ក្រុមហ៊ុន ធី ឯ.ក

COMMO T CO., LTD.

PRIVACY POLICY

Effective date 01st January 2026

Version: 01

TABLE OF CONTENTS

PART I –INTRODUCTION

1. Scope

1.1 This Privacy Policy applies to all prospective Clients, existing Clients, website visitors, and other individuals whose personal data is collected, processed, used, stored, or disclosed by COMMOT CO., LTD. in connection with its business operations and services.

1.2 This Privacy Policy applies to personal data collected through the Company's website, trading platform, mobile applications (if applicable), account opening process, customer support services, electronic communications, business correspondence, and any other interactions between the Client and the Company.

1.3 This Privacy Policy applies throughout the entire business relationship between the Client and the Company, including the period before account opening, during the provision of services, and after the business relationship has ended where the Company is required to retain personal data under applicable laws, regulatory requirements, or legitimate business purposes.

1.4 This Privacy Policy should be read together with the Company's Terms and Conditions, Risk Disclosure Statement, Complaint Handling Policy, and any other documents relating to the Company's services.

2. Purpose of this Privacy Policy

2.1 The purpose of this Privacy Policy is to explain how the Company collects, uses, stores, protects, shares, retains, and otherwise processes personal data in connection with the provision of its derivative brokerage services.

2.2 The Company is committed to protecting the privacy, confidentiality, integrity, and security of personal data and processing such information responsibly and in accordance with applicable laws, regulations, and regulatory requirements.

2.3 This Privacy Policy is intended to help Clients understand:

a. what personal data the Company collects;
b. how personal data is collected;
c. why personal data is collected;
d. how personal data is used and protected;
e. when personal data may be shared with third parties;
f. how long personal data is retained; and
g. the rights available to Clients regarding their personal data.

2.4 By opening an account or using the Company's services, the Client acknowledges that the Company may collect, use, store, disclose, and otherwise process personal data in accordance with this Privacy Policy and applicable laws, regulations, and regulatory requirements.

3. Definitions

For the purposes of this Privacy Policy:

- "*Company*" means COMMOT CO., LTD., a licensed Derivative Broker established under the laws of the Kingdom of Cambodia.
- "*Client*" means any individual or legal entity that applies for, opens, maintains, or uses an account or services provided by the Company.
- "*Personal Data*" means any information relating to an identified or identifiable individual, whether collected directly or indirectly, including identification details, contact information, financial information, and any other information processed by the Company.
- "*Processing*" means any operation performed on Personal Data, including collection, recording, organization, storage, use, consultation, disclosure, transmission, updating, correction, restriction, retention, deletion, destruction, or any other handling of Personal Data.
- "*Third Party*" means any person, company, organization, service provider, professional adviser, regulator, governmental authority, approved financial institution, Central Counterparty (CCP), or other entity to whom Personal Data may be disclosed in accordance with applicable laws, regulatory requirements, or this Privacy Policy.
- "*Applicable Laws*" means all laws, regulations, regulatory requirements, directives, guidelines, and other legally binding requirements applicable to the Company's business operations in the Kingdom of Cambodia.

4. Application of this Privacy Policy

4.1 This Privacy Policy applies to all Personal Data processed by the Company in connection with the provision of derivative brokerage services.

4.2 This Privacy Policy applies regardless of whether Personal Data is collected electronically, in paper form, verbally, or through any other lawful means.

4.3 This Privacy Policy does not apply to third-party websites, applications, or services that are not owned or controlled by the Company, even where links to such websites are available through the Company's website or services.

4.4 Where applicable laws or regulatory requirements impose additional obligations regarding the processing of Personal Data, the Company shall comply with those obligations to the extent required.

PART II – PERSONAL DATA WE COLLECT

5. Personal Data Provided by Clients

5.1 The Company may collect Personal Data directly from Clients during the account opening process, throughout the business relationship, or when Clients use the Company's products or services.

