

PERSONAL DATA PROTECTION AND PROCESSING POLICY

1. PURPOSE

The purpose of this Personal Data Protection and Processing Policy ("Policy") is to set out the principles and practices adopted by Anadolu Isuzu Otomotiv Sanayii ve Ticaret A.Ş. (hereinafter referred to as the "Company") in the context of the Law on Protection of Personal Data No. 6698 ("KVKK" or "Law") and related legislation, to which it is subject when processing personal data, to ensure transparency in data processing activities and to inform data subjects. The Company exercises maximum diligence in accordance with applicable legislation and universal values in order to ensure the security of personal data in compliance with the principles of lawfulness, fairness and transparency.

Data Controller Information:

Title : Anadolu Isuzu Otomotiv Sanayii ve Ticaret A.Ş.
Registered Address : Fatih Sultan Mehmet Mahallesi Balkan Caddesi No:58
Buyaka E Blok Tepeüstü 34771 Ümraniye / Istanbul
Factory Address : Şekerpınar Mah. Otomotiv Cad. No:2 41420 Çayırova / Kocaeli
KEP Address : anadoluisuzu@hs01.kep.tr

2. SCOPE AND APPLICATION

This Policy covers all processes within the scope of the Company's activities in which personal data is processed, whether by automated means or by non-automated means as part of any data recording system, as well as all applications, databases and recording environments containing personal data. In the event of any inconsistency between this Policy, prepared on the basis of applicable legislation regarding the processing and protection of personal data, and the applicable legislation, the applicable legislation shall prevail.

This Policy sets out which data constitutes personal data, which personal data is retained, the administrative and technical measures taken for the protection of personal data, and explanations regarding the processing, retention, disclosure and informing of data subjects, transfer to third parties, and protection of personal data.

Data that has been anonymised for the purposes of statistical assessments or studies and can no longer be associated with any natural person, data relating to legal entities, and other data not classified as personal data under the Law, are excluded from the scope of this Policy.

3. DEFINITIONS

Explicit Consent	Consent that is freely given, specific to a particular subject and based on being informed.
Anonymization	The rendering of personal data in such a form that it cannot be linked to an identified or identifiable natural person even by matching with other data.

Employee	The employees of the Company.
Job Applicant	Natural persons who have applied for a job at the Company through any means or have made their CV and related information available for the Company's review.
Data Subject	The natural person whose personal data is processed.
KVK Board	The Personal Data Protection Board.
KVK Authority	The Personal Data Protection Authority.
Recording Medium	Any medium in which personal data is processed by fully or partially automated means, or by non-automated means as part of any data recording system.
Personal Data	Any information relating to an identified or identifiable natural person.
Anonymization of Personal Data	The rendering of personal data in such a form that it can in no way be associated with an identified or identifiable natural person, even by matching with other data.
Deletion of Personal Data	The process of rendering personal data inaccessible and unusable in any manner by the relevant users.
Destruction of Personal Data	The process of rendering personal data inaccessible, irrecoverable and unusable by any person in any manner.
Personal Data Inventory	An inventory maintained by the Company in accordance with statutory procedures and principles, in which personal data processing activities are associated with the purposes, data categories, recipient groups and data subject groups, and which includes the maximum retention period required for the purposes for which the personal data are processed, personal data envisaged to be transferred to foreign countries, and measures taken for data security.
Processing of Personal Data	Any operation performed on personal data, whether by fully or partly automated means or by non-automated means as part of a data recording system, including collection, recording, storage, retention, alteration, reorganisation, disclosure, transfer, receipt, making available, classification, or blocking of use.
Sensitive Personal Data	Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
Policies and Procedures	The policies and procedures prepared by the Company to ensure compliance with the Law.
Supplier	Third parties, whether natural or legal persons, from whom the Company procures products and/or services.
Third Party	Third natural persons who are in a relationship with the parties defined above in order to ensure the security of commercial transactions

	between such parties and the Company, or to protect the rights and interests of such parties.
VERBİS	The Data Controllers Registry Information System maintained by the KVK Board, in which data controllers are required to register and declare information regarding their data processing activities.
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller.
Data Recording System	A recording system in which personal data is structured and processed according to specific criteria.
Data Controller	The natural or legal person who determines the purposes and means of processing personal data and establishes and manages the system (data recording system) in which data is systematically kept.
Visitor	Natural persons who have entered the Company's physical premises for various purposes or who visit its websites.

