Curtain Agreement

(I) Table of Contents

(II) Management framework and principles

A. Preface

The Curtain Agreement was developed to ensure the privacy protection and fair use of personal data in the digital age. As the volume of data processed continues to increase, individuals and organizations face more challenges and responsibilities to ensure data security and transparency. The purpose of this agreement is to provide clear guidelines internally to ensure data processing is compliant and ethical.

In this agreement, we aim to emphasize the importance of personal data privacy and ensure that personal information is not improperly used, disclosed or misused. We hope to provide individuals and organizations with mechanisms to protect and control their personal data by establishing clear rules and processes.

At the same time, we also encourage appropriate data sharing and collaboration to support effective operations and innovation within the organization. We recognize that data sharing can bring many benefits, but it must also be done within a compliance framework to ensure data security and legality.

In order to better manage and share data, and protect the security of data, we have established a classification system with different confidentiality levels. This will help individuals and organizations understand the sensitivity of their data and take appropriate steps to protect and control it.

Finally, we emphasize individual responsibility and autonomy, and individuals have the right to determine the use and access of their own data. We encourage individuals to actively participate in decision-making processes regarding data processing and ensure they have control over and protection of their data.

The name "Curtain Protocol" was chosen to imply the balance between data processing and privacy protection. As an object that blocks sight, the curtain symbolizes data confidentiality and privacy protection. At the same time, the curtain also symbolizes transparency and openness, allowing the data processing process to be known to legal and authorized persons. The name is intended to convey the idea of ensuring compliance and reasonableness of data processing while protecting privacy.

By complying with the Curtain Agreement, we believe that individuals and organizations can better handle and protect data, ensuring the appropriate use of data and the security of privacy. Only by working together can we establish a sustainable framework for data processing and privacy protection in the digital age.

B. Background

In the digital age, the amount of data processed by individuals and organizations continues to increase, and the processing and privacy protection of data have become critical. With the advancement of technology and the popularization of information, the collection, storage and use of personal data have become the norm. At the same time, issues of privacy protection and reasonable use of data have also attracted increasing attention.

The privacy leakage of personal data may lead to damage to personal rights, destruction of trust and potential risks of abuse. In addition, organizations face challenges such as data security, compliance and reputational risks when dealing with large amounts of data. Therefore, establishing a clear set of guidelines and norms to ensure the appropriate use and protection of data has become a priority.

The purpose of the Curtain Agreement is to regulate internal data processing and privacy protection and ensure that individuals and organizations comply with compliance and ethical standards when processing

data. The Agreement was introduced to provide individuals and organizations with a framework that clarifies the guidelines and principles for data processing, as well as measures and requirements to protect personal privacy.

When formulating the Curtain Agreement, different levels of data sensitivity and access rights need to be taken into account, and corresponding controls and restrictions need to be developed. For example, divide the data into different levels and determine the access rights of personnel according to the level to ensure that only authorized personnel can access and process the data of the corresponding level.

In addition, the formulation of the agreement also needs to focus on the reasonable use and sharing of data. Appropriate sharing and cooperation of data can promote effective operations and innovation within the organization, but at the same time, compliance principles must be followed to ensure the security and legality of data.

By formulating the Curtain Agreement, individuals and organizations can better understand the importance of data processing and privacy protection, clarify their responsibilities and obligations, and take corresponding measures to protect the privacy and security of data. Only by rationally using and protecting data while protecting personal privacy can we establish a trustful and sustainable data processing system in the digital age.

C. Set purpose

1. Provide clear guidance internally on data processing (privacy): The purpose of the Curtain Agreement is to provide clear guidance internally to ensure that individuals and organizations adhere to compliance and ethical standards when processing data. The agreement will clearly stipulate the principles, procedures and specifications for data processing and provide guidance to internal members to ensure that their actions in data processing comply with compliance requirements.

