Personal Data Protection Policy

CP Axtra Public Company Limited and Its Subsidiaries

1. Importance

CP Axtra Public Company Limited and its subsidiaries (collectively referred to as the "Company") highly respect and prioritize the protection of personal data belonging to personnel, customers, business partners, and associates. The Company is committed to safeguarding personal data from misuse and ensuring its security in accordance with applicable laws and international standards.

2. Objectives

2.1 To ensure that all transactions with the Company are secure, reliable, and that the personal data of personnel, customers, business partners, and associates are protected.

2.2 To prevent damage caused by the fraudulent or improper use of personal data for unethical gain.

3. Scope of Policy

This policy applies to CP Axtra Public Company Limited and its subsidiaries, including any foundations or funds established or that may be established by the Company in the future. The policy will be reviewed at least once a year or when deemed necessary.

4. Principles

The Personal Data Protection Law sets forth the standards, practices, and obligations that the Company must adhere to when managing or processing personal data. These guidelines apply to all personal data, including that of customers, employees, and stakeholders involved with the Company.

To comply with relevant practices and responsibilities, the Company must process personal data according to the following principles:

1. Process personal data in a fair and lawful manner.
2. Process personal data in accordance with the purposes for which it was collected, used, or disclosed.
3. Ensure that personal data processed is adequate, relevant, and not excessive.
4. Ensure personal data is accurate and up-to-date.
5. Do not retain personal data longer than necessary.
6. Process data in accordance with individuals' rights to access and correct their data.
7. Ensure personal data is kept secure.

8. Personal data must not be transferred to countries with inadequate data protection standards, unless consent is obtained or as required by law.
9. Personal data must be used correctly and in a way that does not cause harm to the data subject.

The Company has established standards, practices, and processes to support compliance with this policy. The subsections below summarize the key aspects of data protection that the Company must always consider when processing personal data.

4.1 Transparency

The Company informs all data subjects about the use of their personal data through Privacy Notices, which are displayed on the Company's website (for customers, employees, and other relevant stakeholders), as well as through other communication channels. All details regarding the use of personal data are outlined in these notices. The Company will collect, use, or process personal data solely for the purposes communicated to the data subjects.

In general, the Privacy Notice will include the following topics:

4.1.1 Data subject groups or sources of personal data: Generally, the Company collects personal data from the data subjects themselves, which may include customers, suppliers, employees, job applicants, and other external individuals.

4.1.2 The purposes for collecting personal data from data subjects.

4.1.3 Types of personal data collected, including but not limited to name, address, phone number, email, and IP address.

4.1.4 The retention period for personal data.

4.1.5 The rights of the data subjects.

4.1.6 Methods for giving or withdrawing consent.

4.1.7 The security measures for protecting the personal data collected by the Company.

4.1.8 Contact information for the data protection office, in case data subjects have inquiries regarding the Company's use of personal data or wish to exercise their rights.

4.1.9 External individuals or entities who may access the personal data.

4.1.10 Cookie policy, in cases where the Company collects personal data through its website or applications.

4.2 Use of Personal Data

When the use of personal data poses a high risk to the Company's customers or employees, such activities must go through relevant personal data compliance processes, which may include conducting a Data Protection Impact Assessment (DPIA). This is to document the Company's decision-making process in balancing the Company's interests with the privacy rights of its customers or employees.

4.3 Marketing

Customers have the right to choose whether they wish to receive marketing communications from the Company. Whenever customers provide their personal data for marketing purposes, they will be asked if they wish to receive such communications. Marketing materials will only be sent to customers who have agreed to receive them. Customers can change their preferences regarding marketing communications at any time, and the Company must strictly adhere to their preferences.

4.4 Rights of the Data Subject

When the Company receives a request related to privacy rights from any individual, the Company must respond in accordance with the legal requirements and established procedures.

The rights of the data subject include:

4.4.1 The right to access or request a copy of their personal data.

4.4.2 The right to inquire about how their personal data was obtained, in cases where consent was not given.

4.4.3 The right to request the correction of inaccurate personal data.

4.4.4 The right to request the deletion, destruction, or anonymization of personal data in accordance with the processes and requirements designated by law.