4. ROLES AND RESPONSIBILITIES

All departments and employees within the Company's organisation are responsible for complying with and ensuring compliance with this Policy.

A Personal Data Protection Committee ("KVK Committee") has been established within the Company, with the participation of members from relevant departments, for the purpose of monitoring and managing the actions required for compliance with the Law. The principal duties of the KVK Committee are set out below:

- To prepare fundamental policies relating to the protection and processing of personal data, to monitor relevant legislation on personal data protection and, where necessary, to prepare amendments to policies and submit them for senior management approval for entry into force;
- To identify the measures required to ensure compliance with the Law and related legislation, to decide on the manner in which policies relating to the protection and processing of personal data are to be implemented and audited, and to carry out the necessary division of duties and coordination within the Company;
- To raise awareness of personal data protection and processing within the Company and among the Company's business partners;
- To identify the risks that may arise in the Company's personal data processing activities, ensure that necessary measures are taken, and submit improvement proposals to senior management for approval;
- To conduct training and awareness activities regarding personal data protection and the implementation of policies;
- To ensure that data subjects are informed about personal data processing activities and their statutory rights, and to establish a mechanism to respond promptly to applications and to respond to such applications;
- To fulfil any other duties assigned by the Company's senior management regarding personal data protection;

- To coordinate relations with the KVK Board and the KVK Authority.

5. PROCESSING OF PERSONAL DATA

The Company bases its operations on the fundamental principles and rules set out in the Law regarding the processing of personal data and carries out all personal data processing activities in accordance with these principles.

The Company takes the necessary technical and administrative measures to ensure the lawful processing of personal data. Employees are informed that they may not disclose personal data they have learned to others in violation of the provisions of the Law, or use such data outside the scope of the processing purpose, and that this obligation continues after their departure, and the necessary undertakings are obtained from them accordingly.

The Company fulfils its obligation to inform data subjects in accordance with the Law when personal data is collected. In this context, through disclosure notices, information concerning the identity of the Data Controller, the purposes for which personal data is processed, to whom and for what purpose personal data may be transferred, the method and legal basis of collection, and data subjects' rights under the Law is presented in a clear and comprehensible manner.

5.1. General Principles Regarding the Processing of Personal Data

Principle of Compliance with Law and Rules of Good Faith: The Company carries out personal data processing activities in compliance with all legal regulations and the fundamental principle of good faith.

Principle of Accuracy and, Where Necessary, Being Up-to-Date: The Company takes the necessary administrative and technical measures to ensure that personal data is accurate and up-to-date.

Principle of Processing for Specified, Explicit and Legitimate Purposes: The Company processes personal data for legitimate purposes and clearly sets out the specified processing purposes in a manner that can be understood by data subjects.

Principle of Being Relevant, Limited and Proportionate to the Purposes for Which They Are Processed: The Company processes personal data in a manner that is relevant, limited and proportionate to the data processing purposes that have been specified explicitly and legitimately prior to the commencement of the processing activity. Personal data is not processed on the assumption that it may be required in the future if it is not directly related to the achievement of the purpose.

Principle of Retention for the Period Required by Relevant Legislation or for the Purpose for Which They Are Processed: The Company retains personal data for a period limited to that prescribed by relevant legislation or required for the purpose for which it is processed. In this regard, when determining the retention period for personal data, statutory periods under applicable legislation are primarily taken into account; if no period is prescribed by legislation, personal data is retained for the period required for the purpose for which it is processed. Upon expiry of the retention period determined for personal data and/or upon the cessation of the reasons requiring the processing of personal data, personal data is deleted, destroyed or anonymised in accordance with periodic disposal periods and/or upon the application of the relevant data subject.

5.2. Conditions for Processing Personal Data

Apart from cases where data subjects have provided explicit consent, personal data processing activities may be carried out within the scope of one or more of the processing conditions set out below. Accordingly, it is first assessed whether the personal data processing activity is based on any of the processing conditions other than explicit consent, and if none of the processing conditions listed below is present, the data processing activity is not continued without obtaining the data subject's explicit consent.

Existence of the explicit consent of the data subject:

Personal data may be processed by obtaining the explicit consent of the data subject; however, where any of the other processing conditions explained below exists, personal data may be processed without seeking the explicit consent of the data subject.

Explicitly provided for by law:

Where a legal provision expressly permits the processing of personal data, the data processing activity may be carried out within the scope of the relevant statutory provision.

