



## DATA PRIVACY NOTICES

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter referred to only as “GDPR”), the company Kia Slovakia s. r. o. seated at Sv. Jána Nepomuckého 1282/1, 013 01 Teplička nad Váhom, Slovak Republic, ID 35 876 832 provides its data subjects with the following information:

**Controller:** **Kia Slovakia s. r. o.** seated at Sv. Jána Nepomuckého 1282/1, 013 01 Teplička nad Váhom, Slovak Republic, ID 35 876 832, company registered with the Business Registry of the District Court Žilina Sec. Sro, Insert No 15074/L (hereinafter referred to only as the “Controller” or “KaSK”).

**Data Protection Officer (DPO):** [podnet@kia.sk](mailto:podnet@kia.sk) - should you have any questions regarding the processing of personal data, you may contact the Data Protection Officer.

### Rights of the Data Subjects:

#### Right of access (Art. 15 GDPR)

The data subject has the right to be informed whether the personal data concerning him/ her are being processed and, if so, he/she has the right to access his/her personal data. The data subject has the right to be provided with copies of the personal data that Controller processes about him/ her as well as with information on how personal data is processed. Controller provides this information in a form that reflects the form of the data subject request or required method of provision. Controller is entitled to charge a reasonable fee corresponding to the administrative costs in case of repeated requests from data subject if he/she repeatedly requests personal data to the same extent.

#### Right to rectification (Art. 16 GDPR)

Controller is only entitled to process correct and up-to-date personal data, so it is in its interest for the data subject to report of processing of incomplete, incorrect or inaccurate data and to request a correction. Based on the right to correct the processed personal data, Controller will complete or correct incorrect personal data without undue delay

#### Right to erasure (Art. 17 GDPR)

The data subject has the right to demand deleting of all data that are being processed illegally (e.g. the data subject has withdrawn his consent to the data processing and there is no other legal basis of processing).

#### Right to restriction of processing (Art. 18 GDPR)

The data subject has the right to restrict data processing if the right of rectification has been applied or if he/she objects to the personal data erasure, if their processing is illegal or Controller no longer needs these



**Right to data portability (Art. 20 GDPR)**

personal data for processing but the data subject needs the data to prove, assert or defend legal claims. In such cases, Controller will limit the processing of personal data to the time strictly necessary.

The data subject has the right to obtain and request Controller to transfer personal data provided by him/her to another Controller in a structured, commonly used and readable format, but only in the case of data processed on a legal basis, with the consent of the data subject or on the basis of a contract to which the data subject is a party.

**Right to object (Art. 21 GDPR)**

The data subject is entitled to object personal data processing if he/she considers that it is unjustified or he/she requires to reconsider profiling or result of automated decision-making. Controller may not further process personal data unless it proves the necessary legitimate interests for data processing which outweigh the interests, rights and freedoms of the data subject, or the reasons for proving, asserting or defending legal claims.

**Right to withdraw consent (Art. 7 (3) GDPR)**

In case of data processing based on the data subject`s consent, data subject has the right to revoke the consent at any time by sending it to e-mail [podnet@kia.sk](mailto:podnet@kia.sk) or in person at Controller's registered office, Compliance and internal audit section. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

**Right to lodge a complaint (Art. 77 GDPR)**

The data subject may enforce his/her rights and address to Controller any comments or complaints regarding the processing of his/her personal data, by sending an e-mail to [podnet@kia.sk](mailto:podnet@kia.sk) or in writing at the address of Controller's registered seat or in person at the Controller's registered office, while he/her also has the right to file a complaint with the Office for Personal Data Protection of the Slovak Republic, with its registered office at Budova Park One Námestie 1. mája 18, 811 06 Bratislava, Slovak Republic which is the supervisory authority.

**Changes & Amendments to Data Privacy**

If it becomes necessary to implement changes or amendments, these Data Privacy Notices will be updated without delay, and the changes will be announced on our website [www.kia.sk](http://www.kia.sk). Any modifications to our Privacy Notices will become effective upon publication on our website. If you have any questions regarding your rights or specific requests related to your personal data, please contact us using the contact details provided above.