5.2 The Personal Data collected may include, but is not limited to:

a. full name;
b. nationality;
c. date and place of birth;
d. gender;
e. residential or mailing address;
f. telephone number;
g. email address;
h. national identification card, passport, or other government-issued identification documents;
i. tax identification number, where applicable;
j. occupation and employment information;
k. financial information relevant to the Company's services;
l. bank account information used for deposits, withdrawals, or settlement purposes;
m. signature specimens; and
n. any other information reasonably required to establish, maintain, or administer the Client relationship or to comply with applicable laws and regulatory requirements.

5.3 The Company may request additional information or supporting documents where necessary to verify the Client's identity, assess the Client's eligibility, comply with regulatory obligations, or provide the requested products or services.

6. Information Collected Automatically

6.1 When Clients access the Company's website, trading platform, or other electronic services, certain information may be collected automatically.

6.2 Automatically collected information may include:

a. Internet Protocol (IP) address;
b. browser type and version;
c. operating system;

d. device type;
e. language settings;
f. login information;
g. access dates and times;
h. website usage information;
i. trading platform activity logs; and
j. other technical information generated through the use of the Company's electronic services.

6.3 Automatically collected information is used to improve system security, maintain service quality, support technical operations, investigate operational issues, detect unauthorized activities, and enhance the Client experience.

7. Information Received from Third Parties

7.1 Where permitted by applicable laws and regulatory requirements, the Company may obtain Personal Data from third parties.

7.2 Such information may be obtained from:

a. government authorities;
b. regulators;
c. approved financial institutions;
d. Central Counterparties (CCPs);
e. identity verification service providers;
f. sanctions screening providers;
g. fraud prevention agencies;
h. publicly available sources; or
i. other lawful sources.

7.3 Information obtained from third parties may be used to verify identity, conduct customer due diligence (KYC), comply with anti-money laundering and counter-terrorist financing (AML/CFT) requirements, prevent fraud, investigate suspicious activities, comply with regulatory obligations, or provide the Company's services.

8. Sensitive Personal Data

8.1 Where necessary and permitted by applicable laws and regulatory requirements, the Company may collect or process certain categories of sensitive Personal Data for the purpose of complying with legal, regulatory, or contractual obligations.

8.2 Sensitive Personal Data may include information contained in identification documents, biometric verification information (where applicable), or other information required for identity verification, customer due diligence (KYC), anti-money laundering and counter-terrorist financing (AML/CFT) compliance, or other regulatory requirements.

8.3 The Company will take appropriate measures to protect sensitive Personal Data and restrict access to authorized personnel who require such information for legitimate business or regulatory purposes.

8.4 The Company will not collect or process sensitive Personal Data beyond what is reasonably necessary for the provision of its services or compliance with applicable laws and regulatory requirements.

PART III – HOW WE COLLECT PERSONAL DATA

9. Account Opening and Client Onboarding

9.1 The Company collects Personal Data directly from Clients during the account opening process and throughout the Client onboarding procedures.

9.2 Clients may be required to provide Personal Data and supporting documents necessary for identity verification, customer due diligence (KYC), anti-money laundering and counter-terrorist financing (AML/CFT) compliance, suitability assessment, account administration, and other regulatory requirements.

9.3 Where necessary, the Company may request additional information or supporting documents to verify the accuracy, completeness, or authenticity of information provided by the Client.

9.4 The Company may decline to establish or continue a business relationship where the required information or documentation is not provided, cannot be verified, or does not satisfy applicable legal or regulatory requirements.

10. Website and Online Services

10.1 The Company may collect Personal Data when Clients or visitors access or use the Company's website, online portal, mobile applications (where applicable), or other electronic services.

10.2 Personal Data may be collected through online application forms, account registration, contact forms, subscription requests, website cookies, system logs, and other electronic interactions.

10.3 The Company may also collect technical information necessary to maintain website security, improve system performance, prevent unauthorized access, and enhance user experience.

11.Trading Platform and Electronic Services

11.1 The Company may collect information relating to the Client's use of the trading platform and other electronic services provided by or on behalf of the Company.