- Where it is mandatory for the protection of the life or physical integrity of the person him/herself or of another person, where the person is unable to express his/her consent due to actual impossibility or where his/her consent is not legally valid:

Where it is mandatory to process personal data for the protection of the life or physical integrity of the person who is unable to express his/her consent due to actual impossibility or whose consent cannot be given legal validity, personal data may be processed without seeking the explicit consent of the data subject.

- Where processing of personal data belonging to the parties to a contract is necessary, provided that it is directly related to the conclusion or performance of a contract:

Within the scope of the Company's processes, where personal data belonging to the parties to a contract needs to be processed, provided that it is directly related to the conclusion or performance of a contract, the processing activity may be carried out.

- Where it is mandatory for the Company to fulfil its legal obligations:

Where processing is mandatory for the Company to fulfil its legal obligations, the data subject's personal data may be processed.

- Where the personal data has been made public by the data subject:

Where the data subject has made his/her personal data public, the personal data in question may be processed within the limits of the purpose of such disclosure.

- Where data processing is mandatory for the establishment, exercise or protection of a right:

Where it is mandatory to carry out the processing activity for the establishment, exercise or protection of a right, the data subject's personal data may be processed.

- Where data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject:

Where personal data processing is mandatory within the scope of the Company's legitimate interests, personal data may be processed provided that it does not harm the fundamental rights and freedoms of the data subject. In this context, the necessary assessments must be made to

strike a reasonable balance between the interests of the data controller and the fundamental rights and freedoms of the data subject.

The Company pays particular attention to the processing of sensitive personal data. In this context, the Company first carefully determines whether the conditions for processing are present before processing sensitive personal data, and only proceeds with the data processing activity after ensuring the existence of a legal basis.

5.3. Categories of Personal Data Processed

5.3.1. Categories of Personal Data

The categories of personal data processed, whether fully or partly by automated means or by non-automated means as part of a data recording system, identifying or identifiable to the natural person to whom they belong, and their descriptions within the scope of the data processing activities carried out by the Company, are set out below:

Identity:	Information contained in documents such as driving licences, national identity cards, residence permits, passports, bar identity cards, marriage certificates, including name and surname, Turkish identity number, national ID card series/number, passport number, nationality, mother's/father's name, place and date of birth, gender, signature, vehicle registration plate, etc.
Contact:	Information such as telephone number, address, e-mail address, registered electronic mail (KEP) address.
Personnel:	Information such as payroll records, disciplinary investigation records, employment entry/exit records, SSI number, CV information, performance appraisal reports.
Professional Experience:	Information such as diploma details, courses attended, vocational training information, certificates, transcript information.
Financial:	Information such as balance sheet details, current account information, financial performance data, credit and risk information, asset details, payroll records, salary, bonus, fringe benefits, premium payments, individual pension contributions, tax and insurance deductions.
Risk Management:	Information processed for the management of commercial, technical and administrative risks.
Marketing:	Information such as order history, survey data, cookie records, information obtained through campaign activities.
Customer Information:	Information obtained and generated from natural person customers as a result of our commercial activities and the operations of relevant units within those activities.
Physical Space Security:	Information such as entry/exit records of employees and visitors, CCTV footage.
Location:	Location data obtained through applications used by customers, during the use of Company vehicles, and via digital cards issued to visitors, employees and job applicants.

Legal Proceedings:	Information contained in correspondence with judicial and administrative authorities, information in litigation and enforcement files, legal requests, complaints, objections and mediation proceedings of data subjects.
Transaction Security:	Information such as IP address details, website login/logout records, passwords and passcodes.
Audio and Visual Records:	Information such as photographs, videos, and other visual and audio records.

5.3.2. Categories of Sensitive Personal Data

The categories of sensitive personal data processed, whether fully or partly by automated means or by non-automated means as part of a data recording system, identifying or identifiable to the natural person to whom they belong, and their descriptions within the scope of the data processing activities carried out by the Company, are set out below:

Health Data:	Data such as information on disability status, blood type, health reports, periodic medical examination reports.
Criminal Convictions and Security Measures:	Data such as information relating to criminal convictions and security measures.