2. Protection of the privacy of personal data: One of the purposes of the Agreement is to ensure that the privacy of personal data is not subject to improper use, disclosure or abuse. By formulating clear privacy protection measures and requirements, the agreement will ensure that personal data is properly protected, prevent unauthorized access and abuse, and protect personal privacy rights.

3. Promote appropriate data sharing and collaboration: The agreement encourages appropriate data sharing and collaboration to support effective operations and innovation within the organization. By clarifying the compliance framework and regulations, the agreement will help organizations ensure the security and legality of data during data sharing and cooperation, promote information sharing and collaborative work, thereby improving the organization's efficiency and innovation capabilities.

4. Establish a classification system with different confidentiality levels: In order to better manage and share data and protect the security of the data, the protocol has established a classification system with different confidentiality levels. The system will help individuals and organizations understand the sensitivity of data and determine access rights and controls based on different levels to ensure data is appropriately protected and controlled.

5. Emphasis on personal responsibility and autonomy: The agreement emphasizes individual responsibility and autonomy for their own data. Individuals have the right to determine the use and access of their own data and can actively participate in the decision-making process of data processing. The agreement will encourage individuals to exercise autonomy and ensure that they control and protect their data, while also fulfilling corresponding responsibilities and complying with compliance requirements and privacy protection measures.

D. Origin of name

The name Curtain Protocol refers to the balance between transparency and confidentiality between data processing and privacy protection. As an object that blocks sight, the curtain symbolizes the confidentiality and privacy protection of data. At the same time, the curtain also symbolizes transparency and openness, allowing the data processing process to be known to legal and authorized persons. The name is intended to convey the idea of ensuring compliance and reasonableness of data processing while protecting privacy.

Specifically, the origin of this name can be interpreted as the following aspects:

1. Confidentiality and privacy protection: As a shield, the curtain symbolizes the confidentiality and privacy protection of data. It symbolizes keeping data behind a curtain to prevent unauthorized access and disclosure. The word "curtain" in the name emphasizes the importance and protection of personal privacy.

2. Transparency and openness: Curtains also imply transparency and openness. In the process of data processing, transparency means that legal and authorized people can understand and know the data processing process. This transparency helps build trust and compliance. The word "curtain" in the name implies that data processing should be conducted on a transparent and open basis.

3. Balance and rationality: The word "curtain" in the name conveys the concept of seeking a balance between data processing and privacy protection. Data processing needs to comply with the principles of compliance and reasonableness while protecting personal privacy. The curtain serves as a symbol that represents the balance between protecting privacy while ensuring compliance and rationality in data processing.

To sum up, the origin of the name "Curtain Agreement" implies the balance and transparency of data processing and privacy protection, emphasizing the importance of confidentiality and transparency to ensure compliance and rationality of data processing.

(III)Data classification and sensitivity

E. Data classification

1. Own information

Self-data refers to data or information owned by an individual. This data can include personally identifiable information (such as name, address, phone number), personal preferences (such as preferences, interests and hobbies), personal social media account information, health records, financial information, employment history, etc. Their own data is private and individuals have the right to decide how this data is used and processed.

2. Other people's information

Other people's data refers to data that is not directly related to an individual, but that the individual is responsible for processing. These data are usually generated from relationships between others, such as customer information, employee information, partner information, etc. When individuals process other people's data, they need to comply with relevant privacy regulations and confidentiality obligations to ensure the security and legal use of other people's data.

F. Confidentiality level

1. Level 1
Public Information - This is information that is available to everyone and is open to the public without any restrictions. For example, this information may be public records, announcements, publicly published documents, etc.

2. Level 2
Share information widely - this is information that is available to a wide range of people, including a wide range of stakeholders. For example, this information may involve the organization's business activities, products or service information, and may be shared in public or through appropriate channels.

3. Level 3
Limited Sharing Information - This is information that only a few people can know. For example, this information may include the organization's internal data, business secrets, competitive advantages, etc., and is limited to specific personnel or restricted stakeholders.

4. Level 4
Relevant Person/Stakeholder Information - These are information available to persons or stakeholders relevant to a particular matter. For example, this information may include data related to specific projects, contracts, agreements or key interests.