4.4.5 The right to request the transfer of personal data to another data controller.

4.4.6 The right to request the suspension of the use of personal data as prescribed by law.

4.4.7 The right to object to the collection, use, or disclosure of personal data.

4.4.8 The right to withdraw consent given to the Company.

4.4.9 The right to file a complaint if the processing of personal data causes damage to their rights or freedoms.

4.5 Retention and Destruction of Personal Data

The Company does not retain personal data longer than necessary for its intended purposes. Each department must establish an appropriate retention period for the personal data it holds and ensure that it is regularly updated. All personal data should be deleted in an orderly and secure manner according to the defined retention period.

Each department is responsible for determining the retention period for personal data, which must be appropriate and necessary. Clear guidelines must always be in place for the retention of personal data.

To prevent the leakage of personal data, the Company will securely delete or destroy personal data in the following cases:

1. When there is no longer a necessity to retain such personal data.
2. When the collection, use, or disclosure of personal data has fulfilled its purpose.
3. When the data subject expresses an objection to the collection, use, or processing of personal data.
4. When the data subject withdraws their consent for the collection, use, or processing of personal data.
5. Upon the expiration of the agreed retention period, unless required by applicable laws to retain it further.

The Company may consider retaining personal data as necessary for other relevant purposes, as permitted or required by law.

4.6 Data Minimization and Anonymization

The Company will collect personal data only to the extent necessary for its intended purposes and will anonymize data where possible to ensure that it cannot be used to identify individuals.

4.7 Data Security

When processing and transferring personal data, the Company will strictly adhere to personal data protection and security measures to ensure its safety.

4.8 Disclosure and Transfer of Personal Data to Third Parties

When working with third parties on projects that may involve the transfer of personal data, the Company will ensure that appropriate contracts are in place, requiring third parties to comply with personal data protection laws before disclosing personal data to them. Everyone must be aware that unauthorized access to or disclosure of personal data, or activities that do not comply with the law, may result in criminal liability

4.9 Internal Audits

To ensure that the Company complies with laws and policies related to personal data protection, appropriate internal and external audits will be conducted. These audits aim to assess and verify the accuracy, security, and compliance with the Company's personal data protection policies, as well as adherence to applicable laws.

Internal audits, external audits, and audits of relevant third parties will be conducted by designated departments or functions according to the Company's procedures. These audits will evaluate the risks and effectiveness of compliance with the policy. The audit results will be analyzed and used to ensure that the Company's personal data processing complies with applicable laws and policies, and to continuously improve the Company's personal data protection practices, ensuring full compliance with all relevant legal requirements.

5. Roles and Responsibilities

5.1 Board of Directors

5.1.1 Review and approve the personal data protection policy.

5.1.2 Oversee that the Company's business operations comply with applicable laws, Code of Conduct, regulations, policies, practices, and measures, and support effective implementation of the policy.

5.2 Executives

5.2.1 Establish regulations, practices, and measures for the collection, use, and disclosure of personal data that are appropriate to the Company's context and in alignment with policies, applicable laws, and international standards.

5.2.2 Review the policy and approve housekeeping updates, practices, and related measures annually. In cases where significant changes or amendments are proposed, such updates must be presented to the Board of Directors for approval.

5.2.3 Organize an appropriate organizational structure with responsible persons and clear roles to ensure compliance with relevant policies and practices.

5.2.4 Implement a procedure for selecting individuals or entities with adequate personal data protection systems that comply with legal standards, in cases where the Company outsources personal data processing to others.

5.2.5 Oversee the compliance with policies, practices, and regulations and continuously improve operational methods. Ensure that regular reports are provided.

5.2.6 Support the duties of the Company's Data Protection Officer (DPO) by providing sufficient tools, equipment, and facilitating access to personal data to enable effective execution of their duties.

5.2.7 Communicate policies and practices to raise awareness among management and employees at all levels.

5.3 Data Protection Officer (DPO)

5.3.1 Monitor and evaluate the Company's operations to ensure compliance with legal requirements, as well as organize awareness activities and conduct training related to personal data operations.

5.3.2 Provide advice and guidance to the Board of Directors, executives, and employees on complying with the law correctly.

5.3.3 Serve as the point of contact for personal data matters, including protecting the rights of data subjects, coordinating with the Personal Data Protection Commission, and ensuring collaboration.

5.3.4 Maintain confidentiality of personal data encountered or obtained while performing duties.

5.4 Employees

5.4.1 Handle personal data with care, learn, understand, and strictly comply with the laws, Code of Conduct, regulations, policies, practices, and measures of the Company.

