Employee Privacy Notice

Last update on: March 1, 2024

AutoAlliance (Thailand) Company Limited respects your privacy and is committed to protecting it. This Employee Privacy Notice ("**Notice**") explains our practices regarding the collection, use, and/or disclosure of personally identifiable information ("**Personal Data**") that you have provided and that the Company has received from other sources. This Notice applies to you as you are an employee of the Company, and includes the following individuals:

1. Applicants and interviewees
2. Current employees and ex-employees
3. Secondment employees
4. Employees on probation, temporary employees, trainees and interns
5. Retired employees
6. Current and former consultants, agents and representatives, outside staff, and sub-contractors
7. An appointed person to act on behalf of the Company

(hereinafter referred to as the "**employee**" or "**you**").

The Company has personnel and databases in various locations globally and this Notice also provides you information regarding how your Personal Data may be disclosed or transferred globally, where it is not prohibited by the law.

All uses of Personal Data as described in this Notice shall be in accordance with the Personal Data Protection Act B.E. 2562 (2019) and applicable policy and procedures.

Terms used in this Notice

- "**Personally Identifiable Information**" or "**Personal Data**" means types of personal data that are described hereunder.

- The term **"engagement"** includes employment, providing contract services, or receiving something from the Company, and it includes the period during which the Company has unfulfilled contractual obligations to you (e.g. pension obligations to you, your spouse, or family members where applicable).
- **"Process"** means any collection, store, process, use, modification, transfer, disclosure, or otherwise handling of Personal Data.

Types of Personal Data collected

Types of your Personal Data that the Company Processes may vary by the nature of your engagement, relationship, and the interaction you have with the Company. Such Personal Data may be collected from various channels, including direct collection from you (e.g. email, phone, the Company's websites or form, the Company's office, during your application process, during the interview process, when the employment begins, or throughout the employment period or the duration of the engagement) or that the Company collected from other channels (e.g. external service provider (e.g. recruiting companies) business partners (e.g. contractors, insurance companies, hospitals, banks) other third parties (e.g. friends, your family members, referrals, complainants, creditors, former employers)) other third parties' website (e.g. social media) state agencies (e.g., Student Loan Fund, Legal Execution Department, court) and/or public information, such Personal Data types may include:

- **General and contact information** such as prefix, name-surname, age, photo, date of birth, signature, place of birth, gender, nationality, blood type, weight, height, marital status, military service status, educational level, work history, qualifications, interests / hobbies, address, email address, telephone number, social media user account name, and/or other information you chose to disclose to us that may be considered Personal Data.
- **Personal Identification Information contained in documents issued by government agencies, including copies of such documents** such as national identification card, driving license, passport, visa, alien certificate, work permits, house registration, marriage registration, car or

other vehicle registration, resident registration number, social security number, tax identification number, military service identification card, ordination certificate.

- **Work and education information** such as job application-related information (e.g. information on the job application form, educational record, work history, work experience, internship history, job interview results, and opinions on the applicants), the position of interest, type of engagement, engagement period, job classification, job title, department, line of work, career progression, performance information, employee identification number (including Global ID (GID) and Global Personal Identifier (GPID)), years of service, time records, leave information, start and end date, retirement date, place of work, history of working at another organization, professional licenses, important information to use in your background check.
- **Information related to salary and benefits** such as bank account information, salary rate, compensation, benefits, welfare, and information in relation to benefits to receive (e.g. severance pay, pensions, medical expenses, insurance, provident fund), monetary deduction information (e.g. withholding tax or provident fund)
- **Event or training attendance information** such as registration information, course name, course details, training results, and details of training attendance.
- **Surveillance for safety information** such as stills, moving images, and sounds from CCTV, system access information, building access, time recording, internet access, email access, phone usage data, code for information system, and the right to access the Company's information system, electronic data generated by your use of the system.
- **Performance and disciplinary information** such as performance appraisals, promotion information, indicators, disciplinary behavior record, complaints, disciplinary action and warning, details of grievance consideration, and the performance rating history.
- **Other information** such as information necessary for traveling abroad, any other information contained in the documents relating to the Company's business management, or information you asked us to disclose.