5. Level 5
Personal Information - These are the most private information that only an individual can know. This information may include personally identifiable information, personal health records, financial information, etc., and is highly private and confidential.

(I) Access and permission control

G. Personnel authority classification

1. Class A personnel
Level A personnel are the highest level of personnel and have broad access to Level 1 to Level 5 data. They can freely access and process personal data, including public data, widely shared data, limited shared data, related person/stakeholder data, and personal private data.

2. Class B personnel
Level B personnel may access Level 1 to Level 4 data. They have elevated access to public data, widely shared data, limited shared data, and data related to specific transactions. However, they do not have access to the highest levels of personal privacy data.

3. C-level personnel
C-level personnel can access Level 1 to Level 3 data. They have lower access to public data, widely shared data, and limited shared data. They do not have access to the highest levels of personal privacy or data related to specific transactions.

4. D-class personnel
Level 1 to Level 2 data can be accessed by D-class personnel. They have more limited access to public data and lower-level data. They cannot access limited sharing data, personal private data, or data related to specific transactions.

5. Class E personnel

Level E personnel can access Level 1 data. They have minimal access rights, limited to public data. They cannot access any other level of data, including widely shared data, limited shared data, personal private data, or data related to specific transactions.

(II) Data processing principles

H. Principles for processing your own data

1. Level 1

Your own information can be shared in public: This is personal information and can be shared freely in public without restrictions. For example, an individual's name, occupation, educational background, etc. can be voluntarily disclosed in public.

2. Level 2

Your own information can be shared widely, including with a wide range of stakeholders: This is personal information and can be shared with a wide range of stakeholders. This information may involve personal contact information, work experience, social media accounts, etc., and can be shared with relevant personnel on appropriate occasions.

3. Level 3

Your own information is only known to a few people: This is personal information and is only known to a few people. This information may include an individual's family situation, specific health issues, personal financial information, etc., and will only be shared with limited persons when necessary.

4. Level 4

Personal information can be known to the persons or shareholders related to the matter: These are personal information related to a specific matter and can be known to the persons or shareholders related to the matter. For example, sharing personal information with relevant persons in the context of a specific project, contract, agreement or key interest.

5. Level 5

Personal information is only known to the individual: these are the most private information of the individual and only the individual can know it. This information may include personal passwords, private communications, personal diaries, etc., and only the individual can have access and knowledge permissions.

I. Principles for processing other people’s data

1. Comply with the appropriate privacy and confidentiality regulations based on the confidentiality level of the data: When processing other people's data, you need to comply with the appropriate privacy and confidentiality regulations based on the sensitivity and confidentiality level of the data. This means that more stringent protection measures need to be taken for highly sensitive data to ensure that the data is not accessed, used or disclosed by unauthorized persons.

2. Ensure the security and privacy of other people’s data and only share it when necessary: When processing other people’s data, you should ensure its security and privacy. Personal data shall be protected by appropriate technical and organizational measures to prevent unauthorized access, damage or loss of the data. At the same time, when sharing other people's data, you should follow the principle of minimization, share only when necessary, and ensure that the sharing party complies with applicable privacy and confidentiality requirements.

3. Respect the ownership and privacy of others' data and follow legal and ethical principles: When processing other people's data, you should respect their ownership and privacy. This means no unauthorized use, access or disclosure of other people's data. At the same time, you also need to follow legal and ethical principles, ensure that relevant laws, regulations and industry norms are followed during data processing, and respect the privacy rights of others.

(III)Sanctions mechanism

J. Sanctions mechanism

The Sanctions Mechanism is a series of internal sanctions established to ensure compliance with the data processing provisions of the Curtain Agreement.

1. Warning letter

For minor violations, first-time offenders may receive a written warning letter reminding them to pay attention to and comply with the terms of the agreement. The purpose of a warning letter is to serve as a warning, making the violator aware that his or her behavior does not comply with regulations and prompting him to make corrections.

