personal Data, and their rights with respect to such transfers will be clearly communicated. Exabytes will ensure that all data processing activities, including cross-border transfers, comply with the principles of data protection under the PDPA, including the need for transparency, fairness, and security.

8.4 Generative AI (GenAI) Vendor Restrictions

Exabytes ensures that third-party AI vendors process data only for the intended purposes specified in contracts. Data shared with AI vendors is limited to what is strictly necessary for specific AI functionalities, reducing exposure to potential privacy risks. AI vendors must also demonstrate compliance with ethical AI principles, ensuring their models do not produce biased or misleading outputs.

9. User Rights and Control

9.1 User Data Access and Transparency

Users have the right to request access to their personal data and understand how AI models process their information. Exabytes provides transparency regarding AI-driven decision-making, ensuring that users can review AI-generated insights relevant to them.

The User Data Access Request Form is attached hereto as Appendix I.

9.2 Data Correction and Rectification

Users can request corrections to inaccurate or incomplete data stored in AI-driven systems. AI-based recommendations or predictions that affect user experiences are reviewed for accuracy, ensuring fair and correct information is provided.

The User Data Rectification Request Form is attached hereto as Appendix II.

9.3 Data Erasure

Users may request the deletion of their personal data, subject to legal and business obligations. Additionally, users can opt out of having their data used for AI training or automated decision-making, ensuring they have full control over AI interactions.

Users have the right to request the deletion of their Personal Data. Upon such a request, Exabytes shall take all reasonable steps to delete the personal data in its possession, except where retention of the data is required or permitted under applicable laws, regulations, or for legitimate business purposes. Requests for deletion may be submitted via email or through Exabytes' designated support channels.

While Exabytes will delete Personal Data as promptly and securely as possible, some data may not be fully deletable due to the nature of AI model training or legal requirements. Users will be notified where data deletion is not possible.

9.4 Ethical Considerations

Users can request explanations of how their data contributes to AI-generated content or decisions. If AI models influence important decisions (e.g., credit scoring, hiring, or security assessments), users have the right to challenge automated outcomes and request human review.

10. Incident Response and Breach Notification

10.1 AI-Powered Incident Detection

Exabytes utilizes AI-enhanced security monitoring tools to detect anomalies, potential data breaches, or unauthorized AI access in real time. These systems continuously analyze AI activity logs, flagging suspicious patterns for investigation.

10.2 Breach Notification and Response Protocols

In the event of a data breach involving AI-driven data processing, Exabytes adheres to the strict notification guidelines set forth under the amended PDPA. As required by the amendments, regulatory authorities, including the Personal Data Protection Commissioner, will be notified within 72 hours of detection of the breach. Affected users i.e. data subjects will be informed of the breach within 7 days, detailing the nature of the breach, potential consequences, and measures taken to mitigate the impact. Exabytes' incident response teams will implement appropriate mitigation strategies to contain and resolve the security issues promptly.

10.3 AI-Specific Incident Handling

Any security incidents related to AI model vulnerabilities, bias detection, or ethical concerns are addressed with the same urgency as traditional data breaches. AI-driven response mechanisms help identify root causes, prevent future risks, and reinforce AI security policies.

11. Employee Training and Awareness

11.1 Comprehensive Training Programs on AI and Data Privacy

All employees undergo mandatory training programs that cover data protection laws, security best practices, and the ethical use of Generative AI (GenAI). These programs ensure that employees understand how AI systems handle personal data and their responsibilities in safeguarding user privacy. Training includes real-world scenarios, case studies, and role-based exercises to prepare employees for data protection challenges in an AI-driven environment.

11.2 AI Ethics and Responsible Usage Awareness Campaigns

To ensure continuous awareness, Exabytes conducts periodic campaigns highlighting ethical AI practices and responsible data handling. These campaigns include newsletters, webinars, and internal discussions to keep employees updated on AI developments, potential risks, and evolving regulatory requirements. Employees are encouraged to actively participate in shaping AI policies by reporting ethical concerns or suggesting improvements.

11.3 Monitoring and Evaluation of Employee Compliance

Employees' adherence to AI privacy policies is regularly assessed through compliance audits, knowledge assessments, and role-specific evaluations. Any non-compliance or negligent handling of AI-processed data results in corrective actions, including retraining or disciplinary measures. Exabytes fosters a culture of accountability where employees are empowered to uphold AI transparency and fairness.

12. Monitoring and Accountability

12.1 Regular Internal and External Audits

Exabytes conducts periodic internal audits and engages external auditors to evaluate AI compliance with privacy laws and ethical guidelines. These audits assess AI models, data processing activities, and security measures to ensure continued alignment with industry standards such as PDPA, ISO 27001, and NIST AI Risk Management Framework. Any identified gaps are addressed through updated policies and system improvements.

12.2 Incident and Compliance Reporting Mechanisms

Employees, partners, and users can report AI privacy concerns or security incidents through designated communication channels. A dedicated AI compliance team reviews reports, investigates potential violations, and ensures appropriate actions are taken. These reporting mechanisms promote transparency and accountability in AI-driven operations.