- **Information of family members or related persons** such as name and contact information of emergency contact person, father, mother, children, spouse, references, relatives, acquaintances of you who work for the Company, Company's employee that recommends you to apply for a job, your dependants and beneficiaries (e.g. name, date of birth, gender, marital status, health information and certain government-issued identification numbers in the event that a family member receives the welfare that we provide).

- **Sensitive Personal Data** includes:

    - Sensitive Personal Data that is contained in documents issued by government agencies that the Company may separately request your consent, from time to time, where the Company cannot rely on other legal bases.

    - Health and treatment information such as medical information needed to assess claims, care management per employee welfare plans, medical information necessary to provide accommodation, to assist in rehabilitation to return to work, and continuous employment, annual health check, coronavirus disease (COVID-19) screening results, congenital diseases, or genetic diseases.

    - Criminal record.

    - Disability information such as a disabled person identification card.

    - Trade union information such as trade union membership.

Where the Company receives Personal Data of a third person (family members' personal data e.g. name, date of birth, gender, health information and certain government-issued identification numbers) that you have provided to the Company, in the event that a family member receives the welfare that the Company provides, you should ensure that you have the rights and/or authority to provide such Personal Data to the Company and allow the Company to Process such Personal Data in accordance with this Notice. You are responsible for notifying the details of this Notice to such third parties, as well as obtaining consent from such persons (if consent is required) or having other legal bases so that the Company can Process the Personal Data of such third parties lawfully and in accordance with this Notice.

In some cases, as required by the law, the Company cannot Process the Personal Data of a minor, incompetent person, or quasi-incompetent person without the consent of the person with parental authority, guardian, or curator. Therefore, if you are under the age of 20 and have not yet become sui juris, an incompetent person, or a quasi-incompetent person, you must ensure that you have obtained consent from parents, guardian, or curator (in the case where consent is required). In the case where the Company unintentionally collects Personal Data of a person under the age of 20 and has not yet become sui juris, an incompetent person, or quasi-incompetent person, without consent from the parent, guardian, or curator (as the case may be), the Company will delete that Personal Data immediately, or will Process that Personal Data only if the Company can rely on legal bases other than consent, or as permitted by law only.

Purposes

The Company may Process your Personal Data for business-related purposes where consent is required or where the Company can rely on the following legal bases:

Purposes that require consent

The Company may Process your Sensitive Personal Data for the purposes which require consent, this includes:

- Sensitive Personal Data that is contained in documents issued by government agencies, such as religious information from your national identification card. The Company may Process your national identification card for identity authentication and verification or use it as a supporting document for entering into an agreement.
- Health and treatment information to assess the suitability before entering into an agreement; to assess work suitability; to assess suitability for changing the position or the position suitability; to provide welfare rights.
- Criminal record to consider accepting to work, assess eligibility, prohibited the characteristics or suitability to hold any position, and assess suitability before entering into an agreement; to manage Company's human resource and conduct Company's business operations, to prepare and maintain material documents for archiving, to prepare and maintain employee

records, to conduct discipline management; handle complaints, carry out benefit payments, or otherwise service, including for legal compliance, compliance with a competent authority's order.

- Disability information to assess the suitability before entering into an agreement, to calculate and send disability fund payments.
- Trade union information to facilitate the management of trade unions.

The Company will Process sensitive Personal Data only when the Company has obtained your express consent, or when the Company is permitted by the law to do so on a legal basis other than consent. In addition, the Company may request additional consent from you on a case-by-case basis for the Processing of any sensitive Personal Data for which the Company cannot rely on legal bases other than requesting consent.

Purposes that the Company can rely on legal bases other than requesting consent

The Company may Process your Personal Data by relying on the following legal bases (1) Contractual basis for initiating an agreement or entering into an agreement or performance of an agreement with you (especially an employment contract entered with you or service provision contract entered into by the Company and your employer); (2) Legal obligation basis, for fulfilment of our legal obligations; (3) Legitimate interest, for the purpose of our legitimate interests and the legitimate interests of third parties; (4) Vital interest, for the prevention or suppression of danger to a person's life, body, or health; (5) Public interest, for the performance of tasks carried out in the public interest or for exercising official authorities' duties; (6) Establishment, exercise, or defense of legal claims; (7) Necessary for compliance with a law such as assessment of working capacity of the employee, employment protection, social security, to achieve substantial public interest, public interest in public health and/or other applicable legal basis under the relevant laws that the Company may rely upon.