2. Commissioned review

For repeated or more serious violations, an internal review may be commissioned to determine the cause and impact of the violation. The purpose of a commissioned review is to gain an in-depth understanding of the reasons behind violations, identify the root causes of the problem, and propose corresponding improvement measures.

3. Information training

For those who lack the knowledge or skills to comply with the Curtain Agreement, corresponding information training can be provided to enhance their understanding of and compliance with data processing and privacy protection. The purpose of the training is to enhance personnel's professional knowledge and skills so that they can better understand and comply with the provisions of the agreement.

4. Internal disciplinary action

For serious violations of the Curtain Agreement, such as intentionally leaking sensitive data or abusing other people's data, corresponding internal disciplinary measures will be taken, such as suspension, demotion, dismissal, etc. The purpose of internal sanctions is to punish violators and send a clear message within the organization: serious breaches of data processing regulations will result in severe sanctions.

5. Legal pursuit

If a breach of the Curtain Agreement involves a violation of the law or the misuse of another person's data, appropriate legal steps will be taken, such as filing a lawsuit or reporting a crime. The purpose of legal investigation is to protect personal privacy rights and maintain the authority of the law, and to hold violators accountable through legal means.

(IV)Data collection and use

K. Data collection principles

1. Legality

Data collection must comply with applicable privacy and data protection regulations. This includes complying with national or regional privacy laws, data protection laws, privacy laws and other applicable laws and regulations. Ensure that relevant laws are not violated during data collection.

2. Purpose limitation

Clearly define the specific purposes of data collection and ensure that data collected is only used to fulfill specified legitimate purposes. Data collection should not exceed reasonable scope and unauthorized secondary use of data is prohibited. Make sure the purpose of data collection is clear, legal and ethical.

3. Data minimization

Data collection should be limited to the minimum extent necessary to achieve the specific purpose. Take steps to ensure that only necessary data relevant to the purpose is collected and retained and avoid unnecessary data collection. Minimizing data collection reduces potential privacy risks and potential for data misuse.

4. Accuracy

Ensure data collected is accurate, complete and timely. Try to ensure the accuracy of the data and update or correct the data when necessary to maintain the accuracy and completeness of the data. Accurate data is the basis for effective decision-making and the protection of individual rights and interests.

5. Storage period

Determine the storage period of the data, and securely destroy or anonymize the data after the storage period is exceeded in accordance with legal and internal policies. Lawful data processing should comply with prescribed data retention periods and ensure secure processing when the data is no longer required.

6. Obtain consent

Ensure that individuals' informed consent is obtained to the extent legal and compliant. Individuals should be clearly informed of the purpose of collection, data types, use and sharing and other related matters before data collection, and have the right to choose whether to consent. Obtaining explicit consent is an important principle for protecting personal privacy rights.

7. Protect sensitive data

For sensitive data (such as medical records, race, religious beliefs, etc.), additional protective measures should be taken to ensure its security and privacy protection. The collection and processing of sensitive data requires higher security standards and additional safeguards to protect personal privacy and sensitive information.

8. Cross-border data transfer

When it comes to cross-border transfer of data, you should ensure compliance with applicable cross-border data transfer regulations, including following applicable privacy protection standards and mechanisms to the extent possible. When transferring data across borders, attention should be paid to complying with international data transfer regulations and appropriate security measures should be taken to protect the privacy and security of data.

(V) Data storage and security

L. Data storage and security

1. Data classification and labeling

Categorize and label collected data in order to identify the data's sensitivity and level of protection needs. For example, classify data into confidential, internal use, and public. By classifying and labeling data, you can better understand the risk level of your data and take appropriate security measures.

2. Data encryption

For sensitive data, appropriate encryption techniques should be used, including encryption during transmission and encryption during data storage, to ensure data confidentiality. Encryption prevents unauthorized visitors from obtaining sensitive information and provides an additional layer of security.

3. Access control

Implement strict access control mechanisms to ensure that only authorized personnel can access and process data. This can include using authentication, authorization mechanisms and access control lists to restrict access to data. Access controls help prevent unauthorized access to sensitive data and provide traceability and accountability for data use.

