



Privacy Policy and Notice

Privacy Notice for Employees

ServerToday (Thailand) Co., Ltd.

ServerToday (Thailand) Co., Ltd. ("the Company") places great importance on protecting the personal data of applicants and employees, and is committed to ensuring the security of your personal data in compliance with the Personal Data Protection Act B.E. 2562 and other applicable laws. This Privacy Notice explains the details of how we collect, use, and disclose ("process") your personal data, as well as your legal rights as a data subject.

1. Data Subjects

This Privacy Notice covers the personal data of job applicants and Company personnel, such as consultants, executives, officers, current employees, former employees, interns, and any persons related to Company personnel, such as family members and emergency contacts.

"Applicant" means A person applying for employment as a permanent employee, contract employee, outsourced employee, or freelancer working for the Company, whether the application is made directly by the applicant, through internal recruitment, personal referral, or through a recruitment service provider.

"Employee" means An applicant who has been selected to enter into an agreement to work for the Company as an officer, employee, outsourced employee, or freelancer, as applicable.

2. Personal Data

"Personal Data" means information about an individual that can identify that person, directly or indirectly, excluding data of deceased persons specifically. Examples include name, surname, nickname, address, phone number, national ID number, passport number, social security number, driver's license number, tax ID, bank account number, credit card number, email address, IP address, Cookie ID, Log File, etc.

The following is not considered personal data: business contact information that does not identify an individual (e.g., company name, company address, corporate registration number, work phone numbers, work email such as info@servertoday.com), anonymous data, pseudonymous data, and data of deceased persons.

"Sensitive Personal Data" means personal data relating to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union data, genetic data, biometric data, or other data that affects the data subject in a similar manner as determined by the Personal Data Protection Committee. The Company handles such data with special care and will only collect, use, and/or disclose sensitive data with explicit consent or as permitted by law.

Throughout this Privacy Notice, unless specifically stated otherwise, "personal data" and "sensitive personal data" pertaining to the aforementioned users shall be collectively referred to as "personal data."

Where the Company receives a copy of your national ID card or extracts data electronically for identity verification and legal transactions, the data may include religious information (sensitive data). The Company does not intend to collect such data and requests that you redact or obscure this information. If you do not do so, the Company reserves the right to redact it to protect your sensitive personal data.

3. Sources of Personal Data

The Company collects personal data and/or sensitive data through the following processes:

3.1 Data received directly from you

From recruitment and application processes, job application forms, supporting documents for consideration and selection, surveys, interviews, as well as data and data updates from your employment or various processes during your time as an employee or personnel of the Company.

3.2 Data received from other sources

The Company may collect your data from other sources such as recruitment agencies, job application websites, references or endorsers, background checks, navigation systems, and network systems, as necessary and as permitted by law.

3.3 Third-party personal data

The Company may receive third-party personal data related to you that you provide, such as spouse, children, parents, family members, emergency contacts, beneficiaries, references, or former employers. The Company uses this data to manage welfare and benefits, contact in emergencies, or for reference purposes. Please inform such third parties about this Privacy Notice and obtain their consent if necessary, unless another legal provision permits the disclosure of third-party personal data to the Company without consent.

4. Types of Personal Data Collected

The Company may collect the following types of personal data, such as:

- General Data: Name, surname, national ID number, date of birth, address, phone number, email, photograph
- Education & Work History: Special skills, training history, certificates
- Family & Emergency Contacts: Emergency contact persons
- Bank Account Data: Bank account information for salary and compensation payments
- IT System Data: e.g. Email usage logs, document management system, server access logs
- Sensitive Data (if necessary and with consent): e.g. Criminal records or health information

5. Purposes of Collection, Use, and Disclosure

The Company collects, uses, or discloses your personal data under the following legal bases:

- Contract
- Legal Obligation
- Legitimate Interest
- Vital Interest

- Consent — The Company will request your consent where required by law, or where none of the above legal bases are applicable to the personal data collected from you.

The purposes for collecting, using, and disclosing employees' personal data include, for example:

- Screening, selection, and interviewing of job applicants
- Human resource management including employment contracts, performance evaluations, training, salary payments, other benefits, and maintaining entitlements
- Considering suitable future positions
- Complying with labor law, tax law, social security law, and other applicable laws
- Managing welfare, health insurance, accident insurance, or life insurance
- Preparing reports for submission to relevant government agencies
- Controlling building access, CCTV recording, and security measures
- Managing, developing, and improving business operations efficiency
- Managing complaints, disputes, litigation, and risk management
- Conducting internal organizational activities such as parties, training, CSR activities
- Complying with orders from legally authorized agencies

6. Disclosure of Your Personal Data

To fulfill the purposes stated in this Privacy Notice, your personal data may be disclosed to:

6.1 Within the Company

Your personal data may be disclosed or transferred to relevant internal departments only as necessary for the stated purposes. The following persons or teams will be granted access to your personal data as appropriate:

- HR staff or other relevant departments, with access rights defined according to their roles and responsibilities.
- Executives or direct supervisors responsible for management or decision-making concerning you, or when HR-related procedures are involved.
- Support functions such as IT, accounting, and finance.

6.2 Outside the Company

Your personal data may be disclosed or transferred to the following external organizations:

- Government agencies and regulators as required by law (e.g., Revenue Department, Social Security Office, Department of Labour Protection and Welfare, Legal Execution Department, Student Loan Fund, Department of Skill Development, National Office for Empowerment of Persons with Disabilities, Bank of Thailand, SEC, Ministry of Commerce, Ministry of Labour)
- Agents, contractors, and service providers (e.g., payroll processing, provident fund, banks for housing loan welfare, health insurance, accident insurance, training, organizational assessment, travel and accommodation booking, office buildings, external auditors, consultants). The Company ensures these providers comply with legal requirements and protect your data appropriately.
- External organizations or persons for transaction verification purposes such as credit applications or job applications, confirming only employment status and information you have disclosed to such parties.