## **INDEX**

**INFORMATION FOR EMPLOYEES**

**INFORMATION FOR MICROSOFT 365 USERS**

**INFORMATION FOR APPLICANTS FOR EMPLOYMENT, VOCATIONAL TRAINING OR EDUCATION OR SCHOLARSHIP PROGRAMS**

**INFORMATION FOR TEMPORARY ASSIGNED EMPLOYEES**

**INFORMATION FOR STUDENTS, PUPILS AND THEIR LEGAL GUARDIANS**

**INFORMATION FOR VISITORS**

**INFORMATION FOR INDIVIDUALS ENTERING CCTV MONITORED AREA**

**INFORMATION FOR BUSINESS PARTNERS**

**INFORMATION FOR KIA CUSTOMERS**



## CONTROLLER`S EMPLOYEES

### Purposes of Processing:

- Fulfillment of the Controller's legal obligations related to employment and other labor-law relationships with employees, including personnel and payroll administration (e.g., employee records, attendance management, reporting to health insurance companies and the Social Insurance Agency, payroll processing, planning and organizing business trips, reimbursement of incurred expenses, and compliance with obligations related to employing third-country nationals).
- Fulfillment of the Controller's obligations arising from contractual relationships based on employment contracts, agreements on work performed outside the employment relationship, or other agreements concerning individual and collective labour relations (e.g., implementation of social policies, provision and verification of employee benefits, supplementary pension insurance and other types of insurance), including obligations arising from pre-contractual relationships.
- Human resources planning and management, including employee needs analysis, administration of organizational structures, disciplinary committees, training, talent management, succession planning, substitution, career development, remuneration, competency and performance evaluation, organization of surveys and questionnaires, and internal administrative transfers of personal data within Hyundai Motor Group and Kia Corporation.
- Safety and protection of life and health, fire protection, prevention of workplace injuries and hazardous events, and monitoring work rotation schedules.
- Security and protection of the Controller's property, including access control to the Controller's premises, access management to internal infrastructure and information systems (applications, software programs, networks, shared access, web browsers and web-based programs and applications), and prevention and investigation of security incidents.
- Compliance with the applicable legal regulations, internal rules of the Controller, and contractual obligations, including administration of reporting and control duties, performing inspections and audits, investigating violations of rules, procedures, and standards, and handling breaches of employee discipline.
- Administration of inquiries, suggestions, and complaints addressed to the Controller, including the agenda for exercising data subject rights.
- Litigation and non-litigation proceedings, debt recovery, as well as the enforcement and protection of legal claims, including gathering of supporting documents, evidence, and other information, and the submission of initiatives, inquiries, and complaints.



- Corporate administration, including record-keeping of formal requests, proposed changes, and extracts from relevant registers, handling and recording requests for cooperation, management of legal and other documents, and fulfilling obligations related to record retention for archive and registry purposes.
- Administration of process improvement proposals (known as ELAN).
- Organization of events, competitions, and other activities to support employee relations.
- Presentation of the Controller's activities and publication in internal and external media (PR agenda, creation of visual, audio, and audiovisual recordings).

Legal Basis:

- Art. 6 (1) (a) GDPR - Data Subject's Consent - creation and publishing of visual, audio, and audiovisual recordings, or other expressions of data subjects.
- Art. 6 (1) (b) GDPR - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.
- Art. 6 (1) (c) GDPR - processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Art. 6 (1) (f) GDPR - legitimate interests of the Controller
  - protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities,
  - development of employees' skills and abilities and the transfer of data for the global human resources management requirements,
  - streamline internal operations and ensure principles of efficiency and economic performance in the execution of business activities,
  - fulfilment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller,
  - security and protection of the internal infrastructure operation and protection of IT systems against disruption or other unauthorized interference.
- Art. 9 (2) (a) GDPR - the data subject has given explicit consent to the processing - planning and organizing business trips (e.g. food preferences due to certain food intolerance).
- Art. 9 (2) (b) GDPR - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the data subject in the field of employment and social security and social protection law.
- Art. 9 (2) (f) GDPR - processing is necessary for the establishment, exercise or defense of legal claims.
- Art. 9 (2) (h) GDPR - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee.



Categories of Personal Data:

- Identification and Contact Details - name, surname, academic title, birth date, Slovak national identification number, address, ID card number, passport number, private email address and phone number, employee identification number, clothing size, photograph, work email address and phone number, signature.
- Salary and Financial Data - salary data and other income data, data on taxes, contributions and insurance, bank account number, time management data, identification data of the employee's spouse and children to the extent necessary for claiming a tax bonus and annual tax settlement, data on wage deductions, reimbursements for incurred expenses.
- Contractual Data - data to the extent of the employment contract or agreements on work performed outside employment relationship, or to the extent of other agreements related to individual employment relationships (e.g. employment start date, changes or termination of employment, job position and function), or data included in other contracts and agreements concluded between the Controller and the data subject (e.g., liability insurance, participation in a competition or event).
- Profession Data - qualification data and data related to professional competence for performing work, data related to professional education and development of competencies and skills, data on performance and competency evaluation, other data related to work performance results.
- Other Employment-related Data - data regarding roles and responsibilities, organization and functions, including job rotations, business trips, data related to work results and submitted proposals for improvement (ELAN).
- Compliance Data - data regarding breaches or violations of legal regulations, internal rules & policies of the Controller and contractual obligations of the Controller, disciplinary proceedings and measures, data obtained through public and internal databases and registers checks, or data received through the whistleblowing channels, complaints, notifications, or through other communication channels or forms (e.g., conflict of interest disclosure form), and data regarding activity in relation to internal infrastructure and activity and communication within the Controller's information systems.
- Data Related to Dispute and Non-Dispute Proceedings and Debt Recovery - claims data, other data to the extent of the relevant documentation, communication, court hearings, or other related activities.
- Special Categories of Personal Data - health data and medical fitness to work, occupational health and safety and fire protection agenda, and trade union membership data.