Some of the following Personal Data Processing purposes may or may not apply to you. Please consider the following purposes based on your relationship and the type of agreement you have with the Company.

<u>If you are an applicant:</u>

- **Management of job application, verification, and hiring processes** such as employee recruiting; identity verification; recording of information collected from applicants; suitability assessment; qualification check; background check; making hiring decisions; entering into an employment contract or service agreement and proceeding with your employer; proceeding with orientation procedures to applicants; determining salary, benefits, welfare, and other bases of contractual information for new employees in any position.
- **Contacting purposes** such as contact for scheduling the interview; sending of documents; communicating with your designated contacts in case of emergency; and publication of news.
- **Complying with the legal obligation** such as legal action, legal proceedings, or order from a government agency, and/or to cooperating with courts, regulators, government agencies, and law enforcement agencies in the event that the Company has reason to believe that it is obligated to comply with the law and/or order, or has to cooperate as such. We may need to disclose your Personal Data to strictly comply with said legal obligations, legal proceedings, or government authorities' orders, including to comply with internal investigations procedures, complaints or claims, interrogation, crimes or fraud prevention, and/or establish legal claims.
- **Protecting the Company's interests** such as the security and integrity of the Company's business; to exercise the Company's rights, and protect the Company's interest when it is necessary and lawful, for example, to detect, prevent, and take action on any fraud or violation of the law, use of CCTV to monitor the situation to prevent and report crime and for security;
- **Dispute management** such as resolving disputes; enforcement of the Company's agreements; gathering of evidence; establishing, complying, exercising, defending, and/or any other legal proceeding per the Company's statutory rights;
- **For the prevention or suppression of danger to a person's life, body, or health.**

<u>For other types of employee</u>

Apart from the above purposes, the Company may Process your Personal Data for the following:

- **Salary payment, compensation, benefits** such as salary, compensation, and bonus payment; actions to exercise the entitled benefits (e.g. severance pay, pensions, medical expenses, insurance, provident fund); assessments for salary adjustments or compensation;
- **Human resources management** such as employee identity verification; working data recording; managing work related activities; proceeding with orientation procedures for the employee; issuance of employees' identification card, office entrance card and/or other cards; promoting corporate social and environmental responsibility; managing disciplinary matters and termination; tracking working hours; tracking clock-in and clock-out time; monitoring work performance within the Company's premises; monitoring internet, email and telephone usage; issuing a letter certifying work status; arranging employee meetings; general management; providing performance evaluations and promotions; assessing suitability for job position; managing employee retirement plan; managing work permit for foreign employees; blacklist management; promoting and ensuring equality between employees within the organization; carrying out analysis; preparing and maintaining corporate organizational charts; employee and working team management; managing and monitoring business travel; employee analysis; conducting talent management and career development; leave management and approvals; managing health care; issuing reference letter as requested; administering ethics and compliance training; organizing recreational activities; making investment decisions; forecasting and budgeting; evaluating performance and promotion; career support; making a decision to adjust, change, transfer position, relocate employee, including international assignments; adjustment of the type of your employment contract (e.g. from intern to a regular employee) or service agreement as entered with your employer; changes to the employee's legal name (e.g. in case of marriage); proceeding with employment, termination, resignation, and retirement; performing administrative monitoring; performance monitoring; payment; planning and performance assessment; managing complaints; managing cost and reimbursement;
- **Operating Company's business** such as communicating within Group Company or Joint Venture Company, service provider, and business partners; planning, implementing, and

managing relationships and contractual rights; to consider appointing, terminating, and authorizing you to conduct transactions; issuance of Company's credit card under individual's name; satisfactory survey; enforcement of any agreement, contract, policy, or document relating to human resource management work; using your information as documentary evidence of transactions; auditing and accounting (both internal and external); cost analysis and budget controls; controlling and screening of the spread of communicable diseases; data analysis and internal reporting for the benefit of the Company;

- **Information technology management** such as effectively storing your personal data on your information technology server; enhancing information technology securities; monitoring internet or the Company's website usage;
- **Business Organization** such as merger, sale, purchase, joint venture, assignment, transfer or other disposition of our business, assets, or stock, or rehabilitation, capital venture, or any similar transaction, the Company may disclose your Personal Data to our assignee(s) of rights as part of such transactions;

Failure to provide certain Personal Data may result in the Company not being able to comply with your request, and as a consequence, you may not be able to obtain certain welfare or benefits, which may affect the consideration of accepting your employment in a certain position or certain compensation, or affects our ability to comply with our obligation under your employment contract. Also, this may affect responsibility for legal obligations that you or the Company are required to comply with.