11.2 Such information may include login records, trading activity, account activity, transaction records, technical system logs, device information, security events, and other operational records necessary for the administration of the Company's services.

11.3 Information collected through the trading platform may be used for account administration, transaction processing, regulatory compliance, fraud prevention, cybersecurity, operational monitoring, dispute resolution, and service improvement.

12.Communications with Clients

12.1 The Company may collect Personal Data through communications between the Client and the Company.

12.2 Communications may include meetings, telephone conversations, emails, letters, online messaging, customer support requests, complaints, surveys, or other lawful communication channels.

12.3 Where permitted by applicable laws and regulatory requirements, the Company may maintain records of communications for quality assurance, dispute resolution, regulatory compliance, staff training, security monitoring, and record keeping purposes.

13.Regulatory and Compliance Requirements

13.1 The Company may collect, verify, update, or otherwise process Personal Data where necessary to comply with applicable laws, regulations, and regulatory requirements.

13.2 This may include information collected for customer due diligence (KYC), anti-money laundering and counter-terrorist financing (AML/CFT), sanctions screening, fraud prevention, regulatory reporting, tax reporting (where applicable), and other legal or compliance obligations.

13.3 Where required by applicable laws or regulatory requirements, the Company may request updated Personal Data or supporting documentation during the course of the business relationship.

13.4 The Client is responsible for ensuring that the Personal Data provided to the Company remains accurate, complete, and up to date throughout the business relationship.

PART IV – HOW WE USE PERSONAL DATA

14. Account Administration

14.1 The Company uses Personal Data to establish, administer, maintain, and manage the Client's account throughout the business relationship.

14.2 Personal Data may be used to verify the Client's identity, process account applications, maintain account records, update Client information, communicate with the Client, and provide ongoing account administration services.

14.3 The Company may also use Personal Data to respond to Client enquiries, process requests, provide notices, and maintain accurate records relating to the Client's account.

15. Identity Verification and Customer Due Diligence (KYC)

15.1 The Company uses Personal Data to verify the identity of Clients and beneficial owners in accordance with applicable laws, regulations, and regulatory requirements.

15.2 Personal Data may be used to perform customer due diligence (KYC), ongoing customer monitoring, sanctions screening, identity verification, and other compliance procedures required by applicable laws and regulatory requirements.

15.3 The Company may request updated information or supporting documents whenever necessary to maintain accurate Client records or comply with regulatory obligations.

16. Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT)

16.1 The Company processes Personal Data to comply with applicable anti-money laundering, counter-terrorist financing, sanctions, fraud prevention, and other financial crime prevention requirements.

16.2 Personal Data may be used for transaction monitoring, customer risk assessment, investigation of unusual or suspicious activities, regulatory reporting, and compliance with legal obligations.

16.3 Where required by applicable laws or regulatory requirements, the Company may disclose relevant information to competent regulatory authorities or other authorized persons.

17. Trading Services and Client Account Operations

17.1 The Company uses Personal Data to provide derivative brokerage services, facilitate account operations, process transactions, maintain trading records, and administer services requested by the Client.

17.2 Personal Data may be used to support trading activities, account management, operational monitoring, transaction verification, reconciliation, and service administration.

17.3 Where applicable, Personal Data may be processed in connection with settlement arrangements involving approved financial institutions, Central Counterparties (CCPs), or other authorized service providers.

18. Client Money Administration

18.1 The Company may process Personal Data relating to deposits, withdrawals, settlement instructions, bank account verification, and other activities associated with Client Money administration.

18.2 Personal Data is processed solely for the purpose of facilitating authorized banking and settlement arrangements in accordance with applicable laws, regulatory requirements, and the Company's operating procedures.

18.3 The Company does not hold, own, use, or otherwise deal with Client Money except as permitted under applicable laws, regulatory requirements, and the Company's approved operating arrangements.

19. Regulatory Reporting and Compliance

19.1 The Company may process Personal Data to comply with applicable laws, regulations, regulatory requirements, court orders, lawful requests from competent authorities, and other legal obligations.