Data Subject Categories:

Employees of the Controller and other natural persons performing work based on agreements on work performed outside of employment, as well as the employee's spouse and children.

Collection of Personal Data:

Controller collects Personal Data:



- Directly from Data Subject (filling in questionnaires and documents, in communication etc.).
- From the other Controller (e.g. information received through the whistleblowing channels).
- Creation (e.g. photography).

Disclosure of Personal Data:

- Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Seoul, Republic of Korea and Kia Europe GmbH, seated at Theodor-Heuss-Allee 11, 60486 Frankfurt am Main, Federal Republic of Germany - internal administration purposes and global management of human resources.
- Government Authorities - state authorities, law enforcement agencies and courts, notary and executor offices, and other public entities and institutions, the Social Insurance Agency, health insurance companies - for the fulfilment of legal obligations and the enforcement and protection of legal claims, etc.
- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors, supplementary pension savings companies, pension management companies, postal services, banks, trade union organizations, occupational health service providers, and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose). Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e.g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany), provider of private security services, providers of canteen services etc.

Publication of Personal Data:

Personal Data to the extent of the framework defined by the purpose *Presentation of the Controller's activities and publication in internal and external media.*

International Data Transfers:

Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Seoul, Republic of Korea (internal administration purposes and global management of human resources).

Automated Decision-Making and Profiling:

- The Controller ensures automated rotation of employees (production operators) in order to comply with legal requirements for the manual workload.
- The Controller obtains supporting data for determining the amount of the variable component of the salary through a partially automated process (automatic evaluation of key performance results). This processing does not apply to production operators.



Data Retention Period:

The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed on the basis of consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.

Rights of the Data Subjects:

Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.

## MICROSOFT 365 USERS

### Purposes of Processing

Providing smart workplace to KaSK employees and to allow seamless collaboration within the organization and with the Controller's affiliated companies.

Microsoft Teams Recording & Transcribing Meetings - training purposes (creation of training materials), project purposes, accessibility purposes (if users prefer reading over listening), note-taking purposes, creation of meeting summaries & task management (Copilot).

### Legal Basis:

- Art.6 (1) (b) - Performance of a contract with Data Subject or Processing in order to take steps at the request of the Data Subject prior to entering a contract (e.g. processing of name and email address in order to set up employee account for employee to be able to use M365 in connection with their employee duties) or in order to take steps prior to entering a contract.
- Art. 6 (1) (f) GDPR - legitimate interests of the Controller, which is to improve the work experience, to provide a smart workplace, and to ensure an efficient and seamless collaboration within the organization and with the Controller's affiliated companies.
- Art. 9 (2) (a) GDPR - the data subject has given explicit consent to the processing - facial biometry and fingerprints (Windows Hello).

### Categories of Personal Data:

- Identification and Contact Details - name, surname, photography, work email address and phone number, position and function.
- Authentication Details - user name, password or PIN code, security question, facial biometry, fingerprint, activity status.
- Documents and files - text, audio, video.
- Communication - Microsoft Teams (chat, videocalls), MS Outlook (email, calendar).
- Logfiles and system generated protocol data - e.g. IP address, date and time of log-in, log-out.
- Device data - e.g. browser, operating system.
- Recording & Transcribing Meetings (Microsoft Teams):
  - When using the recording feature, the information processed is the audio (voice of participants - only when participants are not muted), video (images of participants - only when the camera is activated), and screen sharing activity. It may include any other content shared during the meeting.



- When using the transcription feature, the information processed is the audio (voice of participants - only when participants are not muted) since transcriptions provide a written record of what was said during the meeting.
- When Copilot is activated, the information processed is the audio (spoken words of all participants in the meeting) and the identity of each speaker to attribute comments and actions correctly. This includes name and any profile information visible about data subjects in the meeting.
- Only the meeting organizer and participants - employees from KaSK can start and stop the recording and transcription. KaSK is not responsible for third-party compliance regarding recording and transcription; participants decide whether to consent or Opt-Out.

Data Subject Categories:

Natural persons who have been assigned smart work tools (e.g., a laptop with Microsoft 365 services installed), and other individuals involved in communication carried out with Microsoft 365 tools.

Collection of Personal Data:

Controller collects Personal Data:

- Directly from Data Subject (e.g. uploading photography).
- From the other Controller (e.g. user activity logs).

Disclosures of Personal Data:

- Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany,
- Microsoft Ireland Operations Limited (One Microsoft Place, South County Business Park, Leopardstown Dublin 18, Ireland,
- Microsoft Corporation (One Microsoft Way Redmond, Washington 98052, USA,
- Third parties acting as Microsoft's subprocessors to support certain functions, such as technical support and service maintenance. A list of the relevant subprocessors used by Microsoft in connection with its services is available at the following link (at the end of the webpage): <https://www.microsoft.com/en/trust-center/privacy/data-access>.
- Access to the transcription is controlled by the meeting organizer and co-organizers. All Participants can view the transcription through the meeting chat, or the Recap tap in Teams.
- Copilot in teams: within the Controller, only users with Copilot license can access the information generated by Copilot. Information processed during a meeting, such as summaries and action items are accessible to the meeting participants.

