

HUMAN RESOURCES PRIVACY POLICY

Plan B Media Public Company Limited. (the “PLANB”, “Company”, “we”, “us”, or “our”) recognizes the importance of the protection of personal data. We follow security measures when collecting, using, and/ or disclosing your Personal Data (as defined below).

This privacy policy (“**Privacy Policy**”) was made to inform you that in the process of employment, service engagement, or human resources management of the Company, we may collect, use, and/or disclose Personal Data relating to you, who might be a job applicant, job interviewee, current or former staff, employee, outsourced staff, intern, secondee, retired staff, officer, manager, executive, director, authorized director, attorney-in-fact, and/or other person whose Personal Data has been received by the Company and companies under PLANB.

This Privacy Policy applies to our employment process, service engagement process, or human resources management at the Company’s place of business, via websites, electronic system, telephone, email, walk-in job application, post, social networking sites, online communication channels and other means where we collect your Personal Data.

From time to time, we may change and/or update this Privacy Policy. We will provide additional notice of significant changes and/or updates. We will post the date on which our Privacy Policy was last updated at the top of the Privacy Policy. We encourage you to read this Privacy Policy carefully and to check Privacy Policy regularly to review any changes and/or updates we might take in accordance with the terms of this Privacy Policy.

1. WHAT PERSONAL DATA WE COLLECT

For the purposes of this Privacy Policy, “**Personal Data**” means any identified or identifiable information about you as listed below.

We may directly or indirectly collect your Personal Data from other sources. For example, we may directly collect your Personal Data in the process of job application, interview, at the beginning of employment or engagement, or throughout the term of employment or term of service agreement which we entered into with your employer, as part of your employment or service engagement.

In addition, we may indirectly collect your Personal Data, e.g., from the Companies under PLANB, our service providers, third-party business alliances (e.g., outsourcers, contractors, insurance companies, hospitals, banks, national credit bureaus) other third parties (e.g., reference persons, complainants, creditors), public sources, and website of third parties or relevant governmental agencies (e.g., Department of Business Development, Revenue Department, Department of Provincial Administration, Royal Thai Police, Anti-Money Laundering Office, Securities Depository). The specific types of Personal Data collected will depend on the relationship which you have with the Company or the Companies under PLANB. The followings are example of Personal Data that may be collected:

- 1.1. **Personal details**, such as title, name, surname, gender, age, nationality, date of birth, place of birth, weight and height, flaw, blood group, signature, photo, VDO records, vehicle plate number, vehicle brand, educational backgrounds, work experience, training experience, language skills, talent, hobby, behavior, interest, occupation, job title, workplace, certification of employment, salary confirmation letter, professional license, certificate of training, information relating to health insurance, smoking or drinking record, alcohol test result, marital status, and/or military status;
- 1.2. **Contact details**, such as postal address, house registration address, national identification card address, work address, phone number, business phone number, mobile phone number, facsimile number, email address, LINE ID, Facebook account, and/or other information-related to social networking sites;
- 1.3. **Identified information from the government agencies**, such as national identification card, passport, house registration, car registration, driving license, death certificate, company affidavit, certificate of personal name change, military record, conscription certificate, VISA, and/or immigration form;
- 1.4. **Work details**, such as staff identification number, job title, employment beginning/termination date, work experience, performance report, information relating to work outside of the workplace (e.g., place, time, and date of the work outside the workplace, travel plan) work record, disciplinary record, transfer record, promotion record, log book (e.g., clock-in, clock-out) complain details, litigation details, bankruptcy record, application or request for withdrawal of any extraordinary rights, and/or inspection form of the director's qualifications;