19.2 Personal Data may be used for regulatory reporting, inspections, audits, investigations, licensing requirements, record keeping, internal controls, and compliance monitoring.

19.3 Where required by law or regulatory requirement, the Company may disclose Personal Data to competent regulatory authorities or other authorized governmental bodies.

20. Customer Support and Communication

20.1 The Company may use Personal Data to communicate with Clients regarding their accounts, products, services, operational matters, regulatory notices, or other information relevant to the business relationship.

20.2 Personal Data may also be used to respond to enquiries, provide customer support, resolve operational issues, and improve the quality of the Company's services.

20.3 Where permitted by applicable laws and regulatory requirements, communications between the Company and the Client may be recorded or retained for quality assurance, dispute resolution, compliance monitoring, staff training, and record keeping purposes.

21. Complaint Handling and Dispute Resolution

21.1 The Company may process Personal Data to receive, investigate, manage, and resolve complaints submitted by Clients or other affected persons.

21.2 Personal Data may be used to investigate disputes, verify relevant facts, communicate with the parties involved, maintain complaint records, and comply with applicable laws and regulatory requirements.

21.3 Information relating to complaints may be retained in accordance with the Company's Complaint Handling Policy and applicable record retention requirements.

22. Business Operations and Service Improvement

22.1 The Company may process Personal Data to improve its products, services, operational processes, system performance, security controls, internal administration, and overall Client experience.

22.2 Personal Data may also be used for internal reporting, statistical analysis, operational planning, risk management, quality assurance, business continuity, staff training, system testing, and other legitimate business purposes.

22.3 Where practical, the Company will use aggregated, anonymized, or de-identified information for analytical or reporting purposes whenever individual identification is not required.

PART V – DISCLOSURE OF PERSONAL DATA

23. General Principles

23.1 The Company respects the confidentiality of Personal Data and will not sell, rent, trade, or otherwise disclose Personal Data to third parties except as permitted or required by applicable laws, regulations, regulatory requirements, this Privacy Policy, or with the Client's consent.

23.2 Where disclosure of Personal Data is necessary, the Company will disclose only the information reasonably required for the relevant purpose.

23.3 The Company takes reasonable steps to ensure that third parties receiving Personal Data are required to maintain appropriate standards of confidentiality and security.

24. Affiliates and Group Companies

24.1 The Company may disclose Personal Data to its affiliated companies where reasonably necessary for internal administration, operational support, risk management, compliance, information technology services, or other legitimate business purposes.

24.2 Any disclosure to affiliated companies shall be limited to the extent reasonably necessary for the relevant purpose and subject to appropriate confidentiality obligations.

25. Central Counterparty (CCP) and Approved Financial Institutions

25.1 Where necessary for the provision of the Company's services, Personal Data may be disclosed to the Central Counterparty (CCP), approved financial institutions, payment service providers, settlement institutions, or other authorized financial service providers.

25.2 Such disclosure may be necessary to facilitate account administration, transaction processing, settlement activities, banking services, Client Money administration, operational support, or compliance with applicable laws and regulatory requirements.

25.3 The Company will disclose only the information reasonably necessary for the relevant service or regulatory purpose.

26. Service Providers

26.1 The Company may engage third-party service providers to perform services on its behalf.

26.2 Such service providers may include providers of:

a. information technology services;
b. cloud hosting services;
c. cybersecurity services;
d. identity verification services;
e. sanctions screening services;
f. document management services;
g. customer support services;
h. professional consulting services; or
i. other business support services.

26.3 The Company requires service providers to use Personal Data only for the purposes for which it was disclosed and to maintain appropriate confidentiality and security measures.

27. Regulators and Government Authorities

27.1 The Company may disclose Personal Data where required or permitted by applicable laws, regulations, regulatory requirements, court orders, or lawful requests from competent regulatory authorities or governmental agencies.

27.2 Such disclosure may be made for licensing, supervision, inspection, investigation, enforcement, regulatory reporting, or other lawful purposes.

27.3 Where permitted by law, the Company may notify the Client before disclosing Personal Data to governmental authorities. However, the Company may be prohibited from providing such notice in certain circumstances.

