Data protection notice for the applicant management process at Bosch Group

We want you on our team!
In this privacy notice, we inform you how your personal data is processed in the applicant management process at Bosch Group (in the following also “Bosch” or “we”/”us”). Additionally, we inform you about your rights under applicable data privacy laws.

Bosch respects your privacy
Protecting your personal data and ensuring the security of all our business data are important concerns for us. We always consider these concerns in our business processes. The personal data collected when you apply online is treated confidentially and strictly in accordance with the statutory provisions.

Data privacy and information security are an integral part of our corporate policy.

Data controller
The Bosch Group legal entity to which you submit your application using the application management system is responsible for processing your data. You will find the contact details of the controller in the job advertisement in the application management system.

Data categories processed
The following are the main categories of personal data processed:

- Master data (e.g. name, date of birth, nationality, place of residence)
- Documents (e.g. references, certificates, résumés)
- Education and training details (e.g. data about school education, university, professional qualification)
- Payment data (e.g. bank account details for travel expenses)
- Organizational data in case of internal applications (e.g. personnel number, cost center, department)
- Communication data (e.g. e-mail address, (mobile) phone number, IT user ID in case of internal applications)
- Audio visual recording in the selection process e.g. for the Junior Managers Program (JMP)
- Log data recorded while using IT systemsg80[-

The information may include personal data classified as sensitive personal data under the Thai Personal Data Protection Act (PDPA) of 2019, such as health information, religion, or sexual orientation.

Purposes of processing and legal bases
We store and assess your personal data in accordance with the Thai Personal Data Protection Act (PDPA) of 2019, national data protection laws, and other applicable laws.

The Thai Personal Data Protection Act, or PDPA of 2019, contains certain provisions regarding the limitation of individuals' rights and freedoms, with Article 26 in conjunction with Articles 32, 33, and 37 of the Constitution of the Kingdom of Thailand. This law permits the enforcement of the Act in accordance with the criteria under Article 26 of the Constitution.

The assessment of personal data occurs during the applicant management process, specifically for the purpose of preparing for an employment relationship with the legal entities of the Bosch Group.

The primary legal basis for this purpose is the PDPA of 2019 in conjunction with the applicable national data protection laws ("to carry out procedures at the request of interested parties prior to the employment contract").

The PDPA of 2019 aligns with global data protection standards, such as the European Union's General Data Protection Regulation (GDPR), reflecting Thailand's commitment to protecting personal data and privacy.

Children
Section 20 of the PDPA of 2019 states that if the data subject is a minor who lacks legal capacity under Section 27 of the Civil and Commercial Code, consent from the data subject must be obtained as follows:

1. In cases where the consent of the minor is not an action that the minor is entitled to undertake independently, as specified in Sections 22, 23, or 24 of the Civil and Commercial Code, such action must be consented to by the person responsible for the minor's care.

2. If the minor is under ten years old, consent must be obtained from the person responsible for the minor's care.

Collecting of personal data
As a rule, your personal data is collected directly from you during the hiring process.

The easiest way to apply for a job at Bosch is a direct application for a position advertised on one of our job portals, where you enter your data in the candidate profile created individually for the advertised position. You hereby have the possibility to send us the data be connecting to a social network, by a manual input and/or by using “CV Parsing” (Transferring some data from your CV to our job portal).

We recommend to only upload documents in pdf format. Due to technical reasons other data formats lead to temporary local data copies in order to be displayed.
The data from paper applications is transferred manually to the application system. You receive an email in order for you to activate your manually created application. In this email, we inform you, whether we will send your paper application back or shred it. If you do not activate your application within 30 days, your data is deleted from our application management system and you will not be considered any further in the selection process.

Additionally, you have the possibility to be referred by a Bosch Group employee. For this purpose, you need to give your application documents to this employee, who then uploads it in the application management system. You receive an email with which you can activate your application. If you do not activate your application within 30 days, your data is deleted from our application management system and you will no longer be considered in the selection process. Your application is linked with the employee who uploaded it in the application system. This helps us in identifying that this employee has referred you. Furthermore, this employee can track the status of your application (invitation, rejection etc.) on an overview page but has no access to the details of the application process.

We keep you up to date on the status of your application via e-mail.

Prior to sending your application, you have the possibility to you give your consent for allowing your profile to be shared with further hiring managers or recruiters that offer open positions.