Disclosure of Personal Data

Your Personal Data may be disclosed within Group Company and to other entities (e.g. suppliers of goods or services to the Company) with whom the Company has used the services for handling Personal Data for the "Purposes" outlined herein as necessary. Your Personal Data may be disclosed to others for legitimate business purposes. The recipient of your Personal Data includes the following:

- **Group Company or Joint Venture Company**: The Company may disclose your Personal Data, or your Personal Data may be accessible by entities within the Group Company and Joint Venture Company for the purposes aforementioned.

- **The Company's service provider**: The Company may be required to disclose your Personal Data in order to use the service or to have the service provider provide services on the Company's behalf. The Company will only provide Personal Data as necessary for the provision of service and will ask those service providers not to use your Personal Data for any other purposes other than those agreed with the Company. The said service provider shall include, but not be limited to: (1) welfare service providers such as welfare service provision and program assistance; (2) recruiter and human resources operation service providers; (3) information technology service providers; (4) logistics and freight service providers; (5) information analysis service providers; (6) data storage and cloud service providers; (7) document storage and document destruction service providers; (8) printing service and document delivery service providers; (9) work permit and visa related service providers; (10) banks and financial institutions; (11) survey providers;

- **Business Partners**: The Company may disclose and/or transfer your Personal Data to the Company's business partners.

- **Persons required by law**: The Company may disclose your Personal Data in order to perform its duties in accordance with the applicable laws, and cooperate with government agencies, and/or other law enforcement agencies when the Company has reason to believe that it has to comply with the law, order, or to cooperate as such.

- **Consultant**: The Company may disclose your Personal Data to consultants, which includes but is not limited to a legal consultant and/or auditor.

- **An Assignee of rights and/or duties**: The Company may undergo business reorganization, to which the Company may be required to disclose your Personal Data to the assignee(s) of rights and/or duties.

- **Other Personal Data recipient:** The Company may disclose your Personal Data to other persons or juristic persons for the purposes contemplated in this Notice. Such Personal Data recipients may include, but are not limited to, persons or juristic persons you requested us to disclose your Personal Data to, the exercise of rights to inspect records from CCTV, the general public, and/or other public disclosures.

Cross-border transfer of Personal Data

The Company may transfer your Personal Data to persons or juristic persons in countries outside of Thailand, for example, to store Personal Data in the database of the global Group Company, and to the Company-approved suppliers globally. In the event it is necessary to transfer your Personal Data to destination countries that may have a higher or lower standard of Personal Data protection, we will take steps and measures to ensure that your Personal Data is securely transferred and that the receiving parties have in place an appropriate level of data protection standards or other measures as applicable with the laws. If necessary, we may request your consent where consent to cross-border transfer is required by law.

Personal Data Security Measures

The Company uses systems, policies, and measures to protect your Personal Data from access to, use, alteration, correction, modification, or disclosure of Personal Data unlawfully or without authorization. Such measures include limiting access to appropriate personnel who have a legitimate business need to access Personal Data. Our retention policies and procedures require that Personal Data be deleted from our systems or destroyed when the retention period expires.

The Company's suppliers are required to keep Personal Data confidential and secure, utilizing appropriate administrative, technical, and physical safeguards. They are not permitted to use Personal Data for any other purpose than to carry out the services that they are performing for the Company.

Personal Data Retention Period

The Company will retain your Personal Data for as long as it is necessary for the purposes stated in this Notice. The Company may extend the Personal Data retention period if it is necessary to comply with the laws, regulations, and the Company's internal policies, or when there is a dispute.