5.4. Groups of Data Subjects Whose Personal Data is Processed

The groups of data subjects whose personal data is processed by the Company are set out below:

Employee	Job Applicant
Reference for Job Applicant	Intern
Employee's Relatives	Shareholder / Partner
Customer	Visitor
Supplier	Supplier Employee / Authorised Representative
Potential Customer Investor Student Prospective Business Partner Trade Fair Participant Subcontractor Employee Others: Persons in Dispute with the Company Parent / Guardian / Representative Public Authority Officials	Service Providers Dealer Candidate / Employee / Authorised Representative / Customer Authorised Service Candidate / Employee / Authorised Representative / Customer Board Member Proxy (Attorney, authorised person, etc.)

5.5. Purposes of Personal Data Processing

The Company carries out personal data processing activities for the following processing purposes:

- Conducting employee candidate / intern selection and placement processes
- Conducting job applicant application processes
- Fulfilling obligations arising from employment contracts and legislation for employees
- Conducting fringe benefits and perquisites processes for employees
- Conducting employee satisfaction and loyalty processes
- Conducting audit and ethics activities
- Conducting in-house and external training activities
- Managing access authorisations
- Ensuring that activities are carried out in compliance with legislation
- Conducting finance and accounting operations
- Management and/or supervision of relationships with subsidiaries
- Conducting corporate and partnership law transactions
- Conducting Company affiliation processes
- Ensuring physical space security
- Ensuring secondment processes
- Follow-up and management of legal affairs
- Conducting corporate relations and communication activities
- Planning human resources processes
- Conducting and auditing business activities
- Planning and executing in-house orientation activities
- Conducting occupational health and safety activities
- Receiving and evaluating proposals for improvement of business processes
- Conducting business continuity activities
- Conducting logistics activities
- Conducting procurement and sales processes for goods and services
- Organisation and event management
- Conducting performance appraisal processes
- Conducting risk management processes
- Conducting emergency management processes
- Conducting information security processes
- Establishing and managing IT infrastructure
- Conducting retention and archiving activities
- Conducting corporate social responsibility and civil society activities
- Conducting contract processes

- Planning and executing corporate governance activities
- Planning and executing corporate sustainability activities
- Conducting sponsorship activities
- Conducting strategic planning activities
- Follow-up of requests and complaints
- Conducting remuneration policy
- Conducting investment processes
- Conducting talent and career development activities
- Providing information to authorised persons, institutions and organisations
- Conducting management activities
- Creating and monitoring visitor records
- Ensuring the security of data controller operations

The Company carries out sensitive personal data processing activities for the following processing purposes:

- Conducting emergency management processes
- Fulfilling obligations arising from employment contracts and legislation for employees
- Conducting fringe benefits and perquisites processes for employees
- Conducting occupational health and safety activities
- Ensuring that activities are carried out in compliance with legislation
- Providing information to authorised persons, institutions and organisations
- Follow-up and management of legal affairs

The Company has separately and in detail regulated and published the "POLICY ON THE PROCESSING AND PROTECTION OF SENSITIVE PERSONAL DATA" regarding the process of processing sensitive personal data.

6. TRANSFER OF PERSONAL DATA

Within the scope of the personal data processing purposes determined by the Company, it may be necessary to transfer personal data to third parties. The transfer of personal data refers to the disclosure of data by transmitting it to a third party, making it accessible, or making it available for examination in any manner, and may be carried out by any written, verbal, visual or electronic means. In this context, the Company may transfer personal data to third parties in line with its processing purposes and by providing the necessary security measures.

In transfers of personal data to be carried out by the Company, the personal data transfer conditions regulated under Articles 8 and 9 of the Law are complied with. Provisions in other laws regarding the transfer of personal data are reserved.

6.1. Domestic Transfer of Personal Data

Where necessary for the achievement of processing purposes, personal data may be transferred to third parties in accordance with Article 8 of the Law, provided that the processing conditions are met and adequate safeguards are in place.

6.2. International Transfer of Personal Data

Where necessary for the achievement of processing purposes, personal data may be transferred to third parties in accordance with Article 9 of the Law, provided that the processing conditions are met, adequate safeguards are in place, and an adequacy decision has been issued by the KVK Board regarding the country, sectors within the country, or international organisations to which the transfer is to be made.

Where no adequacy decision has been issued by the KVK Board, personal data may be transferred to third parties by executing standard contractual clauses published by the KVK Board or by providing one of the other appropriate safeguards specified in Article 9 of the Law, provided that the processing conditions are met, adequate safeguards are in place, and the data subject has the possibility of exercising his/her rights and seeking effective legal remedies in the country to which the transfer is to be made.