During the application process, we will ask you whether we are allowed to forward your application data to other suitable open positions. If applicable, we may also offer you membership in a Bosch applicant community.

Staffing of particularly sensitive job positions may require a further check of your application data and your career path. The result of this check is documented in the application management system. We inform you about such checks in a transparent manner in the framework of our job advertisements. This check takes place taking local legal requirements into consideration and by involving carefully selected service providers.

Membership in a Bosch Candidate Pool
Bosch Group Thailand offers certain target groups the opportunity to register in a Bosch Candidate Pool. Bosch Candidate Pools have the purpose of checking profiles and CVs for placement to a specific open position or to a Bosch Talent Community within our Active Sourcing Tool. Recruiters contact the respective candidates by e-mail (e.g. to send out suitable job proposals) or by phone (e.g. to check for professional preferences). Before you become a member of a Bosch Candidate Pool, you consent to the processing of your personal data over a consent form. Your membership is limited to maximum duration of 2 years. After that, your data will be deleted.
You can revoke your consent at any time for the future by contacting the HR IT Support Germany: SupportDeutschland.HRIT@de.bosch.com.

Participation in Bosch recruiting events
Some Bosch locations organize Recruiting-Events in order to win potential candidates for multiple, similar job advertisement. Special event pages on different internet platforms inform about the contents of these events. You may apply for participation in these events by uploading your application in our application system via the link created for this purpose.

Recipients of your personal data

- **Within a legal entity of the Bosch Group**

Only the people involved in the application process (e.g. line managers and associates of the recruiting department, HR associates and associate representatives) have access to your personal data for the purposes mentioned above within the legal entity of the Bosch Group to which you have applied.

- **Other legal entities within the Bosch Group**

Other legal entities are data controllers themselves. The above mentioned persons involved in the recruiting process may belong to different companies of the Bosch Group. Therefore, your data may be transferred to the respective persons worldwide within the Bosch Group.

In case of your appointment, your data is transferred from our application management system to our HR-administration systems. In this process, your data may be transferred to a different legal entity and will thereafter be processed as employee data. An exchange of your personal data with other legal entities within the Bosch Group takes place especially in order to fulfill the contracts as well as due to our legitimate interest to organize the internal workflows (e.g. Shared Services, execution of transfers or relocations across legal entities).

- **Recipients outside the Bosch Group**

We may disclose your personal data to other data controller only if necessary, for the application, if the third party or we have a legitimate interest in this disclosure, or if you have provided your consent. You will find the details of the legal bases in the section “Purposes of processing and legal bases”.

- **Data processors**

In addition, we use service providers to fulfill our contractual and legal obligations among other things. Insofar as these service providers processes personal data on our behalf, we have concluded the contracts required under the data protection law with them.

We select our service providers carefully and monitor them on a regular basis, especially regarding their diligent handling and protection of the data that they store and process. All service providers are obliged to maintain confidentiality and to comply with the statutory provisions. Service providers may also be other companies of the Bosch Group.

You will find a list of our contractors and service providers (with whom we have a long-term or ongoing business relationship) in *Annex 1*.

Transfer to recipients outside Thailand
According to the Thai Personal Data Protection Act (PDPA) of 2019, cross-border data transfers must comply with specific requirements to ensure that personal data remains protected even when transferred to other countries. Below is a detailed overview of the requirements and guidelines for cross-border data transfers under the PDPA of 2019:

1. General Requirements for Adequate Protection
- Adequacy Standard: Personal data can only be transferred to countries or international organizations that provide an adequate level of protection equivalent to that required under the PDPA of 2019. The adequacy of protection will be assessed based on various factors, including the legal and regulatory framework of the receiving country or organization.

2. Specific Mechanisms for Transfer
- If the receiving country does not provide adequate protection comparable to the PDPA of 2019, cross-border data transfers may be permitted under specific conditions:
  - Standard Contractual Clauses (SCCs): Organizations can use contractual agreements, such as SCCs, to ensure compliance with data protection requirements. These clauses are designed to provide contractual guarantees regarding the protection of personal data.
  - Binding Corporate Rules (BCRs): Multinational organizations may use BCRs to ensure data protection across their global operations. These rules must be approved by the Personal Data Protection Committee (PDPC) and outline how data protection standards will be maintained.
  - Other Safeguards: Organizations may use other safeguards or legal mechanisms that provide sufficient protection for personal data, which may include specific contractual provisions or compliance with industry standards.