4. Prevent data leakage

Establish security measures to prevent data leakage, including firewalls, intrusion detection systems, data loss prevention and security audits. These measures can reduce the risk of data breaches and provide the ability to monitor and respond to abnormal activity in real time.

5. Prevent unauthorized data modification

Implement data integrity protection measures such as digital signatures, database logging, and version control to prevent unauthorized data modification. Maintaining data integrity ensures data accuracy and reliability and prevents malicious tampering with data.

6. Secure storage and backup

Choose secure storage media and facilities, and back up your data regularly to prevent data loss or damage. Backup data should be stored in a secure location with appropriate access controls to ensure reliable recovery and reconstruction of the data.

7. Training and education

Provide training and education related to data storage and security to ensure that employees have appropriate security awareness and knowledge and know how to comply with security measures. Training and education can increase employee awareness and compliance with data security and reduce the risk of human error and security breaches.

8. Monitoring and auditing

Establish a monitoring and auditing mechanism to track data access and usage, detect abnormal behavior in a timely manner and conduct corresponding responses and investigations. Monitoring and auditing can help identify potential security threats and provide an audit trail of data access and usage.

9. Partner management

For external partners or third-party vendors, put in place appropriate contractual terms and controls to ensure they comply with data storage and security requirements. Establishing appropriate cooperative relationships with partners and clarifying security responsibilities and obligations can help ensure the security and confidentiality of data during the cooperation process.

(VI)Data sharing and transfer

M. Data sharing and transfer

1. Legality

Data sharing and transfer must comply with applicable legal, regulatory and contractual requirements. This means that organizations must comply with privacy and data protection regulations when sharing and transferring data, and ensure that their actions are within the bounds of the law.

2. Authorize

Organizations must obtain legal authorization before sharing and transferring data. This includes explicitly obtaining the individual's informed consent or sharing and transferring in accordance with laws and regulations. Organizations need to ensure that authorization methods comply with applicable legal requirements.

3. Clear purpose

Data sharing and transfer must clearly specify its purpose. Organizations must clearly define the purposes for data sharing and transfer, ensuring that data is only used to achieve specified legitimate purposes and is not used beyond what is reasonable. The use of data must be consistent with the purpose stated in advance.

4. Recipient privacy protection

Before sharing and transferring data, organizations must ensure that the recipient has appropriate privacy safeguards in place and is able to comply with relevant privacy and data protection regulations. Organizations should evaluate recipients to ensure they have appropriate security measures and privacy capabilities in place to protect the security and privacy of data.

5. Data sharing agreement

Establishing a clear data sharing agreement or contract is critical to ensuring legality. These agreements should clearly define the scope, purpose, authorization, confidentiality requirements and other terms of data sharing and transfer, and clarify the responsibilities and obligations of both parties. These agreements provide clear guidance to ensure the legality and compliance of data sharing and transfers.

6. Cross-border data transfer

When it comes to cross-border data transfers, organizations must ensure compliance with applicable cross-border data transfer regulations. This includes complying with applicable privacy protection standards and mechanisms, or using appropriate legal measures (such as data transfer mechanisms) to ensure the legality and security of cross-border transfers.

7. Oversight and review

Establishing oversight and review mechanisms are important steps to track the performance of data sharing and transfers. Organizations should regularly review partner compliance to ensure compliance with relevant legal, regulatory and contractual requirements, and promptly detect and respond to any violations.

8. Data transfer termination and tracking

Organizations must comply with requirements when data sharing and transfers cease. This includes tracking the data that has been shared and ensuring it is deleted or destroyed as required by contract or law. Organizations need to take appropriate steps to ensure data is not misused or leaked after termination.

(VII)Protection of personal rights

N. Protection of personal rights

1. Transparency and informed consent

In the process of collecting and using personal information, organizations should provide full transparency and clear information, clearly explain to individuals the purposes for which their personal information will be used, and obtain informed consent. This can be achieved by having clear privacy policies and notices and providing necessary information when personal information is collected. Individuals should have a clear understanding of how their information will be used in order to make informed decisions.