- 1.5. **Financial details**, such as details relating to the opening of bank account, copy of bank book, bank account number, credit/debit card number, transaction details, expense details, disbursement document, current return, salary, wage, other income and deduction, withholding tax details, details in the loan application, document/minutes of shareholder's meeting, copy of shareholder register, shareholder/security holder number, security account number, number of shares/securities, and/or amount of dividend;
- 1.6. **Transaction details**, such transaction data, contract details, power of attorney, and other receipts (e.g., advertisement space lease agreement, land deed);
- 1.7. **Profile details**, such as user account, and password,;
- 1.8. **Technical details, such as Internet Protocol (IP) address**, media access control, computer traffic record, website history, operating system and platform, and other technology on devices used to access the platform;
- 1.9. **Other details**, such as other details in job application, resume, terms of reference (TOR), details of bidding, report of interests, and/or details of engineering project;
- 1.10. **Personal details relating to you**, such as details of children (e.g., birth certificate, number of children, type/gender of children, relationship, educational institution, copy of national identification card, birth certificate or letter of exercising parental power certification, document showing education expense, school record, education certificate, welfare), certificate of marriage and/or document of spouse (e.g., income, relationship, copy of national identification card, information relating to health insurance)
- 1.11. **CCTV details**, please see our CCTV Policy for more details on how we collect, use and/or disclose Personal Data by our CCTV
- 1.12. **Sensitive data**, such as Sensitive Data as shown in the identified document (e.g., religion), health information (e.g., medical certificate), criminal background, disability information, biometric data (e.g., fingerprint/facial recognition), Sensitive Data incorporated in the complaint/report and lawsuit (e.g., religion, health information, disability, or criminal record which might be shown in the daily report/ report to the police station or details in the daily report together with copy of daily report).

If you provide Personal Data of any third party (such as parent, spouse, children, emergency contact, or referral person) to us, e.g., their name, family name, address, relationship, contact details,

and related documents, you represent and warrant that you have the authority to do so by (i) informing such other persons about this Privacy Policy; and (ii) obtaining consents (where required by law or necessary) to permit us to use such Personal Data in accordance with this Privacy Policy.

We do not intentionally collect your sensitive data ("Sensitive Data"). However, in case that we do, we will only collect, use, and/or disclose Sensitive Data on the basis of your explicit consent or where permitted by law.

We only collect the Personal Data of children, quasi-incompetent person and incompetent person where their parent or guardian has given their consent. We do not knowingly collect Personal Data from any person under the age of 20 without their parental consent when it is required, or from quasi-incompetent person and incompetent person without their legal guardian's consent. In the event that we learn that we have unintentionally collected Personal Data from anyone under the age of 20 without parental consent when it is required or from quasi-incompetent person and incompetent person without their legal guardians' consent, we will immediately delete such Personal Data or only collect, use and/or disclose if we can rely on other legal basis apart from consent or where permitted by law.

2. WHY WE COLLECT, USE AND/OR DISCLOSE PERSONAL DATA

We collect, use and/or disclose Personal Data for the following purposes:

2.1. THE PURPOSES OF WHICH WE RELY ON CONSENT:

We rely on consent for the collection, use, and/or disclosure of Personal Data and/or Sensitive Data for the following purposes:

2.1.1. Personal Data for the Purposes of Marketing and Communications Which We Cannot

Rely on Other Legal Bases: To provide marketing communications, re-marketing, advertisement, privilege, sales, special offers, notification, newsletter, update report, announcement, promotional activity, news and information relating to our products or services, including products and services of Companies under PLANB and our business alliances, to you;

2.1.2. Sensitive Data as Shown in the Government Issued Document: To identify and verify;

2.1.3. Health Information (e.g., medical certificate): To check record, qualifications, and suitability for employment, to examine and monitor performance during employment, to keep as work record, to arrange work schedule, to grant leave, to support the procurement

and disbursement of welfare, medical fee, annual health check-up, and insurance, to analyze and improve human resources management, to contact in case of emergency, or to dispense medicine at our workplace;

2.1.4. Criminal Record: To check record, qualifications, and suitability for employment in certain positions, and/or to blacklist;

2.1.5. Biometric Data (e.g., fingerprint/facial recognition): To enter/exit working area, and/or to clock-in, clock-out;

2.1.6. Disability Data: To check record, qualifications, and suitability for employment and/or manage the complaint, calculate and make payment to the Empowerment for Person with Disabilities Fund;

2.1.7. Sensitive Data Incorporated in the Complaint/ Report and Lawsuit (e.g., religion, health information, disability): To receive complaint and solve the problem, to record and verify information, request for additional information, provide information, and/or contact; and

2.1.8. Health Information to Comply with the Laws or Orders of the Government Authority Which We Cannot Rely on Other Legal Bases: e.g., to provide to the government agency in relation to disease control.