12.3 Documentation of AI Model Training and Data Processing

To maintain accountability, Exabytes documents all AI training datasets, model updates, and data processing activities. This documentation includes data sources, anonymization techniques, bias mitigation strategies, and model validation results. By keeping thorough records, Exabytes ensures that AI-generated outputs remain transparent, reliable, and legally compliant.

12.4 AI System Monitoring for Fairness and Bias

Exabytes actively monitors AI models to detect and mitigate biases that could result in unfair outcomes. AI-generated decisions, content, and recommendations undergo regular reviews to ensure compliance with fairness and non-discrimination principles. If an AI model exhibits biased behavior, corrective actions—such as retraining with diverse datasets or adjusting algorithm parameters—are implemented.

13. Ethical Considerations

13.1 Transparency in AI Data Processing

Exabytes is committed to full transparency regarding how AI systems collect, analyze, and generate insights from user data. Users are informed about AI usage in data processing through privacy policies, consent forms, and AI-generated content disclaimers. Clear documentation is provided for any automated decision-making processes affecting individuals.

13.2 Fair and Non-Discriminatory AI Systems

AI models deployed by Exabytes are designed to uphold fairness and avoid discriminatory outcomes. Bias detection tools analyze AI-generated content to ensure inclusivity and equal representation. If AI models demonstrate any unintended biases, corrective measures are implemented to align with ethical AI principles and diversity standards.

13.3 User Privacy as a Priority in AI Development

Privacy-by-design principles are embedded into AI systems, ensuring that data protection is considered at every stage of AI model development. Personal information is anonymized, access to AI systems is restricted, and user consent is obtained before AI-driven data processing. Exabytes prioritizes user privacy when designing AI solutions, ensuring ethical data handling practices are followed.

13.4 Bias Mitigation and Responsible AI Deployment

Exabytes actively works to identify, reduce, and eliminate biases within AI algorithms through continuous monitoring, diverse training data, and human oversight. AI engineers and compliance teams collaborate to ensure that AI-generated content and decisions remain impartial, accurate, and ethical. AI-generated outputs are regularly tested against fairness benchmarks to prevent discrimination or misinformation.

13.5 Human Oversight of AI Decision-Making

To prevent AI from making unchecked decisions, Exabytes incorporates human oversight in all AI-driven processes that affect individuals. AI-generated decisions that impact financial transactions, security assessments, or user access require human review before final implementation. Human intervention ensures accountability, ethical reasoning, and fairness in AI-powered decision-making.

14. Review and Conclusion

14.1 Annual Policy Review and Updates

Exabytes reviews this Generative AI Data Privacy Policy annually, or as needed, to reflect changes in regulations, technological advancements, and business practices. Policy updates are based on audit findings, user feedback, and evolving ethical AI standards. Employees, partners, and stakeholders are informed of any significant changes to ensure continued compliance and transparency.

14.2 Commitment to AI Privacy and Security

Exabytes remains committed to maintaining the highest standards of AI privacy, security, and ethical responsibility. By adopting a privacy-first approach, implementing robust security measures, and fostering transparency in AI operations, Exabytes ensures that user trust and regulatory compliance remain top priorities.

14.3 Encouraging AI Innovation with Responsibility

While Exabytes embraces AI-driven innovation, it does so with a strong focus on ethical AI usage and responsible data handling. The organization continuously invests in AI research and development while ensuring that AI applications align with privacy, security, and fairness principles.

14.4 User Engagement and Feedback on AI Policies

Users, employees, and stakeholders are encouraged to provide feedback on AI policies and data privacy practices. Exabytes values user input and actively incorporates feedback into AI governance strategies to enhance trust, accountability, and ethical AI implementation.

Appendix I

User Data Access Request Form

A. Applicant's Information

i. Full Name
ii. IC/Passport No.
iii. Contact Number
iv. Email Address
v. Company Name

B. Data Access Request

Please indicate the type(s) of data you wish to access (tick where applicable):

☐ Personal identification data
☐ Financial or billing information
☐ AI-generated insights or recommendations
☐ Behavioral or usage data
☐ Employee data
☐ Other (please specify): ______________________________

C. Reason for Request

(Please briefly state your reason for requesting access to the data.)

D. Declaration

I confirm and certify that the information provided in this form and any documents submitted are true and accurate. I understand that Exabytes may request additional information to verify my identity and process this request in accordance with the Personal Data Protection Act 2010.

Signature: ____________________

Date: ________________________

Appendix II

User Data Rectification Request Form

A. Applicant’s Information

i. Full Name
ii. IC/Passport No.
iii. Contact Number
iv. Email Address
v. Company Name (if applicable)

B. Data To Be Corrected

Please describe the data you believe is incorrect or incomplete, and specify the corrections required.

Personal Data Item (e.g. name, postal address, telephone number, etc.)	Before Correction	After Correction

C. Supporting Documentation

D. Declaration

I confirm and certify that the information provided in this form and any documents submitted are true and accurate. I understand that Exabytes may require verification before updating my personal data and will process this request in line with the Personal Data Protection Act 2010.

Signature: ____________________

Date: ________________________

Document version record:

Version	Prepared/Modified by	Release Date	Content/Reason of Modification	Reviewed and approved by
1.0			**New Publish**	