2. Minimize and Purpose

Organizations should collect and use only the minimum amount of personal information necessary and only for specific legitimate purposes and not beyond what is expressly stated in advance. This means that organizations should avoid collecting unnecessary personal information and ensure that the information collected is closely relevant to the specific purposes they pursue.

3. Personal information security

To ensure the security of personal information, organizations should implement appropriate technical and organizational measures to prevent unauthorized access, destruction, disclosure or misuse of personal information. This may include the use of encryption technology, access controls, security audits and monitoring, among other measures, to protect the confidentiality, integrity and availability of personal information.

4. Access and correction rights

Individuals should have access to their personal information and the right to request that inaccurate, outdated or unnecessary information be corrected or deleted. Organizations should provide appropriate mechanisms to enable individuals to exercise these rights and respond to their requests within a reasonable time.

5. Right to forget

Subject to applicable law, individuals have the right to request the deletion of personal information relating to them, unless legitimate storage or processing needs exist. Organizations should endeavor to meet an individual's right to be forgotten, subject to regulatory requirements.

6. Revocable consent

Individuals should have the right to withdraw their consent to the use of their personal information at any time and to request that further collection and use of their personal information cease. Organizations should establish mechanisms to allow individuals to easily withdraw consent and cease use of personal information upon receipt of a withdrawal request.

7. Right to data portability

Subject to applicable law, individuals have the right to request that their personal information be transferred to another organization or service provider. This promotes individuals' control over their personal information and supports data portability.

8. Regulatory and Oversight Mechanisms

Organizations should establish an independent regulator or corresponding oversight mechanism to ensure compliance with personal information protection regulations and to investigate complaints and breaches. This helps ensure that an organization processes personal information in accordance with compliance requirements and provides an independent entity to oversee and review its data processing practices.

9. Education and awareness raising
Organizations should provide education and training on personal information protection to increase individuals' awareness and awareness of their rights and privacy protection. This can include training employees on best practices for handling personal information, increasing awareness of privacy risks and promoting a culture of personal information protection.

10. Legal Basis and Compliance
Organizations should ensure compliance with applicable personal information protection regulations and related legal requirements. This includes establishing internal policies, procedures and document management to ensure compliance and taking appropriate steps to address challenges and risks in protecting personal information. Organizations should work closely with legal and compliance departments to ensure that their data protection and privacy practices comply with legal requirements and keep relevant policies and measures updated to adapt to the changing regulatory environment.

(VIII)Data processing supervision and review

O. Data processing supervision and review

1. Regulatory Authority
Identify and work with the appropriate regulatory authorities to ensure that the organization's data processing activities are compliant with local privacy and data protection regulations.

2. Internal control mechanism
Establish internal monitoring mechanisms, such as a privacy and compliance team, to oversee the organization's data processing practices, ensure compliance and promptly detect and respond to breaches.

3. Review compliance
Conduct regular internal reviews to assess the organization's data processing practices for compliance with privacy and data protection legislation and to ensure the effectiveness of relevant policies and procedures.

4. Privacy Impact Assessment (PIA)
Conduct privacy impact assessments on high-risk data processing activities, evaluate possible risks and propose corresponding control and improvement measures.

5. Monitor data access and usage
Establish recording and monitoring systems to track data access and usage and ensure that only authorized personnel are granted access to personal data.

6. Training and education
Provide internal training and education to ensure that members of the organization understand the requirements of privacy and data protection regulations and have correct data handling practices.

7. Complaint handling mechanism
Establish an effective complaints handling mechanism to enable individuals to lodge complaints related to data processing and respond to and resolve complaints in a timely manner.

8. External Audit

Regular external audits are conducted where an independent third party assesses the organization's data processing practices to ensure compliance and provide recommendations for improvement.