Where we rely on consent for the collection, use and/or disclosure of Personal Data, you have the right to withdraw your consent by contacting the Company (as detailed in Item 8 of this Privacy Policy). The withdrawal of consent will not affect the collection, use and/or disclosure of Personal Data and Sensitive Data that was previously consented before the withdrawal. However, if you do not give consent or withdraw your consent, we may not be able to employ, or engage your service or the service under the service agreement which we have with your employer.

2.2. THE PURPOSE THAT WE MAY RELY ON OTHER LEGAL BASES FOR COLLECTION, USE, AND/OR DISCLOSURE OF PERSONAL DATA

We may also rely on (1) contractual basis, for our initiation or fulfilment of a contract with you; (2) legal obligation, for the fulfilment of our legal obligations; (3) legitimate interest, for the purpose of our legitimate interests and the legitimate interests of third parties. We will balance the legitimate interest pursued by us and any relevant third party with your interest and fundamental rights and freedoms in relation to the protection of your Personal Data; (4) vital interest, for preventing or suppressing a danger

to a person's life, body or health; (5) public interest, for the performance of a task carried out in the public interest or for the exercising of official authorities; (6) for establishing and raising the right to claim in the future; and/or (7) for legal compliance, e.g., for fulfillment of the objectives in relation to employee's performance evaluation, labor protection, or social security or other legal grounds permitted under applicable data protection law (as the case may be). Depending on the context of the interactions with us, we may collect, use and/ or disclose Personal Data for the following purposes:

- 2.2.1. **To manage job application and/or employment:** such as, compilation of data from job applicant as part of the job application process, verification and background check, assessment of suitability and qualifications of job applicant, employment decision making, entering into employment agreement or service agreement, the preparation of work permit and employment document, and/or determination of salary, welfare, and other basic contractual information in any particular position;
- 2.2.2. **To contact and communicate:** such as, to contact and communicate relating to your interview or activity, document delivery, to contact your emergency contact when necessary, and/or to publish news and invitation to events;
- 2.2.3. **To administrate, pay remuneration, and provide welfare:** such as to pay salary and provide welfare, expense, bonus, compensation, medical and health disbursement, and other rights and privileges to you and other related person, e.g., annual health check-up, medical treatment, leave management/approval, insurance, social security, provident fund management, reward, gym membership, meal support via staff identification card, welfare of cooperative member, scholarship, or baby-sitting welfare after school and during school break, including benefit payment according to insurance policy and life insurance policy;
- 2.2.4. **To manage human resources and employment relationship:** such as to record work record, to monitor performance and working hours, to manage work hours, including to prepare employment documents for foreign employee, arrange activity in relation to work, to evaluate competency, suitability, and performance, to consider adjustment, relocation, of position or workplace, to permanently or temporarily assign employee for a secondment, to consider salary adjustment, to issue staff identification card, card for entering and exiting office and/or other card to specify the area permitted, to analyse, plan, and manage resources and internal affair in order to oversee the overall of the work, support and

facilitate work and use of the Company's assets, including maintenance and repair, to guarantee work, to advise, consider, manage, and solve the complaint, disciplinary action, employment termination, resignation, and retirement, manage and administrate the accounting, blacklisted employee internally and in the Companies under PLANB and/or issue documents or certification letter, e.g., certification letter for employment status or reward letter;

2.2.5. To arrange for training: such as orientation, internal and external training and seminar, including facilitating the event and evaluate the training and attendee's satisfaction;