28. Professional Advisers

28.1 The Company may disclose Personal Data to its professional advisers where reasonably necessary for legitimate business purposes.

28.2 Professional advisers may include external legal advisers, auditors, accountants, compliance consultants, or other professional advisers engaged by the Company.

28.3 Professional advisers receiving Personal Data are expected to maintain confidentiality in accordance with applicable professional obligations.

29.Business Transfers

29.1 If the Company undergoes a merger, acquisition, corporate restructuring, sale of business, transfer of assets, or similar transaction, Personal Data may be disclosed or transferred to the extent reasonably necessary for the completion of the transaction.

29.2 Any successor or acquiring entity shall be expected to continue protecting Personal Data in accordance with applicable laws and regulatory requirements.

30.Legal Requirements

30.1 The Company may disclose Personal Data where necessary to:

a. comply with applicable laws, regulations, or regulatory requirements;
b. protect the Company's legal rights or legitimate interests;
c. prevent fraud, financial crime, money laundering, terrorist financing, cybercrime, or other unlawful activities;
d. establish, exercise, or defend legal claims; or
e. protect the rights, property, or safety of the Company, its Clients, employees, or other persons.

30.2 Where disclosure is required by law, the Company will disclose only the information reasonably necessary to satisfy the relevant legal or regulatory obligation.

PART VI – DATA SECURITY

31.Protection of Personal Data

31.1 The Company is committed to protecting Personal Data against unauthorized access, collection, use, disclosure, alteration, loss, destruction, or any other form of unauthorized processing.

31.2 The Company implements appropriate administrative, technical, and physical safeguards designed to protect Personal Data throughout its lifecycle.

31.3 Security measures adopted by the Company are reviewed periodically and may be updated where necessary to address changes in technology, operational requirements, cybersecurity risks, and applicable laws or regulatory requirements.

32. Access Control

32.1 Access to Personal Data is restricted to authorized personnel who require such access for the performance of their official duties.

32.2 Authorized personnel shall access and process Personal Data only to the extent necessary for legitimate business purposes and in accordance with the Company's internal policies, procedures, and applicable laws.

32.3 The Company maintains appropriate access control measures to help prevent unauthorized access, misuse, alteration, or disclosure of Personal Data.

33. Confidentiality

33.1 Directors, management, employees, representatives, contractors, and other persons authorized to process Personal Data are required to maintain the confidentiality of Personal Data obtained during the course of their duties.

33.2 Confidentiality obligations continue after the termination of employment, engagement, contractual relationship, or other association with the Company, to the extent required by applicable laws, contractual obligations, or regulatory requirements.

33.3 The Company may require employees, contractors, or service providers to comply with confidentiality obligations before being granted access to Personal Data.

34. Cybersecurity and Information Security

34.1 The Company implements reasonable cybersecurity and information security measures designed to protect Personal Data and information systems from unauthorized access, cyber threats, malware, ransomware, phishing attacks, data breaches, and other security risks.

34.2 The Company may implement security monitoring, authentication controls, encryption, network protection, system monitoring, vulnerability management, backup procedures, and other appropriate security measures to protect Personal Data.

34.3 While the Company takes reasonable steps to protect Personal Data, no electronic system, communication network, or method of data transmission can be guaranteed to be completely secure.

34.4 Clients are responsible for protecting their own account credentials, passwords, authentication methods, devices, and other security information used to access the Company's services.

35. Personal Data Breach Management

35.1 The Company will take reasonable steps to investigate any actual or suspected Personal Data breach that may affect the confidentiality, integrity, or availability of Personal Data.

35.2 Where appropriate, the Company may implement measures to contain, investigate, mitigate, and remediate the impact of a Personal Data breach.

35.3 Where required by applicable laws, regulations, or regulatory requirements, the Company may notify competent regulatory authorities and affected individuals of a Personal Data breach.

35.4 The Company will review significant Personal Data breaches and, where appropriate, improve its internal controls, policies, procedures, or security measures to reduce the risk of similar incidents occurring in the future.