Publication of Personal Data:

No publishing of data will be carried out.



International Data Transfers:

Any content data at rest will only be stored in data centers located in the European Union (for more information please see here: <https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide>). However, it may also be required for the purpose of using the M365 to transfer certain personal data to Microsoft Corporation in the United States. The United States do not provide an adequate level of protection for personal data. Therefore, all transfers to Microsoft Corporation in the United States are governed by the EU Standard Contractual Clauses (processor-to-processor) between Microsoft Ireland Operations Limited and Microsoft Corporation (a copy of which can be requested at [it-service-desk@kia.eu](mailto:it-service-desk@kia.eu)).

An exception to the above is the data transfer to the Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Soul, Republic of Korea and for the purposes of processing related to project and task management and trainings (meetings recordings & transcriptions).

Automated Decision-Making and Profiling:

No automated decision-making or profiling of data will be carried out.

Data Retention Period:

The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notices or as required by applicable law. (i) Data that relate to the account and the relevant user will be deleted 90 days after deletion of the account; (ii) content data will be deleted in accordance with the relevant retention periods that have been defined and that apply to the relevant content data (if not deleted before, Microsoft will retain content data in a limited function account for 90 days after expiration or termination of subscription so that the data may be extracted; after the 90-day retention period ends, Microsoft will disable the account and delete the data); (iii) technical data (such as log-files or system-generated data) will be deleted within 180 days from collection/creation.

Microsoft Teams meeting recordings and transcriptions will be kept for 45 days. If the information is no longer necessary based on the previous, call recordings are automatically deleted after 45 days.

Rights of the Data Subjects:

Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.



## APPLICANTS FOR EMPLOYMENT, VOCATIONAL TRAINING OR EDUCATION OR SCHOLARSHIP PROGRAM

### Purposes of processing:

- Selection of a candidate for a vacant job position or a position within a vocational education and training program (so-called dual education) or a scholarship program.
- Maintaining a database of the applicants for the purpose of offering vacant positions.

### Legal Basis:

- Art. 6 (1) (a) GDPR - Data Subject`s Consent - in case the applicant wishes to be listed in the database.
- Art. 6 (1) (b) GDPR - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.
- Art. 9 (2) (h) GDPR - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee.

### Categories of Personal Data:

- Identification and Contact Details - name, surname, academic title, birth date, Slovak national identification number, address, ID card number, private email address and phone number, employee identification number, photograph, signature.
- Salary and Financial Data - salary data.
- Profession Data - qualification data and data related to professional competence for performing work, data related to professional education.
- Other Recruitment-related Data - data to the extent provided in CVs, certificates, diploma, academic progress data (grades, score) - pupils and students etc.
- Special Categories of Personal Data - health data and medical fitness to work.

### Data Subject Categories:

Job applicants, Applicants for vocational training or education or scholarship program utilized by the Controller, Legal Guardians of those applicants for vocational training or education or scholarship program utilized by the Controller who are without full legal capacity.

### Collection of Personal Data:

#### Controller collects Personal Data:

- Directly from Data Subject (e.g. applying for the job position).
- From the other Controller (e.g. employment portal, social networks, recommendation of the Employee).



Disclosures of Personal Data:

- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., occupational health service provider, recruitment agencies in case of a vacant positions for temporary assigned employees, educational institutions - in relation to applicants for vocational education and training or a scholarship program who are their students and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).
- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e.g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany), provider of private security services, etc.

Publication of Personal Data:

No publication of data will be carried out.

International Transfers of Data:

No international transfers of data will be carried out.

Automated Decision-Making or profiling:

No automated decision-making or profiling of data will be carried out.

Data Retention Periods:

- For the purpose of recruiting a job applicant - personal data is deleted one year after the conclusion of the selection process, which occurs either upon the formation of a contractual relationship or upon delivery of a notice to the applicant indicating that no such relationship will be established.
- For the purpose of recruiting an applicant for vocational education and training or a scholarship - personal data is deleted 18 months from the date of delivery of the application for vocational education and training or scholarship.
- For the purpose of maintaining a database - personal data is deleted one year from the date of consent, or earlier if it is withdrawn.

Rights of the Data Subjects:

Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.