6.3. Parties to Whom Personal Data is Transferred

The nature of personal data transfers and the parties with whom sharing is made vary depending on the type and nature of the relationship between the data subject, the data recipient and the Company, the purpose of the transfer and the relevant legal basis, and such parties are generally as follows:

Business Partners
Suppliers
Dealers
Authorised Service Providers
Service Providers
Shareholders
Subsidiaries and Affiliates
Legally Authorised Public Institutions and Organisations
Legally Authorised Private Law Persons
Lawyers / Law Firms / Consultants
Other third parties

Personal data processed by the Company may be transferred to AG Anadolu Grubu Holding A.Ş., the holding company to which it is affiliated, for the purposes of compliance with group principles and strategies and the protection of the rights and reputation of the companies, and may also be processed by AG Anadolu Grubu Holding A.Ş.

7. RIGHTS AND OBLIGATIONS REGARDING PERSONAL DATA

7.1. Informing Data Subjects

The Company is obliged to inform data subjects when personal data is collected, pursuant to Article 10 of the Law.

In this context, when collecting personal data, the Company notifies data owners, in compliance with the Communiqué on the Procedures and Principles to be Complied with in

Fulfilling the Obligation of Disclosure, of who will process the personal data, the purposes for which their personal data will be processed, to whom and for what purpose the processed personal data may be transferred, the method and legal basis of personal data collection, and the rights of the data subject under Article 11 of the Law, and obtains explicit consent where necessary. When the purpose of personal data processing changes, the obligation to inform data subjects for such new purpose is separately fulfilled prior to the data processing activity.

7.2. Rights of Data Subjects

Data subjects have the following rights pursuant to Article 11 of the Law:

- To learn whether personal data has been processed.
- To request information if personal data has been processed.
- To learn the purposes of processing personal data and whether it is being used in accordance with those purposes.
- To know the third parties to whom personal data has been transferred, domestically or abroad.
- To request correction of personal data if it has been processed incompletely or inaccurately.
- To request deletion or destruction of personal data within the scope of Article 7 of the Law, in cases where the reasons requiring processing have ceased to exist although it has been processed in accordance with the Law and other applicable legislation, and to request that the transaction carried out in this context be notified to third parties to whom personal data has been transferred.
- To request that corrections and deletions be notified to third parties to whom personal data has been transferred.
- To object to the emergence of a result against the person him/herself by means of analysis of processed data exclusively through automated systems.
- To learn which personal data is retained by the Company.
- To request compensation for damages in the event of damage arising from the unlawful processing of personal data.

Where the circumstances specified in Article 28(1) of the Law are present, it is stipulated that the provisions of the Law shall not apply, and accordingly, it is not possible for data subjects to assert the rights enumerated in the Law in respect of personal data processed by the Company.

In the cases specified in Article 28(2) of the Law, data subjects may not assert the other rights enumerated in the Law, with the exception of the right to demand compensation for damages.

7.3. Conclusion of Data Subject Requests

Where data subjects submit their requests relating to their personal data in writing to the Company or via registered electronic mail (KEP) address, secure electronic signature or mobile signature, together with documents verifying their identity and the application form at <https://anadoluisuzu.com.tr/img/basvuru-formu.pdf> completed in accordance with the instructions, the Company will carry out the necessary processes to conclude the request in accordance with Article 13 of the Law, as soon as possible and within a maximum of thirty (30) days, depending on the nature of the request.

Within the scope of ensuring data security, the Company may request information to verify whether the data subject submitting the application is the owner of the personal data subject to the application. The Company may also direct questions to the data subject regarding the application in order to ensure that the data subject's application is concluded in the manner appropriate to the request.

The Company is also not under any obligation to respond in cases where the data subject has not provided contact information or verification cannot be made; the application form has not been completed fully and correctly as specified; information has been provided incompletely; or the application has not been submitted through the channels or in the manner specified in the instructions at <https://anadoluisuzu.com.tr/img/basvuru-formu.pdf>. In cases where the contact address provided by the data subject cannot be reached, it shall be deemed that a response has been given to the data subject regarding their application.

The Company may reject the request, with a stated justification, in cases where the data subject's application may impede the rights and freedoms of other persons, requires disproportionate effort, or the information is publicly available.