PART VII – DATA RETENTION

36. Retention of Personal Data

36.1 The Company will retain Personal Data only for as long as necessary to fulfil the purposes for which it was collected, including the provision of services, account administration, legal obligations, regulatory compliance, dispute resolution, and legitimate business purposes.

36.2 The Company may retain Personal Data for longer periods where required or permitted by applicable laws, regulations, regulatory requirements, court orders, or other lawful obligations.

36.3 The retention period for different categories of Personal Data may vary depending on the nature of the information, the services provided, legal requirements, and operational needs.

37. Record Retention

37.1 The Company maintains records relating to Clients, transactions, communications, complaints, regulatory matters, and other business activities in accordance with applicable laws, regulatory requirements, and the Company's Record Retention Policy.

37.2 Records that may be retained include, but are not limited to:

a. account opening documentation;
b. customer due diligence (KYC) records;
c. anti-money laundering and counter-terrorist financing (AML/CFT) records;
d. transaction and trading records;
e. deposit, withdrawal, and settlement records;
f. communications between the Company and the Client;
g. complaint handling records;
h. regulatory reporting records;
i. audit records; and
j. other records required by applicable laws, regulatory requirements, or the Company's internal policies.

37.3 Where applicable laws or regulatory requirements require records to be retained for a specified minimum period, the Company will retain those records for at least that period.

38.Secure Disposal of Personal Data

38.1 Where Personal Data is no longer required for the purposes for which it was collected and there is no legal or regulatory requirement to retain it, the Company may securely delete, destroy, anonymize, or otherwise dispose of such Personal Data.

38.2 The Company will take reasonable steps to ensure that the disposal of Personal Data is carried out in a secure manner designed to prevent unauthorized access, recovery, disclosure, or misuse.

38.3 Where deletion of Personal Data is requested by a Client, the Company will consider the request in accordance with applicable laws, regulatory requirements, and its legal obligations.

38.4 The Company may decline or delay a request to delete Personal Data where retention is required for legal, regulatory, compliance, accounting, audit, dispute resolution, fraud prevention, anti-money laundering, counter-terrorist financing, or other legitimate business purposes.

PART VIII – CLIENT RIGHTS

39.Right to Access Personal Data

39.1 Clients may request information regarding the Personal Data held by the Company relating to them, subject to applicable laws, regulations, and regulatory requirements.

39.2 Where permitted by applicable laws and regulatory requirements, the Company may provide a copy of the Client's Personal Data or other relevant information maintained by the Company.

39.3 The Company may request sufficient information to verify the identity of the person making the request before providing access to Personal Data.

39.4 The Company may refuse or limit access where permitted or required by applicable laws, regulations, or regulatory requirements.

40. Right to Correct Personal Data

40.1 Clients are responsible for ensuring that the Personal Data provided to the Company is accurate, complete, and up to date.

40.2 Clients may request the correction or updating of inaccurate, incomplete, or outdated Personal Data maintained by the Company.

40.3 The Company may request supporting documents where reasonably necessary to verify the requested correction.

41. Withdrawal of Consent

41.1 Where the processing of Personal Data is based on the Client's consent, the Client may withdraw that consent at any time by notifying the Company.

41.2 Withdrawal of consent shall not affect the lawfulness of processing carried out before the withdrawal of consent.

41.3 Where Personal Data is required for the provision of the Company's services or to comply with applicable laws, regulations, or regulatory requirements, withdrawal of consent may affect the Company's ability to provide certain products or services.

42. Restriction of Processing

42.1 Clients may request that the Company restrict the processing of Personal Data where permitted by applicable laws and regulatory requirements.

42.2 The Company may continue processing Personal Data where such processing is required to comply with legal obligations, regulatory requirements, contractual obligations, fraud prevention, dispute resolution, or other legitimate business purposes.

43.Complaints and Privacy Requests

43.1 Clients who have questions, concerns, or complaints regarding the processing of their Personal Data may contact the Company using the contact details provided in this Privacy Policy.