5.4.2 Immediately report to the Data Protection Officer upon discovering any personal data breach or leak.

5.4.3 Report any actions that may potentially violate this policy through the Company's whistleblowing and complaint channels.

6 Training

The Company provides communication and dissemination of personal data protection policies and practices through appropriate trainings, meetings, or other suitable activities for its personnel. The effectiveness of the training will be evaluated as deemed appropriate after the sessions.

7 Whistleblowing

Complaints or whistleblowing reports should be made when any actions are suspected of violating policies and related practices, in accordance with the Company's whistleblowing policies and procedures. Whistleblowers or complainants will be protected, and their information will be kept confidential, with no impact on their employment status, both during the investigation and after the process has been completed.

8 Seeking Advice

In cases where there is uncertainty about whether an action may violate laws, regulations, policies, or practices related to personal data protection, advice can be sought from supervisors, responsible departments or personnel, the compliance function, the legal function, or the human resources function before proceeding with any actions.

9 Penalties

If any company personnel directly or indirectly violate or fail to comply with policies, practices, or measures, they will be subject to disciplinary action in accordance with the Company's work regulations.

10 Relevant Laws, Regulations, and Standards

This policy has been established in reference to the Personal Data Protection Act B.E. 2562, which took effect on June 1, 2021. Should this law be amended or its interpretation changed, including any retroactive implications, or should any new regulations, announcements, orders, criteria, or practices be issued under this Act, the Company will consider the impact of such changes to review and update this policy accordingly. Any updates will be aligned with the revised law or its interpretation and will be submitted to the Company's management or Board of Directors for approval before implementation.

Appendix

Definitions

“**Board of Directors**” refers to the directors of the Company.

“**Management**” refers to the executives of the Company.

“**Employee**” refers to employees below the executive level of the Company.

“**Personal Data**” refers to any information related to an individual that enables the identification of that individual, whether directly or indirectly, excluding information related to deceased persons.

“**Data Controller**” refers to a person or legal entity with the authority and responsibility to make decisions regarding the collection, use, or disclosure of personal data.

“**Data Processor**” refers to a person or legal entity that processes personal data on behalf of or under the instructions of the Data Controller. The Data Processor must not be the same entity as the Data Controller.

“**Data Subject**” refers to the owner of the personal data.

“**Sensitive Personal Data**” refers to personal data that is considered sensitive and must not be collected without explicit consent from the data subject. This type of data is particularly vulnerable to misuse and may lead to unfair discrimination. Therefore, extra caution must be exercised in its handling. Sensitive personal data includes race, ethnicity, skin color, political opinions, religion, sexual behavior, criminal records, health information, disabilities, union membership, genetic data, biometric data, and any other information as defined by law.

"Personal Data Source" refers to the origin from which personal data is obtained from the data subject, such as:

- Transactions, form submissions, comments, feedback, or inquiries made through websites, applications, phone calls, emails, direct interactions, or other means.
- Participation in marketing activities, sweepstakes, events, and other activities.
- Services provided via websites, applications, or e-commerce service providers.
- Collection of personal data from public sources, business directories, commercial databases, or social media platforms, whether the data subject voluntarily discloses the information or has consented to its disclosure by others.
- Collection of personal data from third parties, such as family members, emergency contacts, beneficiaries, work guarantors, job application websites, references, recruitment agencies, government entities, educational institutions, securities depositories, banks, or authorized bond selling agents, whether the data subject voluntarily discloses the information or has consented to its disclosure by others.
- Submission of documents for business contracts or employment agreements with the Company.
- Submission of documents related to job applications.
- Recording of still images or video footage via CCTV in areas under the Company's control.

- Visiting the Company's website, whether intentionally or unintentionally.

"Third Parties" refers to individuals or legal entities other than the data subject, the data controller, and the data processor hired to process data on behalf of the Company.

"Data Protection Officer (DPO)" refers to the person appointed to provide advice and ensure that the data controller or data processor complies with personal data protection laws.

"Privacy Notice" refers to a notification informing data subjects about the purposes, methods of collection, processing, and storage of their personal data by the Company.

"Cookie" refers to a unique file created by a website and stored on the user's computer or communication device, which stores personal data, usage information, and user settings to enhance the user's website experience.

List of Amendments to the Personal Data Protection Policy

CP Extra Public Company Limited and Its Subsidiaries

No:	Responsible Person	Description	Reviewed by	Approved by	Effective date
					01/10/2567

Note: The list of policy amendments is intended for internal administration only.