3. Data Transfer Agreements
- Contractual Agreement: When transferring data internationally, organizations must have a contract in place with the data recipient that specifies data protection obligations. This contract should detail how personal data will be managed, protected, and retained in accordance with the PDPA of 2019.

4. Notification of Data Transfer
- Notification to PDPC: In certain cases, organizations may need to notify the Personal Data Protection Committee about cross-border data transfers, especially if significant risks are involved or if the transfer is made to a country or entity that does not provide adequate protection.

5. Rights of Data Subjects
- Protection of Rights: Organizations must ensure that the rights of data subjects are protected even when their data is transferred internationally. This includes maintaining access to their data and the ability to exercise rights under the PDPA, such as correction, deletion, and objection.

6. Data Security Measures
- Secure Transfers: Organizations must implement appropriate security measures to protect personal data during cross-border transfers, including encryption, access controls, and secure transfer protocols.

7. Compliance and Auditing
- Regular Audits: Organizations should conduct regular audits and assessments to ensure that data protection standards remain in place for international transfers, ensuring ongoing compliance with the PDPA of 2019 and identifying potential issues or risks.

8. Guidance and Updates
- Regulatory Guidance: Organizations should stay informed about updates and guidelines from the Personal Data Protection Committee regarding cross-border data transfers. The PDPC may issue additional rules or guidance that impact how cross-border data transfers are managed.

Duration of storage (in Thailand)
Principally, we store your data for as long as it is necessary for the purposes for which they were collected or processed or for as long as we have a legitimate interest in storing the data. In all other cases, we delete your personal data with the exception of data we are obliged to store for the fulfillment of legal obligations.

Cookies
Categories
We distinguish between cookies that are mandatorily required for the technical functions of the online service and such cookies and tracking mechanisms that are not mandatorily required for the technical function of the online service.

It is generally possible to use the online service without any cookies that serve non-technical purposes.

- **Technically required cookies**

By technically required cookies we mean cookies without those the technical provision of the online service cannot be ensured. These include e.g. cookies that store data to ensure smooth reproduction of video or audio footage.
Such cookies will be deleted when you leave the website.

- **Marketing cookies and tracking mechanisms**

General
By using marketing cookies and tracking mechanisms we and our partners are able to show you offerings based on your interests, resulting from an analysis of your user behavior:

- Statistics:
By using statistical tools, we measure e.g. the number of your page views.

- Conversion tracking:

Our conversion tracking partners place a cookie on your computer ("conversion cookie") if you accessed our website via an advertisement of the respective partner. Normally these cookies are no longer valid after 30 days. If you visit certain pages of our website and the cookie has not yet expired, we and the relevant conversion partner can recognize that a certain user clicked on the advertisement and thereby was redirected to our website. This can also be done across multiple devices. The information obtained by means of the conversion cookie serves the purpose of compiling conversion statistics and recording the total number of users who clicked on the respective advertisement and were redirected to a website with a conversion tracking tag.

- Social plugins:

Some of the pages of our online service involve content and services of other providers (e.g. Facebook, Twitter) which also may use cookies and active modules.

- Retargeting:

These tools create user profiles by means of advertising cookies or third-party advertising cookies so called "web beacons" (invisible graphics that are also called pixels or tracking pixels), or by means of comparable technologies. These are used for interest-based advertising and to control the frequency with which the user looks at certain advertisements. The relevant provider is the controller responsible for the processing of data in connection with the tool. The providers of the tools might disclose information also to third parties for the purposes mentioned above. Please note the data protection notices of the relevant provider in this context.

- Please note that using the tools might include transfer of your data to recipients outside of the EEA where there is no adequate level of data protection pursuant to the GDPR (e.g. the USA). For more details in this respect please refer to the following description of the individual marketing tools:

Security during data processing

We take all the necessary technical and organizational measures to ensure appropriate levels of security and to protect your personal data particularly from the risks of unintended or unlawful destruction, manipulation, loss, alteration, or disclosure to or access by unauthorized third parties. We are constantly trying to improve our security measures and keep them state of the art.