## TEMPORARY ASSIGNED EMPLOYEES

### Purposes of Processing:

- Fulfillment of the Controller's legal obligations related to temporary assignment of employees (personnel administration, time management).
- Human resources planning and management, including temporary assigned employee needs analysis, administration of organizational structures, violations of work standards and policies, occurrence of damage related incidents, trainings, organization of surveys and satisfaction questionnaires.
- Safety and protection of life and health, fire protection, prevention of workplace injuries and hazardous events, and monitoring work rotation schedules.
- Security and protection of the Controller's property, including access control to the Controller's premises, management and control of access to internal infrastructure and information systems (applications, software programs, networks, shared access, web browsers, and web-based programs and applications), prevention and investigation of security incidents.
- Compliance with the applicable legal regulations, internal rules of the Controller, and contractual obligations, including administration of reporting and control duties, performing inspections and audits, investigating violations of rules, procedures, and standards, and handling breaches of employee discipline.
- Administration of inquiries, suggestions, and complaints addressed to the Controller, including the agenda exercising right of data subjects.
- Litigation and non-litigation proceedings, debt recovery, as well as the enforcement and protection of legal claims, including gathering of supporting documents, evidence, and other information, and the submission of initiatives, inquiries, and complaints.
- Administration of process improvement proposals (known as ELAN).
- Organization of events, competitions, and other activities to support employee relations.
- Presentation of the Controller's activities and publication in internal and external media (PR agenda, creation of visual, audio, and audiovisual recordings).



Legal basis:

- Art. 6 (1) (a) GDPR - Data Subject`s Consent - creation and publishing of visual, audio, and audiovisual recordings, or other expressions of data subjects.
- Art. 6 (1) (b) GDPR - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.
- Art. 6 (1) (c) GDPR - processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Art. 6 (1) (f) GDPR - legitimate interests of the Controller
  - protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities,
  - to support the development of skills and competencies of temporary assigned employees,
  - streamline internal operations and ensure principles of efficiency and economic performance in the execution of business activities,
  - fulfilment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller,
  - security and protection of the internal infrastructure operation and protection of IT systems against disruption or other unauthorized interference.
- Art. 9 (2) (f) GDPR - processing is necessary for the establishment, exercise or defense of legal claims.
- Art. 9 (2) (h) GDPR - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee.

Categories of Personal Data:

- Identification and contact details - name, surname, academic title, birth date, Slovak national identification number, address, private email address and phone number, temporary employee identification number, clothing size, photograph, and signature.
- Salary and Financial Data - salary data and other income data, data on taxes, contributions and insurance, time management data and data on wage deductions, reimbursements for incurred expenses.
- Contractual data - information included in contracts and agreements concluded between the Controller and the data subject (e.g. participation in a competition or event).
- Professional data - qualification details and data related to professional competence for performing work activities, including information on professional training and development of skills and competencies.



- Other personal data related to temporary assignment - data regarding roles and responsibilities, organization and functions, including job rotations, business trips, data related to work results and submitted proposals for improvement (ELAN).
- Compliance data - data regarding breaches or violations of legal regulations, internal rules & policies of the Controller and contractual obligations of the Controller, data obtained through public and internal databases and registers checks, or data received through the whistleblowing channels, complaints, notifications, or through other communication channels or forms (e.g., conflict of interest disclosure form), and data regarding activity in relation to internal infrastructure and activity and communication within the Controller's information systems.
- Data related to litigation and non-litigation proceedings and debt collection - claims data, other data to the extent of the relevant documentation, communication, court hearings, or other related activities.
- Special categories of personal data - health data and medical fitness to work, occupational health and safety and fire protection agenda.

Data Subject Categories:

Temporary Assigned Employees.

Collection of Personal Data:

The Controller collects personal data:

- Directly from the data subject (by completing forms and documentation, communication).
- From another Controller (e.g. a temporary employment agency).
- Creation (e.g. a photograph).

Disclosure of Personal Data:

- Government authorities - state authorities, law enforcement agencies and courts, notary and executor offices, and other public entities and institutions, the Social Insurance Agency, health insurance companies - for the fulfilment of legal obligations and the enforcement and protection of legal claims, etc.
- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors, postal services, banks, trade union organizations, occupational health service providers, and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).
- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e.g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany), provider of private security services, providers of canteen services etc.



Publication of Personal Data:	Personal data to the extent necessary by the purpose <i>Presentation of the Controller's activities and publication in internal and external media.</i>
International Data Transfers:	No international transfers of data will be carried out.
Automated Decision-Making and profiling:	<ul style="list-style-type: none"><li>- The Controller ensures automated rotation of temporary assigned employees (production operators) in order to comply with legal requirements for the manual workload.</li></ul>
Data Retention Period:	The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed based on consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.
Rights of the Data Subjects:	Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.