2.2.6. For the operation of the Company and the Companies under PLANB: such as to administrate the internal operation and assets of the Company, to contact and communicate with the Companies under PLANB and business alliance, to consider and assign, withdraw, or grant authority to you to make any transaction with the Companies under PLANB and business alliance, including stating your name and Personal Data in the relevant contract for such purposes, and for other purposes related to or as specified in the employment agreement or service agreement which the Company has entered into with you or your employer, work rules or regulations in relation to human management, or in any documents relating to human resources management, to use as supporting evidence for any transaction, to assess risks and make decision regarding investment and fund raising, to use as evidence and reference, to prepare and keep important document of the Company, and/or to use the employee database to elect welfare committee of the workplace and safety committee of the workplace according to labour law as the Company reasonably requires;

2.2.7. For the business of the Company and the Companies under PLANB: such as for you to try new product of the Company and/or Companies under PLANB, including offering product of the Company and/or Companies under PLANB, including business alliance, to install advertising media, to explore, plan, manage, sale, increase value of advertising space and/or to provide service to you (e.g., procuring train ticket, returning or refunding the train ticket);

2.2.8. To fulfil financial obligation of the organization, including (internal and external) audit and accounting requirements: such as to project and determine budget, and analyse and

control cost/budget, e.g., to use as a supporting information for opening account, complete financial statement, borrow and procure funds for the Company, to evaluate salary and other income, to proceed tax procedures (e.g., withholding income tax) and disbursement, make payment, issue bill, to verify the accuracy of accounting and document relating to payment, and/or to prepare accounting, balance sheet, and expense summary of the Company or the Companies under PLANB;

2.2.9. To manage IT system: such as to manage IT system, communication system, IT security system, for control access to data system and IT security audit; to manage internal business for internal compliance requirements, policies and procedures; and to update our database;

2.2.10. To comply with laws and orders of competent authority: such as, in case the Company or the Companies under PLANB has reasonable reason to believe that it shall comply with the law, order or provide cooperation, to comply with the law, legal proceedings or government authorities' orders which can include orders from government authorities outside Thailand and/or cooperate with court, regulators, government authority and law enforcement bodies, the Company may need to disclose Personal Data to strictly comply with the said legal obligations, proceedings or government orders. This includes to investigate or prevent crime, fraud, and/or establish the right to claim under the law;

2.2.11. To protect our interests: such as, to protect the security and integrity of our business and the business of the Companies under PLANB or other relevant party; to exercise our rights or protect interest of the Company, Companies under PLANB, or other relevant party where it is necessary and lawfully to do so, for example to detect, prevent and respond to fraud claims, intellectual property infringement claims or violations of law; to manage and prevent loss of our assets and property; to validate the credibility and completeness of internal operation, to monitor and prevent wrongdoings in the workplace of the Company and Companies under PLANB, to secure the compliance of laws, rules, policies, terms and conditions of the Company, Companies under PLANB and other relevant party; to detect and prevent misconduct within our premises; to follow up on incidents; to prevent and report criminal offences and to protect the security and integrity of the business of the Company and Companies under PLANB;

2.2.12. Business transfer or merger: in case of sale, transfer, merger, organizational restructuring, or other event of the same nature, the Company may transfer your Personal Data to one or many other third party(ies) as part of such transaction;

2.2.13. To manage risks: such as, to perform risk management, performance monitoring and risk assessments; and/or

2.2.14. To provide security: such as, to prevent or suppress a danger to a person's life, body, health, or asset, or for disease/epidemic control, and to proceed in case of emergency.

Where the Personal Data we collect from you is needed to meet our legal, regulatory, or contractual obligations or enter into an agreement with you, if you do not provide your Personal Data when requested, we may not be able to achieve the aforementioned purposes.

3. TO WHOM WE MAY DISCLOSE OR CROSS-BOARDER TRANSFER PERSONAL DATA

We may disclose or transfer Personal Data to the third parties mentioned in Items 3.1 – 3.7. These third parties may be located in Thailand or outside Thailand. You can visit their privacy policy to learn more details on how they collect, use and/or disclose your Personal Data since you could also be subject to their privacy policies.