Additionally, where the Company has received your written consent to disclose information to external parties, such as a new employer, the Company may disclose your information to verify your previous employment status, or provide your information to educational institutions you previously attended for the purpose of quality development and graduate research projects.

7. Cross-Border Data Transfers

The Company may send or transfer your personal data internationally when necessary, as follows:

7.1 The Company may send or transfer your personal data to other persons both domestically and internationally where necessary to fulfill a contract you are party to, or pursuant to a contract between the Company and another person or juristic person for your benefit, or to carry out your pre-contractual request, or to prevent or suppress harm to the life, body, or health of you or others, to comply with law, or as necessary to carry out a mission of significant public interest.

7.2 The Company may store your data on computers, servers, or clouds operated by third parties, and may use software or platform services provided by third parties to process your

personal data. The Company will not allow unauthorized persons to access personal data and will require such third parties to maintain appropriate personal data security measures.

7.3 Where it is necessary to send or transfer your personal data internationally, the Company will comply with personal data protection law and implement appropriate measures to ensure your data is protected, that you can exercise your rights as required by law, and that recipients maintain appropriate data protection measures, process the data only as necessary, and take steps to prevent unauthorized use or disclosure.

8. Data Retention

8.1 The Company will retain your personal data for as long as necessary, taking into account the necessity and purposes for which it was collected, used, and processed, including compliance with applicable legal requirements, such as:

- Applicants not selected: Data retained for 6 months from the date of notification, so the Company can contact you for potentially suitable future positions.
- Company employees: Data retained for no more than 10 years from the date of termination of employment, for the purpose of verification and dispute resolution within the legally prescribed limitation period.

8.2 The Company will review and delete, destroy, or permanently anonymize personal data upon expiry of the retention period, when data is no longer relevant or necessary for the purposes of collection, or when the Company must comply with your valid deletion request.

9. How We Protect Your Personal Data

The Company implements measures in accordance with Section 37 of the PDPA and ISO/IEC 27701 standards, including appropriate technical, physical, and organizational security measures to prevent unauthorized loss, access, use, alteration, modification, or disclosure of personal data, including:

- Access control with authentication and authorization systems
- Data encryption for stored and transmitted data
- Logging and monitoring of data-related activities

- Data backup and disaster recovery (DR & BCP)
- PDPA and ISO/IEC 27701 training for employees and stakeholders
- Regular review, testing, and assessment of security measures
- Requiring data recipients to maintain confidentiality and process data only as specified by the Company

10. Data Subject Rights

Data subjects have the following rights regarding their personal data:

10.1 Right to Withdraw Consent

You may withdraw consent at any time while the Company retains your data, unless restricted by law or a contract that benefits you.

Note: Withdrawal may affect your access to certain services, benefits, or information. For your own benefit, please consider the impact before proceeding.

10.2 Right to Access

You may request access to and copies of your personal data, including information about its sources.

Exception: The Company may refuse if disclosure would affect others' rights or is prohibited by law or court order.

10.3 Right to Data Portability

You may request your data in a machine-readable format and request transfer to another controller, where technically feasible.

Note: This right applies only to data provided with your consent or necessary for the Company's service delivery.

10.4 Right to Object

You may object to processing based on legitimate interests or public interest.

The Company will cease processing unless it can demonstrate compelling legal grounds or the processing is necessary for legal claims.

You may also object to the use of your data for marketing or scientific, historical, or statistical research purposes.

10.5 Right to Erasure

You may request deletion, destruction, or anonymization of your data if it was processed unlawfully, is no longer necessary, or you have withdrawn consent or exercised your right to object.

Exception: Where the Company has a legal obligation or the data is necessary for legal claims.

10.6 Right to Restrict Processing

You may request temporary suspension of processing, for example while awaiting verification of a correction or objection request, or when the Company should delete data under law but you request restriction instead.

10.7 Right to Rectification

You may request correction of your data to ensure it is accurate, current, complete, and not misleading.

10.8 Right to Complain

If you believe the Company has collected, used, or disclosed your data in violation of law, you may file a complaint with the competent authority.

Additional Note: The exercise of the above rights may be limited by law, such as when the Company has legal obligations or court orders, or when exercising the right would violate others' rights. If a request must be denied, the Company will clearly explain the reasons.

11. Third-Party Website Links

The Company's applications or website may contain links to third-party social networks, platforms, and websites. While the Company strives to link only to sites with adequate personal data protection standards, it cannot be responsible for the content or data protection standards of other sites. Personal data you provide to third-party websites is collected by those parties and governed by their own privacy policies. We recommend reviewing their policies separately.

12. Contact Information

If you have questions or wish to exercise your rights, please contact:

Data Controller

ServerToday (Thailand) Co., Ltd.

111/128 Moo 2, Ratchaphruek Rd., Bangraknoi, Mueang Nonthaburi, Nonthaburi 11000

Email: dpo@servertoday.com

Website: www.servertoday.com

Telephone number: 02-026-3112

Data Protection Officer

DPO Team

111/128 Moo 2, Ratchaphruek Rd., Bangraknoi, Mueang Nonthaburi, Nonthaburi 11000

Email: dpo@servertoday.com

Telephone number: 02-026-3112

13. Governing Law

This Privacy Notice is governed by and interpreted in accordance with Thai law. Thai courts shall have jurisdiction over any dispute that may arise.

14. Changes to This Privacy Notice

The Company regularly reviews this Privacy Notice to ensure consistency with practices and applicable laws. Any significant changes will be communicated through appropriate channels along with the updated version. We recommend checking this notice periodically.

This notice is effective as of May 6, 2025