43.2 The Company will review and respond to privacy-related requests or complaints within a reasonable period, taking into account the nature and complexity of the request and applicable legal or regulatory requirements.

43.3 The Company may request additional information to verify the identity of the person submitting a privacy request before taking any action.

43.4 Where a Client is dissatisfied with the Company's response, the Client may pursue any rights or remedies available under applicable laws.

PART IX – COOKIES AND WEBSITE TECHNOLOGIES

44.Cookies

44.1 The Company's website may use cookies and similar technologies to improve website functionality, enhance user experience, maintain website security, and support the provision of the Company's online services.

44.2 Cookies are small text files that may be stored on a user's device when visiting the Company's website. Cookies help the website recognize returning visitors and improve the performance and functionality of the website.

44.3 The Company may use cookies for purposes including:

a. maintaining website security;
b. remembering user preferences;
c. improving website performance;
d. supporting account login functions;
e. analyzing website usage; and
f. improving the quality of the Company's online services.

45.Website Analytics

45.1 The Company may collect statistical or analytical information regarding the use of its website and online services to better understand website performance and user experience.

45.2 Information collected for analytical purposes is used to improve the Company's website, products, services, security measures, and operational efficiency.

45.3 Where practical, analytical information will be aggregated or anonymized and will not be used to identify individual users unless required for security, legal, or regulatory purposes.

46.Browser Settings and Cookie Preferences

46.1 Most internet browsers allow users to manage, disable, or delete cookies through their browser settings.

46.2 Clients who choose to disable cookies should be aware that certain features or functions of the Company's website or online services may not operate properly.

46.3 By continuing to use the Company's website, Clients acknowledge that cookies may be used in accordance with this Privacy Policy unless they have disabled cookies through their browser settings.

PART X – GENERAL PROVISIONS

47.Changes to this Privacy Policy

47.1 The Company may amend, revise, update, or replace this Privacy Policy from time to time to reflect changes in applicable laws, regulations, regulatory requirements, business operations, technologies, products, services, or internal practices.

47.2 The latest version of this Privacy Policy will be made available on the Company's website or through other communication channels determined by the Company.

47.3 Clients are encouraged to review this Privacy Policy periodically to remain informed of how the Company collects, uses, stores, discloses, and protects Personal Data.

47.4 Where required by applicable laws or regulatory requirements, the Company will notify Clients of material changes to this Privacy Policy through appropriate communication channels.

48.Contact Information

48.1 Clients who have questions, requests, or concerns regarding this Privacy Policy or the Company's processing of Personal Data may contact the Company using the contact details below.

- COMMO T CO., LTD
- Telephone: 023 236 336
- Email: info@commot.com.kh
- Website: www.commot.com.kh

48.2 The Company may request sufficient information to verify the identity of the person making an enquiry or request before providing information relating to Personal Data.

48.3 The Company will make reasonable efforts to respond to privacy-related enquiries or requests within a reasonable period, subject to applicable laws, regulatory requirements, and the nature of the request.

49.Governing Law

49.1 This Privacy Policy shall be governed by and interpreted in accordance with the laws of the Kingdom of Cambodia.

49.2 The Company shall process Personal Data in accordance with applicable laws, regulations, and regulatory requirements governing its business operations.

49.3 Nothing in this Privacy Policy shall limit or exclude any rights or obligations arising under applicable laws, regulations, or regulatory requirements.

50.Effective Date

50.1 This Privacy Policy shall become effective on the date approved by the Company.

50.2 The Company shall review this Privacy Policy periodically to ensure that it remains appropriate, accurate, and consistent with applicable laws, regulations, regulatory requirements, technological developments, and the Company's business operations.

50.3 Where necessary, the Company may update this Privacy Policy to reflect changes in legal requirements, business operations, products, services, or information security practices.

Document Information	Details
Document Name	Privacy Policy
Company	COMMO T Co., LTD.
Version	01
Effective Date	01st January 2026
Document Owner	COMMO T Co., LTD.
Approved by	Board of Director / CEO
Review	Annual or As Required
Classification	Public