## VOCATIONAL EDUCATION AND TRAINING, SCHOLARSHIP PROGRAM, AND SUPPORT FOR FINAL THESES

Purpose of processing:

- Fulfilment of the Controller's legal obligations related to vocational education and training (dual education).
- Fulfilment of the Controller's obligations arising from contractual relationships, including obligations arising from pre-contractual relationships.
- Human resources planning and management including pupils and students' needs, administration of organizational structures, violations of work standards and policies, occurrence of damage related incidents, education and trainings, and the organization of surveys and satisfaction questionnaires.
- Safety and protection of life and health, fire protection, prevention of workplace injuries and hazardous events.
- Security and protection of the Controller's property, including access control to the Controller's premises, access management to internal infrastructure and information systems (applications, software programs, networks, shared access, web browsers and web-based programs and applications), and prevention and investigation of security incidents.
- Compliance with the applicable legal regulations, internal rules of the Controller, and contractual obligations, including administration of reporting and control duties, performing inspections and audits, investigating violations of rules, procedures, and standards, and handling breaches of employee discipline.
- Administration of inquiries, suggestions, and complaints addressed to the Controller, including the agenda for exercising data subject rights.
- Litigation and non-litigation proceedings, debt recovery, enforcement and protection of legal claims, including gathering of supporting documents, evidence, and other information, and the submission of initiatives, inquiries, and complaints.
- Organization of events, competitions, and other activities to support relations.
- Presentation of the Controller's activities and publication in internal and external media (PR agenda, creation of visual, audio, and audiovisual recordings).



Legal Basis:

- Art. 6 (1) (a) GDPR - Data Subject`s Consent - creation and publishing of visual, audio, and audiovisual recordings, or other expressions of data subjects.
- Art. 6 (1) (b) GDPR - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.
- Art. 6 (1) (c) GDPR - processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Art. 6 (1) (f) GDPR - legitimate interests of the Controller
  - protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities,
  - support the development of skills and competencies of pupils and students,
  - streamline internal operations and ensure principles of efficiency and economic performance in the execution of business activities,
  - fulfillment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller,
  - security and protection of the internal infrastructure operation and protection of IT systems against disruption or other unauthorized interference.
- Art. 9 (2) (f) GDPR – processing is necessary for the establishment, exercise or defense of legal claims.

Categories of Personal Data:

- Identification and contact details - name, surname, academic title, birth date, Slovak national identification number, address, private email address and phone number, temporary employee identification number, clothing size, photograph, and signature.
- Salary and financial data - time management data.
- Contractual data - information included in contracts and agreements concluded between the Controller and the data subject.
- Professional data - qualification details and data related to professional competence for performing work activities, including information on professional training and development of skills and competencies.
- Other personal data related to vocational education and training or the scholarship program - data concerning assigned roles and responsibilities, organizational and functional placement including rotations, data related to academic and work performance, and data within the scope of the final thesis.
- Compliance data - data regarding breaches or violations of legal regulations, internal rules & policies of the Controller and contractual obligations of the Controller, data obtained through public and internal databases and registers checks, or data received through the whistleblowing channels, complaints,



notifications, or through other communication channels or forms (e.g., conflict of interest disclosure form), and data regarding activity in relation to internal infrastructure and activity and communication within the Controller's information systems.

- Data related to litigation and non-litigation proceedings and debt collection - claims data, other data to the extent of the relevant documentation, communication, court hearings, or other related activities.
- Special categories of personal data - data concerning health and medical fitness for work, occupational health and safety, and fire protection agenda.

Data Subject Categories:

Pupils, students, and the legal guardians of underage pupils and students.

Collection of Personal Data:

The Controller collects personal data:

- Directly from data subject (e.g. by filling out forms and documentation, communication).
- From another data Controller (e.g. a school).
- Creation (e.g. photograph).

Disclosure of Personal Data:

- Government Authorities - state authorities, law enforcement agencies and courts, notary and executor offices, and other public entities and institutions - for the fulfilment of legal obligations and the enforcement and protection of legal claims, etc.
- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors, postal services, banks, occupational health service providers, schools, universities and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).
- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e. g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany), provider of private security services, providers of canteen services etc.

Publication of Personal Data:

Personal Data to the extent of the framework defined by the purpose *Presentation of the Controller's activities and publication in internal and external media.*

International Data Transfer:

No international transfers of data will be carried out.

Automated Decision-Making and profiling:

No automated decision-making or profiling of data will be carried out.



Data Retention Period:

The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed based on consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.

Rights of the Data Subjects:

Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.

## VISITOR MANAGEMENT

### Purpose of processing:

- Safety and protection of life and health, fire protection, prevention of occupational injuries and hazardous events.
- Safety and protection of life and health, fire protection, prevention of workplace injuries and hazardous events, and monitoring compliance with designated work rotation schedules.
- Security and protection of the Controller's property, including access control to the Controller's premises, management and control of access to internal infrastructure and information systems (applications, software programs, networks, shared access, web browsers, and web-based programs and applications), prevention and investigation of security incidents.
- Compliance with the applicable legal regulations, internal rules of the Controller, and contractual obligations, including administration of reporting and control duties, performing inspections and audits, investigating violations of rules, procedures, and standards.
- Presentation of the Controller's activities and publication in internal and external media (PR agenda, creation of visual, audio, and audiovisual recordings).

### Legal Basis:

- Art. 6 (1) (a) GDPR - Data Subject's Consent - creation and publishing of visual, audio, and audiovisual recordings, or other expressions of data subjects.
- Art. 6 (1) (f) GDPR - legitimate interest of the Controller
  - protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities,
  - streamline internal operations and ensure principles of efficiency and economic performance in the execution of business activities,
  - fulfilment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller,
  - security and protection of the internal infrastructure operation and protection of IT systems against disruption or other unauthorized interference.
- Art. 9 (2) (f) GDPR – processing is necessary for the establishment, exercise or defense of legal claims.