User rights

To enforce your rights, please use the information in the section "Contact information of the data protection officer". Please make sure that we can unambiguously identify you.

- **Right to information and access**

You have the right to obtain confirmation from us about whether or not your personal data is being processed, and, if this is the case, access to your personal data.

- **Right to correction and deletion**

You have the right to obtain the rectification of inaccurate personal data. As far as statutory requirements are fulfilled you have the right to obtain the completion or deletion of your data. This does not apply to data which is necessary for billing or accounting purposes or which is subject to a statutory retention period. If access to such data is not required, however, its processing is restricted (see the following).

- **Restriction of processing**

If the legal requirements are fulfilled, you can demand that we restrict the processing of your data.

- **Objection to data processing based on the legal basis of “legitimate interest”**

You have the right to object to the processing of your personal data at any time, insofar as this is based on legitimate interest. We will then terminate the processing of your data, unless we demonstrate compelling legitimate grounds according to legal requirements which override your rights.

- **Withdrawal of consent**

In case you consented to the processing of your data, you have the right to revoke this consent at any time with effect for the future. The lawfulness of data processing prior to your withdrawal remains unchanged.

Data portability

If the legal requirements are fulfilled, you may request to receive data that you have made available to us in a structured, common and machine-readable format or - if technically feasible - to request that the data be transmitted to a third party.

Right to lodge complaint with supervisory authority

You have the right to lodge a complaint with a supervisory authority. You can appeal to the supervisory authority, which is responsible for your place of residence or your state of residency or to the supervisory authority responsible for us through email: DPEnquiries@bosch.com

Contact details of the supervisory authority:

Office address:

Data Protection Officer, ASEAN
Robert Bosch (S.E.A.) Pte. Ltd.
11 Bishan Street 21
Singapore 573943
Email: asean.dpo@sg.bosch.com
Phone number: +65 6258 5511

Contact information for the Data Protection Officer in Germany

- To contact Bosch's Data Protection Officer in Germany: SupportDeutschland.HRIT@de.bosch.com

Adjustments to the Data Protection Notice

We reserve the right to adjust our security and data protection measures. In such cases, we will amend our data protection notice accordingly. Please, therefore, notice the current version of our data protection notice in the job advertisement.

Contact information of the data protection officer

You can reach our data protection officer under:

Data protection officer
Information Security and Privacy (C/ISP)
Robert Bosch GmbH
Postbox: 30 02 20
70442
Stuttgart
GERMANY
E-Mail: DPO@bosch.com

To assert your rights please use the following link: https://request.privacy-bosch.com/

Should the legal entity to which your request refers not be selectable on the linked page, or to notify a data protection incident please use the following link:
https://www.bkms-system.net/bosch-dataprotection

Effective date: 29.10.2024

Annex 1:
GDPR Data Privacy Notice

Service Provider	Processing
SmartRecruiters GmbH Dircksenstraße 47 10178 Berlin SmartRecruiters SP. Z o.o. Fabryczna 20, 31-553 Krakow, Poland SmartRecruiters Inc. 225 Bush Street, San Francisco, CA 94104, USA	Provision and development of the cloud platform ("Software as a Service") for the above purposes. Processing of the provided personal data.
Signum GmbH Rungestraße 19 10179 Berlin	Processing of the personal data for career path check
Amazon Web Services Inc. 10 Terry Avenue North Seattle, WA 98109-5210, USA	Provision and operation of the technical infrastructure for the Cloud-Platform ("Plattform as a Service")
Mailgun Technologies, Inc. 112 East Pecan Street Suite 1135 San Antonio, TX 78205, USA	Processing of the generated email communication between BOSCH and the applicant
Text Kernel BV Nieuwendammerkade 28A17 Amsterdam, Noord-Holland 1022 AB The Netherlands	Provision, operation and further development of the application to import the data from CVs (CV-parsing)
I.K. Hofmann Projektmanagement GmbH Lina-Ammon-Str. 19 90471 Nürnberg	Processing of personal data for video interviews / selection process
Catalytic Inc. 954 W. Washington BLVD Suite 700 Chicago, IL 60607	Processing of personal data for reimbursement of personal job interview expenses.
HiredScore, Inc. 158 Mercer Street, Suite 3M, New York, NY 10012	Provision of AI solution for suggesting suitable offers for job applicants