3.1. Companies under PLANB

As the Company is part of Companies under PLANB which all collaborate. For instance, the Company may refer or recommend you to the Companies under PLANB or partially share systems, including service systems and/or database, we may need to transfer your Personal Data to, or otherwise allow access to such Personal Data by Companies under PLANB, for the purposes set out in this Privacy Policy. Other companies under PLANB may rely on the consent obtained by us to use your Personal Data.

3.2. Our service providers

We may use other companies, agents or contractors to perform services on behalf or to assist with the provision of our services. We may share Personal Data to third-party service provider, including but not limited to (1) companies that coordinate and prepare employment documents for foreign employee; (2) service providers who provide employee's benefit calculation services; (3) service providers who

provide payroll and payment system; (4) fund management companies who manage provident fund; (5) infrastructure, software, internet and website developers and IT service providers; (6) data storage and cloud service providers; (7) document storage and eradication service providers; (8) warehouse and logistic service providers; (9) travel service providers/ travel agencies; (10) event organizers; (11) credit rating agencies; (12) printing houses; (13) voting and vote counting service providers; (14) uniform manufacturers; (15) card manufacturers; (16) training institutions; and/or (17) inspection agencies to inspect standard compliance.

In the course of providing such services, the service providers may have access to your Personal Data. However, we will only provide our service providers with the Personal Data that is necessary for them to provide the services, and we will ask them not to use your Personal Data for any other purposes. We will ensure that all the service providers we work with will keep your Personal Data secure.

3.3. Our business partners

We may transfer your Personal Data to our business partners to operate our business and provide the services including, but not limited to, outsourcers, project owners, financial institutes or banks, securities companies, Securities Depository, business partners, insurance companies, hospitals, training agencies/institutions, hotels, provided that the receiving business partner shall agree to treat Personal Data in a manner consistent with this Privacy Policy.

3.4. Third parties permitted by law

In certain circumstances, we may be required to disclose or share your Personal Data to third party in order to comply with a legal or regulatory obligations. This includes, without limitation, Ministry of Interior, Ministry of Commerce, Ministry of Labor, Ministry of Health, Revenue Department, Department of Labor Protection and Welfare, Department of Intellectual Property, Department of Business Development, Excise Department, Customs Department, Consular Department, Department of Rail Transport, Legal Execution Department, Department of Skill Development, Department of Disease Control, district office, Social Security Office, Immigration office, Stock Exchange of Thailand (SET), Securities and Exchange Commission (SEC), Bank of Thailand (BOT), Office of Insurance Commission (OIC), Board of Investment (BOI), Anti-Money Laundering Office (AMLO), Student Loan Fund, police, embassy, consulate, government authority, law enforcement agency, court, regulator, or other third party

where we believe this is necessary to comply with a legal or regulatory obligation, or otherwise to protect our rights, the rights of any third party or individuals' personal safety; or to detect, prevent, or otherwise address fraud, security or safety issues.

3.5. Professional advisors

We may disclose Personal Data to our expert advisors including, but not limited to, (1) independent advisors, project advisors, financial advisors; (2) legal advisors who assist us in our business operations and provide litigation services such as defending or initiating legal actions; and/or (3) auditors who provide accounting services or conduct financial audit for the Company.

3.6. Third parties connected with business transfer

We may disclose or transfer your Personal Data to our business partners, investors, significant shareholders, assignees or transferees in the event of any reorganization, restructuring, merger, acquisition, sale, purchase, joint venture, assignment, or any other similar events involving transfer or other disposition of all or any portion of our business, assets or stock. If any of above events occurs, the receiving party will comply with this Privacy Policy to respect your Personal Data.

3.7. Other third parties

We may be required to disclose Personal Data based on the legal grounds in accordance with the purposes as specified in this Privacy Policy to other third parties such as the Thai Institute of Directors, educational institutions, shareholders, creditors, debtors, customers, complainants or other third parties that we receive a request to access our CCTV records, and/or other person as the case may be.