Categories of Personal Data:

- Identification data of data subjects - name, surname, academic title, date of birth, personal identification number, ID card number, service card number, passport number, residential address, signature, vehicle registration number, and the name of the legal entity represented by the data subject, position and function within the represented legal entity, MAC address of the visitor's device connecting to the Controller's network.
- Data related to compliance with rules - data on violations of rules arising from applicable legal regulations, internal policies of the Controller, and contractual obligations; data obtained from checks of outputs from public and internal databases and registers; or data from reporting channels, complaints, notifications, or other means of providing information (e.g. conflict of interest disclosure form); and data regarding activity related to the Controller's internal infrastructure and activity and communication within the Controller's information systems.
- Data related to dispute and non-dispute proceedings and debt recovery - data to the extent of legal claims, documentation, communication, court hearings, and data processed based on other related activities.
- Special categories of personal data - data processed in the context of occupational health and safety and fire protection agendas.

Data Subjects Categories:

Natural persons (visitors) entering the premises and areas of the data Controller.

Collection of Personal Data:

Data Controller collects Personal Data:

- Directly from the data subject (e.g. by filling out the forms and documentations, communication).
- From another data Controller (e.g. the data subject's employer).
- Creation (e.g. a photograph).

Disclosure of Personal Data:

- Government Authorities - state authorities, law enforcement agencies and courts, notary and executor offices, law firms, accounting and tax advisors, auditors and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).
- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors, supplementary pension savings companies, pension management companies, postal services, banks, trade union organizations, occupational health service providers, and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).



- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e.g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany), provider of private security services, providers of canteen services etc.

Publication of Personal Data:	Personal Data to the extent of the framework defined by the purpose <i>Presentation of the Controller's activities and publication in internal and external media.</i>
International Data Transfer:	No international transfers of data will be carried out.
Automated Decision-Making and profiling:	No automated decision-making or profiling of data will be carried out.
Data Retention Period:	The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed based on consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.
Rights of the Data Subjects:	Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.



## CCTV MONITORING

Purpose of Processing:	Monitoring by camera systems to improve the protection of the Controller's property, to enhance the protection of life and health, to obtain evidence for the purpose of asserting potential legal claims, and to monitor work discipline.
Legal Basis:	Art. 6 (1) (f) GDPR - legitimate interest of the Controller protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities.
Categories of Personal Data:	Personal data to the extent of video recording (video recordings capturing the entry of identifiable individuals into areas under surveillance).
Data Subject Categories:	Naturals persons entering area under surveillance.
Disclosures of Personal Data:	Law enforcement agencies and courts (e.g., bodies of the Police Force of the Slovak Republic, state authorities within the system of prosecution and courts of the Slovak Republic), other administrative bodies (e.g., district offices, municipalities), and other entities, if necessary for asserting the Controller's legal claims (e.g., insurance companies, business partners).
Publication of Personal Data:	No publication of data will be carried out.
International Transfers of Data:	Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Seoul, Republic of Korea - online stream of CCTV devices installed as integral part of the global fire prevention system.
Automated Decision-Making or profiling:	No automated decision-making or profiling will be carried out.
Data Retention Period:	The personal data will be automatically deleted after 14 days.
Rights of the Data Subjects:	Right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.

## BUSINESS PARTNERS

### Purpose of processing:

- Contract management - the establishment, modification, and termination of commercial contractual relationships and ensuring their fulfillment.
- Compliance with the applicable legal regulations, internal rules of the Controller and contractual obligations, including administration of reporting and control duties, performing inspections and audits, investigating violations of rules, procedures, and standards, and handling breaches of employee discipline.
- Litigation and non-litigation proceedings, debt recovery, enforcement and protection of legal claims, including gathering documentation, evidence, and other information, and submitting initiatives, inquiries, and complaints.
- Presentation of the Controller's activities and publication in internal and external media (PR agenda, creation of visual, audio, and audiovisual recordings).

### Legal Basis:

- Art. 6 (1) (f) GDPR - legitimate interest of the Controller
  - protection of rights, legally protected interests and property, safety, protection of life and health, as well as the detection and prevention of crime and other antisocial activities,
  - streamline internal operations and ensure principles of efficiency and economic performance in the execution of business activities,
  - fulfilment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller,
  - security and protection of the internal infrastructure operation and protection of IT systems against disruption or other unauthorized interference.
- Art. 9 (2) (f) GDPR - processing is necessary for the establishment, exercise or defense of legal claims.

### Categories of Personal Data:

- Identification and Contact Details - name, surname, academic title, work email address and telephone number, signature, name of the legal entity represented by the data subject, position and function within the represented legal entity, photograph.
- Other data to the extent defined by the relevant contractual obligation - e.g. driver location data of a test drive supplier.
- Data related to legal disputes - data to the extent of legal claims, documentation, communication, court hearings, and data processed based on other related activities.