Data Subject Rights

Subject to the conditions prescribed by applicable laws and our data subject rights management procedures, you may have the following rights:

1. **Right to Access:** You have the right to access or request a copy of your Personal Data that the Company collects, uses, and/or discloses. However, the Company will not provide non-disclosure information such as information that is protected by exclusive rights, or trade secret information.
2. **Right to Rectification:** You have the right to request that your Personal data be corrected, updated, completed, and not misleading. If you become aware that any Personal Data the Company holds about you is incorrect or if you wish to update your Personal Data, you can contact your HR representative to request the correction or updates to your Personal Data.
3. **Right to Data Portability:** You may have the right to obtain your Personal Data in an electronic format, and to transmit such data to another data controller.
4. **Right to Object:** You may have the right to object to certain collection, use, and/or disclosure of your Personal Data at any time, to the extent that is permitted under the applicable law.
5. **Right to Restrict:** You may have the right to restrict the Company's use of your Personal Data in some cases.
6. **Right to Withdraw Consent:** For the purposes, you have provided your consent to the Company to collect, use, and/or disclose Personal Data, in certain cases you may have the right to withdraw your consent at any time.
7. **Right to Personal Data Deletion or Destruction:** You may have the right to request us to delete, destroy, or make Personal Data that we collected, used, and/or disclosed about you anonymized.

8. **Right to Complaints**: Where you believe that the Company's operation is not in accordance with the Personal Data Protection Act B.E. 2562 (2019), you have the right to lodge a complaint to the competent authority.

The exercise of rights set forth above may be restricted by the applicable law and exemptions. In some cases, the Company may lawfully refuse your request, such as where the Company is legally obligated or has a court order. However, if the Company refuses to comply with your request, the Company will inform you of the reason.

The Company may require the data subject to provide proof of identity prior to the Company complying with your request, and in some cases, the Company may charge a fee for complying with your request as permitted by law.

Global Personal Identifier data Collection and Use Statement

The Company respects your privacy and is committed to protecting it. We provide this statement to inform you of the Global Personal Identifier (GPID) so that you are aware of its purpose and how your personal information will be used. The purpose of the GPID is to uniquely identify you and to distinguish you from other individuals within Ford/Company in a globally consistent and sustainable manner without relying on government-issued identifiers and other similar personal data. To do this, we require you to supply your name, date of birth, month of birth, and day of the week of birth. Authorized Ford/Company system administrators will be able to use the GPID database to identify individuals to help manage and control access to Company systems, facilities, and services. The data you submit is visible only to those authorized administrative staff for the management of identity. Your date of birth, month of birth, and day of the week of birth will not be passed to any other internal or external system.

GPIDs are used openly to identify people in Ford globally and they are for identification purposes only. Knowledge of a GPID does not provide any authorization, authority, or access. For authorization, authority, or access to Ford/Company systems, facilities and services, other items or information are required, such as a password or entry card. A GPID identifier and associated name may be transmitted by the Company to a service provider when necessary for proper identification

and only if the service provider could not meet its obligations to the Company or you without the information (e.g. travel administration, vouchers, and other similar processes that today identify you as a person).

The GPID application will assign you a unique life-long identifier that will be retained for the duration of all your engagements with the Company and will be retained beyond the end of your last engagement as needed for the Company to identify you. An engagement includes employment, providing contract services, or receiving something from the company, and includes the period during which the company has unfulfilled obligations to you (e.g. pension obligations to you or your spouse where applicable). This process is to enable even employees, contractors, and others who return to Company after a period away to receive the same GPID. After the retention period, your GPID and your personal data which has been used to generate the GPID will be securely destroyed.

Since the Company operates globally, the information you submit may be transferred outside the country of origin to other Company locations or Company operations and initially will be retained by the Company in the United States in a GPID database. This and all other transmissions will remain secure and under our sole control.

Should you have any questions regarding the accuracy of your data, other questions about GPID, or require further information, please send your request by e-mail to gpidhelp@Company.com.

Contact the Company

If you wish to exercise your right as a data subject or have any questions regarding your Personal Data under this Notice, please contact the Company at:

- *49 Moo 4, Tambol Pluakdaeng, Amphur Pluakdaeng, Rayong*
- *Tel. 038-954111 or 038-954222*
- *psrisong@aat.ford.com*