4. CROSS-BORDER TRANSFERS OF PERSONAL DATA

We may disclose or transfer Personal Data to third parties or servers located overseas, which the destination countries may or may not have the same data protection standards as Thailand's. This includes, without limitation, IT service providers, system developers and maintenance service providers, data storage and cloud service providers, bank/financial institutes, securities companies, shareholders, companies that we invest in, business alliances, agents and distributors, advisor companies, in case of international transfer to customers overseas, business partners or alliances overseas, hotels, training

agencies, embassies, and/or consulates. We take steps and measures to ensure that Personal Data is securely transferred, that the receiving parties have in place suitable data protection standard and that the transfer is permitted under the law.

5. HOW LONG DO WE KEEP PERSONAL DATA

We retain Personal Data for as long as is reasonably necessary to fulfil purpose for which we obtained them and to comply with our legal and regulatory obligations. However, we may have to retain Personal Data for a longer duration, as required by applicable law.

6. DATA SECURITY

As a way to protect personal privacy of your Personal Data, we maintain appropriate security measures, which include administrative, technical and physical safeguards in relation to access control, to protect the confidentiality, integrity, and availability of Personal Data against any accidental or unlawful or unauthorized loss, alteration, correction, use, disclosure or access, in compliance with the applicable laws.

In particular, we have implemented access control measures which are secured and suitable for our collection, use, and/or disclosure of Personal Data. We restrict access to Personal Data as well as storage and processing equipment by imposing access rights or permission, access management to limit access to Personal Data to only authorized persons, and implement user responsibilities to prevent unauthorized access, disclosure, perception, unlawful duplication of Personal Data or theft of device used to store and process Personal Data; This also includes methods that enabling the re-examination of access, alteration, erasure, or transfer of Personal Data which is suitable for the method and means of collecting, using and/or disclosing of Personal Data.

7. RIGHTS AS A DATA SUBJECT

Subject to applicable laws and exceptions thereof, a data subject may have the following rights to:

7.1. Access: Data subjects may have the right to access or request a copy of the Personal Data we are collecting, using and/or disclosing. For privacy and security, we may require proof of the data subject's identity before providing the requested Personal Data;

- 7.2. **Rectification:** Data subjects may have the right to have incomplete, inaccurate, misleading, or not up-to-date Personal Data that we collect, use and/or disclose rectified;
- 7.3. **Data Portability:** Data subjects may have the right to obtain Personal Data we hold about that data subject, in a structured, electronic format, and to transmit such data to another data controller, where this is (a) Personal Data which you have provided to us, and (b) if we are collecting, using and/or disclosing that data on the basis of data subject's consent or to perform a contract with the data subject;
- 7.4. **Objection:** Data subjects may have the right to object to certain collection, use and/or disclosure of Personal Data subject to the applicable law;
- 7.5. **Restriction:** Data subjects may have the right to restrict our use of Personal Data where the data subject believes such Personal Data to be inaccurate, that our collection, use and/or disclosure is unlawful, or that we no longer need such Personal Data for a particular purpose;
- 7.6. **Withdraw Consent:** For the purposes the data subjects have consented to our collection, use and/or disclosure of Personal Data, data subjects may have the right to withdraw consent at any time;
- 7.7. **Deletion:** Data subjects may have the right to request that we delete, destroy or anonymize Personal Data that we collect, use, and/or disclose, except we are not obligated to do so if we need to retain such Personal Data in order to comply with a legal obligation or to establish, exercise or defend legal claims; and
- 7.8. **Lodge a complaint:** Data subjects may have the right to lodge a complaint to the competent authority where the data subject believes our collection, use and/or disclosure of Personal Data is unlawful or non-compliance with applicable data protection law.

8. OUR CONTACT DETAIL

If the data subject wishes to contact us to exercise the rights relating to your Personal Data or if there are any queries about your Personal Data under this Privacy Policy, please contact our Data Protection Officer (DPO) at: Plan B Tower, 1700 Phetchaburi Rd, Bang Kapi, Huai Khwang, Bangkok 10310, Thailand. Email: a.angkana.ch@planbmedia.co.th

- *Pinijsorn Luechaikajohnpan* -
(Pinijsorn Luechaikajohnpan, Ph.D.)
Authorized Director