Data Subject Categories:	Natural persons acting on behalf and representing data Controller's business partner.
Collection of Personal Data:	Controller collects Personal Data: <ul style="list-style-type: none"><li>- Directly from the data subject (through communication).</li><li>- From another data subject (e.g. the data subject's employer).</li></ul>
Disclosure of Personal Data:	<ul style="list-style-type: none"><li>- Government Authorities - state authorities, law enforcement agencies and courts, notary and executor offices, and other public entities and institutions, the Social Insurance Agency, health insurance companies - for the fulfilment of legal obligations and the enforcement and protection of legal claims, etc.</li><li>- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose).</li><li>- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller - providers of IT services (e.g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany) etc.</li></ul>
Publication of Personal Data:	Personal Data to the extent of the framework defined by the purpose <i>Presentation of the Controller's activities and publication in internal and external media.</i>
International Data Transfers:	Kia Corporation, with its registered office at 12 Heolleung-ro, Seocho-gu, Seoul, Republic of Korea - for operational processes and internal administrative purposes.
Automated Decision-Making and profiling:	No automated decision-making or profiling will be carried out.
Data Retention Period:	The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed based on consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for



personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.

Rights of the Data Subjects:

Right to withdraw consent, right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.



## KIA CUSTOMERS

### Purpose of processing:

- Contract management - the establishment, modification, and termination of commercial contractual relationships and ensuring their fulfillment.
- Litigation and non-litigation proceedings, debt recovery, enforcement and protection of legal claims, including gathering documentation, evidence, and other information, and submitting initiatives, inquiries, and complaints.
- Administration of inquiries, suggestions, and complaints addressed to the Controller, including the agenda for exercising data subject rights.

### Legal Basis:

- Art. 6 (1) (b) GDPR - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering a contract.
- Art. 6 (1) (f) GDPR - processing is necessary for the purposes of the legitimate interests pursued by the Controller
  - fulfilment of rights and obligations based on legal regulations, contractual and pre-contractual obligations, as well as compliance with the internal policies of the Controller.
- Art. 9 (2) (f) GDPR - processing is necessary for the establishment, exercise or defense of legal claims.

### Categories of Personal Data:

- Identification and Contact Details - name, surname, academic title, address, email address, telephone number, and signature.
- Other data as required by the relevant contractual obligation - data included in documentation related to claims, VIN, vehicle registration number.
- Data related to legal disputes - data to the extent of legal claims, documentation, communication, court hearings, and data processed based on other related activities.

### Data Subject Categories:

Natural persons - Kia customers.

### Collection of Personal Data:

Controller collects Personal Data:

- Directly from the data subject (as part of communication).
- From another data Controller (e.g. the legal representative of the data subject).



Disclosure of Personal Data:

- Government Authorities - state authorities, law enforcement agencies and courts, notary and executor offices, and other public entities and institutions - for the fulfilment of legal obligations and the enforcement and protection of legal claims, etc.
- Contractual partners of the Controller who process personal data of Data Subjects on their own behalf (e.g., law firms, accounting and tax advisors, auditors and other natural or legal persons who are business and contractual partners of the Controller, according to the extent of the framework defined by the relevant purpose). Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Seoul, Republic of Korea and Kia Europe GmbH, seated at Theodor-Heuss-Allee 11, 60486 Frankfurt am Main, Federal Republic of Germany - internal administration purposes.
- Contractual partners of the Controller who process personal data of Data Subjects on behalf of the Controller providers of IT services (e. g. Hyundai Autoever Europe GmbH, seated at Kaiserleistrasse 8A, 63067 Offenbach am Main, Federal Republic of Germany).

Publication of Personal Data

No publishing of data will be carried out.

International Data Transfer:

Kia Corporation, seated at Heolleung-ro, Seocho-gu 12, Seoul, Republic of Korea (operation processes and internal administration purposes).

Automated Decision-Making and profiling:

No automated decision-making or profiling will be carried out.

Data Retention Period:

The Controller will only process your personal data for as long as it is necessary for the purposes set out in this Privacy Notice or as required by applicable law. In general, personal data collected in connection with the initiation, continuation, or termination of an employment relationship is deleted once that relationship is terminated. Data processed on the basis of consent will be erased no later than the moment such consent is withdrawn, unless legal obligations require the Controller to retain it. Additionally, personal data may be retained for the purpose of asserting, exercising, or defending legal claims, for as long as those claims remain enforceable. Retention periods for personal data related to the Controller's activities and documentation are determined by relevant legislation or outlined within the Controller's internal policies.

Rights of the Data Subjects:

Right of access to personal data, right to rectification or right to erasure, or right to restriction of processing, right to restriction of processing, or right to object as well as right to data portability and right to lodge a complaint with supervisory authority - the Office for Personal Data Protection of the Slovak Republic.