7.4. Protection and Security of Personal Data

The Company attaches great importance to protecting the confidentiality, integrity and security of personal data and, accordingly, takes the necessary technical and administrative security measures to protect personal data processed and stored in all environments against risks such as unauthorised access, damage, loss, alteration or disclosure.

The Company continuously updates and improves its data security processes, taking into account technological developments, data security risks and legal obligations. Accordingly, technical and administrative security measures for the protection of personal data are implemented using the most up-to-date and effective methods. Within the scope of the personal data processing activity carried out by the Company, in cases where personal data is determined to have been unlawfully obtained by unauthorised persons, the situation will be reported to the KVK Board and the relevant data subjects within 72 hours. In such cases, the necessary administrative and technical measures will be ensured in accordance with the guidelines set out in the Data Breach Management Policy.

Examples of principal administrative and technical measures applied are set out below; details of the measures taken within the scope of the protection and security of personal data are explained in the Personal Data Retention and Disposal Policy and Information Security Policy.

7.4.1. Administrative Measures

- The Company trains its employees on personal data protection law and ensures their awareness is raised.
- In cases where personal data is subject to transfer, the Company ensures that the contracts concluded with the parties to whom personal data is transferred contain provisions to the effect that such parties will fulfil their obligations to ensure data security.
- The personal data processing activities carried out by the Company are examined in detail and periodically reviewed and updated as necessary. Within this scope, the steps to be taken to ensure compliance with the personal data processing conditions stipulated in the Law are identified.

- The Company identifies the practices to be fulfilled to ensure compliance with the Law, regulates these practices through internal policies, and periodically reviews and updates them as necessary.

7.4.2. Technical Measures

- With regard to the protection of personal data, the Company takes technical measures to the extent permitted by technology and within reasonable limits, and the measures taken are updated and improved in parallel with developments.
- Expert personnel are employed or specialist consultants are engaged, where necessary, in technical matters.
- Regular audits are conducted to monitor the implementation of the measures taken.
- Software and systems designed to ensure security are established.
- Access to personal data being processed within the Company is restricted to the relevant employees in accordance with the determined processing purpose.

7.4.3. Audit Activities

The Company audits the compliance of personal data processing activities with applicable legislation and the functioning of the technical and administrative measures taken within the scope of ensuring the protection and security of personal data, and carries out practices to ensure continuity of operation. Personal data processing processes are updated in line with the audit results, and activities are conducted to develop and improve the measures taken for the protection of data.

8. USE OF CLOSED-CIRCUIT TELEVISION (CCTV)

Visual and audio data may be collected by the Company through a closed-circuit camera system throughout its business premises, including its registered office building, regional offices, production facilities, warehouses and distribution areas, for purposes such as ensuring physical space security, ensuring the safety of the building interior and surroundings, vehicles and equipment, visitors and employees, and preventing conduct constituting a criminal offence, and such data may be retained only for the period required for these stated purposes. All necessary technical and administrative measures will be taken by the Company to ensure the security of personal data obtained through the closed-circuit camera system.

9. USE OF WEBSITES

On websites owned and managed by the Company, visitors' internet activities within the site are recorded by technical means (e.g. cookies) in order to enable persons visiting the sites to conduct their visits appropriately, to provide personalised content, to offer social media features, to facilitate repeat visits by remembering visitors upon their return, and to carry out online advertising activities.

The Company may stop using cookies on the websites it owns and manages, change their types or functions, or add new cookies.

The Company will process personal data obtained through such cookies in accordance with the Law and the terms and conditions of this Policy.

Detailed explanations regarding the protection and processing of personal data in respect of the relevant websites are included in the "Privacy Policy" and "Cookie Policy" texts of the respective websites.

10. FINAL PROVISIONS

This Policy will be reviewed by the KVK Committee at least once a year and updated where necessary. The KVK Committee is authorised and responsible for the entry into force, amendment, implementation and revocation of this Policy.

In the event of any conflict between any section of this Policy and applicable legislation, the provisions of applicable legislation shall prevail over that specific section of the Policy.

This Policy was prepared and approved by the KVK Committee and was last updated on 29/12/2025. In the event that this Policy is translated into a language other than Turkish, the Turkish text shall always prevail in any differing expressions between the two texts. This Policy may not be reproduced, copied or distributed without the written permission of Anadolu Isuzu Otomotiv Sanayii ve Ticaret A.Ş.

In cases where there is a conflict between the Turkish version which is the original language of the text and any translation of the policy, the Turkish text shall prevail.