9. Document management and record retention
Establish appropriate document management and record retention mechanisms to retain relevant data processing documents and records for future review and demonstration of compliance.

10. Keep improve
Continuously improve the organization's data processing practices and revise and update relevant policies, procedures and controls based on the results of monitoring and review.

(IX)Scope and amendments to the agreement

P. Scope and amendments to the agreement

1. Definition of scope of application
Clearly define the scope of application in the agreement, including the covered entities, scope and geographical scope, etc. This helps determine which entities, projects or activities are covered by the agreement.

2. Clarity of terms
The agreement should have clear terms and definitions to ensure that all parties have a consistent understanding of the agreement. This includes clear definitions of key terms and concepts to avoid ambiguity and differences in interpretation.

3. Revision procedure
The agreement should clearly set out how amendments will be made. This includes the procedure for specifying the amendment, the parties proposing the amendment, the review process, and the conditions under which the amendment will be effective. The revision process should be fair, transparent and enforceable.

4. Consensus principle
Amendments to the agreement should be based on the voluntariness and consensus of all parties. It usually requires the parties to negotiate, negotiate and sign an amended agreement to reach a consensus.

5. Timeliness and effective date
The agreement should clearly specify the effective date of the amendment, as well as the period for which the amendment will be effective. This helps determine the applicable time frame and deadlines for the amendment.

6. Notification mechanism
The agreement should set out the notification procedures for amendments, including how the parties will be notified of the amendments, their effective date and relevant details. This ensures that all parties are informed of revisions in a timely manner.

7. Compatibility
Any amendments shall be compatible with the other terms of the Agreement. Amendments shall not violate the fundamental principles and purposes of the Agreement.

8. Dispute resolution
The agreement should clearly set out the revised dispute resolution mechanism, including procedures and steps for conducting arbitration or litigation.

9. File saving and version control
Versions of the protocol should be saved in order to track revisions and identify the most recent version of the protocol. This helps manage and maintain the history of the protocol and ensures that the latest protocol version is used.

Q. Governing law

The establishment, interpretation and execution of this Agreement shall be governed by the laws of Hong Kong.

1. Established
According to this clause, the establishment of this agreement will be in accordance with the provisions of Hong Kong law. This means that when drafting, signing and entering into force this Agreement, the parties shall abide by the provisions of Hong Kong law regarding the formation of contracts. For example, it complies with the elements of the contract (applicant, recipient, legitimate purpose, legal consideration, etc.) and the requirements for contract formation (offer, acceptance, expression of intention, etc.).

2. Explain
In the event of disputes, ambiguities or ambiguities in the interpretation of the terms of this Agreement, Hong Kong law will prevail. This means that in interpreting disputes, the court or dispute resolution agency will refer to and apply the interpretation principles, legal provisions and relevant case law of Hong Kong law.

3. Implement
According to this clause, the execution of this agreement will comply with the provisions of Hong Kong law. This includes that during the execution of this Agreement, each party shall abide by the provisions of Hong Kong law regarding the performance of contractual obligations, liability for breach of contract and remedies. If a dispute occurs, the court or dispute resolution agency will handle and decide the relevant matters in accordance with Hong Kong law.

R. Copyright Notice

1. All content in this agreement, including but not limited to text, images, videos, audio, scripts and other materials, are protected by copyright laws. These contents are provided by copyright owners or legally authorized persons and are protected by international copyright laws and related laws.

2. All content is for personal use only. Any commercial use of any content contained in this Agreement is strictly prohibited, including but not limited to the reproduction, modification, distribution, transmission, display, performance or creation of derivative works from the content. You may not use the content in any manner or by any means without the express written permission of the copyright owner.

3. When copying the content of this Agreement, you must retain all copyright notices, attributions, rights protection and other relevant information of the original content. Modification of the content, deletion or obscuration of any copyright notice or other legal notice is prohibited.

4. When reprinting the content of this agreement, you must indicate the original author's name, original source and other relevant information in a prominent position, and provide an effective link to the original content.

5. Modification, derivation, distribution, sale or any other form of exploitation of the contents of this agreement is prohibited without the express written permission of the copyright owner. This includes, but is not limited to, using the content for commercial purposes, distributing the content on other websites or media, and creating secondary creations or derivative works from the content.

6. The use of the contents of this agreement must comply with all applicable laws and regulations. You are responsible for ensuring that your use complies with local laws.

7. All trademarks, logos and images featured on this Agreement are the property of their respective owners. The use, reproduction or display of these trademarks, logos and images is prohibited without the express written permission of the respective owners.

8. This Agreement may contain third-party content or provide links to other materials. These third-party contents or links are provided only for the convenience of users and do not constitute an endorsement or evaluation of these contents. We are not responsible for the accuracy, legality, reliability or completeness of such third-party content and disclaim any liability arising therefrom.

9. We are not responsible for any loss, damage or legal liability arising from the use of the content of this Agreement or access to third-party links. Your use of the content on this website is at your own risk.

10. This copyright statement may be changed or updated at any time without prior notice. We recommend that you check the latest version regularly.

If you have any questions about the copyright statement, please contact Carson:
carson.developer1125@gmail.com

S. Supplementary Provisions

1. If matters not covered in this agreement need to be changed or revised, they must be agreed in writing by Party A and Party B or in accordance with legal provisions.

2. If any provision of this Agreement is partially invalid or unenforceable, the validity of the other provisions will not be affected. Any invalid or unenforceable provision shall be construed to the maximum extent permitted by law, and efforts shall be made to effectuate the purposes of the agreement.

3. In order to prove the agreement between the two parties, Party A and Party B signed two copies of this agreement on the above-mentioned date, and each party retains one copy as valid evidence.

4. Any amendment or change to this Agreement shall be in writing and signed by authorized representatives of Party A and Party B to ensure its validity and enforceability.

5. Any notice or communication in this Agreement, unless otherwise specified, shall be in writing and sent by registered mail, courier or email to the address or email address specified in advance by Party A and Party B.

6. The headings in this Agreement are for convenience only and shall not be construed to limit or affect the meaning or scope of any provision of this Agreement.

7. This Agreement constitutes the entire agreement between Party A and Party B on specific matters and supersedes any previous oral or written agreement, contract or commitment.

8. Any assignment, transfer or authorization in this Agreement shall be subject to the written consent of Party A and Party B, unless otherwise provided.

9. This Agreement does not constitute a partnership, agency, employment or employer-employee relationship between Party A and Party B. Both parties A and B are independent entities and shall not under any circumstances be deemed to be the representatives or agents of the other party.

10. This Agreement is governed by and shall be governed by applicable law. Any disputes related to this Agreement shall be submitted to a court of competent jurisdiction for resolution.

11. The interpretation, execution and performance of this Agreement shall comply with the relevant laws and regulations of the country/region where Party A and Party B are located. In the event of any conflict or dispute, the local court shall be the final interpretation and ruling authority.

12. Any waiver of a right or delay in exercising a right in this Agreement will not constitute a waiver of other rights. Any single or partial exercise of a right does not exclude other exercises of that right or the exercise of other rights.

13. Any confidentiality clauses in this Agreement shall continue to be effective after the termination of the Agreement and shall continue to be binding on the confidential information and business interests of Party A and Party B.

14. Any dispute or claim under this Agreement shall be raised within a reasonable time after arising or will be deemed to be waived. This provision does not apply to continuing breaches of this Agreement.

15. Any notice, request or document under this Agreement shall be delivered by appropriate means, including registered mail, courier, email or fax, and shall be deemed to have been validly given upon delivery.

16. The abolition, modification or exemption of any agreement or provision in this Agreement shall be subject to the written consent of Party A and Party B, and shall only be binding on that agreement or provision.

17. Any drawings, attachments or schedules in this Agreement shall be deemed an integral part of the Agreement and shall have the same legal effect.

Party A	Party B
Name:	Name:
Signature:	Signature:
Date:	Date: