

POLICY ON THE PROTECTION AND PROCESSING OF SENSITIVE PERSONAL DATA

1. PURPOSE

The purpose of this Policy on the Protection and Processing of Sensitive Personal Data ("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"), related legislation, the resolution of the Personal Data Protection Board dated 31/01/2018 and numbered 2018/10 regarding "Adequate Measures to be Taken by Data Controllers in the Processing of Sensitive Personal Data" and other relevant resolutions, to which it is subject when processing sensitive personal data, to ensure transparency in sensitive personal data processing activities, to take the necessary technical and administrative measures and to ensure that the Company fulfils its obligations regarding sensitive personal data 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 sensitive personal data in compliance with the principles of lawfulness, fairness and transparency.

2. SCOPE AND APPLICATION

This Policy covers all processes within the scope of the Company's activities in which sensitive 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 sensitive personal data. In the event of any inconsistency between this Policy, prepared on the basis of applicable legislation regarding the processing and protection of sensitive personal data, and the applicable legislation, the applicable legislation shall prevail.

This Policy sets out which data constitutes sensitive personal data, which sensitive personal data is retained, the administrative and technical measures taken for the protection of sensitive personal data, and explanations regarding the processing, retention, disclosure and informing of data subjects, transfer to third parties, and protection of sensitive 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 sensitive 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.
Data Subject	The natural person whose personal data is processed.
KVK Committee	The Personal Data Protection Committee 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.
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.
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.
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.
Registered Electronic Mail (KEP) Address	A qualified form of electronic mail that provides legal evidence regarding the use of electronic messages, including their transmission and delivery.

4. ROLES AND RESPONSIBILITIES

All departments and employees within the Company's organisation are responsible for complying with and ensuring compliance with this Policy; the Company's KVK Committee is responsible for the preparation, updating and implementation of this Policy.

5. PROCESSING OF SENSITIVE PERSONAL DATA

Pursuant to the Law, sensitive personal data are defined as data relating to individuals' 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.

The Company bases its operations on the fundamental principles and rules set out in the Law regarding the processing of sensitive personal data and carries out all sensitive personal data processing activities in accordance with these principles. The Company takes the necessary technical and administrative measures to ensure the lawful processing of sensitive personal data.

Sensitive personal data processed by the Company are tracked through the Personal Data Inventory, with periodic reviews and updates carried out under the responsibility of all departments across the organisation, and the Personal Data Inventory is kept up-to-date in accordance with the relevant business processes.

The Company may transfer sensitive personal data to third parties, taking the necessary security measures, for lawful sensitive personal data processing purposes. In this regard, the Company acts in compliance with the provisions set out in Articles 8 and 9 of the Law.

5.1. General Principles Regarding the Processing of Sensitive Personal Data

- Sensitive personal data are processed in accordance with the principles of (i) compliance with law and rules of good faith, (ii) accuracy and, where necessary, being up-to-date, (iii) processing for specified, explicit and legitimate purposes, (iv) being relevant, limited and proportionate to the purposes for which they are processed, and (v) retention for the period required by relevant legislation or for the purpose for which they are processed.
- Within the scope of compliance with law and rules of good faith, the processing of sensitive personal data is based on a legitimate legal basis; it is not carried out in an arbitrary or unjust manner that would result in adverse consequences for the data subject; and data subjects are adequately informed.
- Within the scope of the Company's processes, sensitive personal data are only processed for a specified, explicit and legitimate purpose. The processing of sensitive personal data is relevant, limited and proportionate to the purposes determined within

those processes. In cases not related to achieving the purposes determined within the processes and where processing is not mandatory, unnecessary data processing activities are avoided.

- Processed sensitive personal data must be kept accurate and up-to-date and it is essential that they are retained for the period required by relevant legislation or for the purpose for which they are processed. In this context, where a period has been determined by relevant legislation for the retention of sensitive personal data, such period is complied with; where no period has been determined by legislation, the data is retained for the period required for the purpose for which it is processed. Upon expiry of the statutory or processing-purpose retention period, the data is deleted, destroyed or anonymised within the framework of the Company's Personal Data Retention and Disposal Policy.

5.2. Conditions for Processing Sensitive Personal Data

As explicitly stated in Article 6 of the Law, it is possible to process sensitive personal data in expressly stipulated exceptional circumstances.

The processing of sensitive personal data by the Company is carried out only in the following circumstances and in compliance with the conditions set out in the Law, including the condition that adequate safeguards determined by the KVK Board are in place:

- Existence of the explicit consent of the data subject
- Explicitly provided for by law
- 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 personal data has been made public by the data subject and is in accordance with his/her intention to make it public
- Where data processing is mandatory for the establishment, exercise or protection of a right
- Where necessary by persons under an obligation of confidentiality or by authorised institutions and organisations for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and care services and planning, management and financing of health services
- Where mandatory for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance
- With respect to foundations, associations and other non-profit organisations or entities established for political, philosophical, religious or trade union purposes, provided that they act in accordance with applicable legislation and their purposes, remain limited to their fields of activity and are not disclosed to third parties; only in relation to current or former members and affiliates of such organisations or entities or persons who are in regular contact with such organisations or entities

5.3. Informing Data Subjects When Collecting Sensitive Personal Data

Pursuant to Article 10 of the Law, data controllers or persons authorised by them are required to inform data subjects when personal data, including but not limited to sensitive personal data, is collected. In this context, when fulfilling its obligation to inform data subjects, the Company provides information on at least the following matters:

- The identity of the data controller and its representative, if any
- The purposes for which the 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
- The rights granted to data subjects under Article 11 of the Law and how such rights may be exercised

Except in cases where alternative methods and approaches are adopted, disclosure notices presented to data subjects in physical or electronic form in a provable manner are used by the Company to fulfil the obligation to inform. Company employees involved in processes where sensitive personal data are processed must ensure that the required disclosure notices are provided to data subjects and that data subjects are informed prior to the collection of personal data.

5.4. Purposes of Processing Sensitive Personal Data

The Company processes sensitive personal data in accordance with the general principles set out in Article 4 of the Law and specified above, in a manner based on and limited to at least one of the data processing conditions specified in Article 6 of the Law. The Company informs each relevant group of data subjects separately in the relevant disclosure notices regarding data processing categories and purposes, pursuant to Article 10 of the Law and secondary legislation.

The data processing purposes associated with personal data categories have been declared in the Data Controllers Registry Information System (VERBİS) and the system is kept accessible to the public and all data subjects at verbis.kvkk.gov.tr.

6. RETENTION AND DISPOSAL OF SENSITIVE PERSONAL DATA

Pursuant to the obligation to delete, destroy or anonymise personal data as regulated under Article 7 of the Law, all personal data, including sensitive personal data, that has been processed in compliance with the Law and other applicable legislation but whose reasons for processing have ceased to exist, is deleted, destroyed or anonymised by the Company upon its own decision or upon the request of the relevant data subject.

Detailed information regarding the retention and disposal of personal data is set out in the Company's Personal Data Retention and Disposal Policy.

7. ENSURING THE SECURITY AND CONFIDENTIALITY OF SENSITIVE PERSONAL DATA

All necessary measures are taken by the Company, to the extent possible and in accordance with the nature of the data to be protected, in order to prevent the unlawful disclosure, access, transfer or other security deficiencies that may occur with regard to sensitive personal data.

In this context, all necessary administrative and technical measures are taken by the Company; such measures are reviewed and updated in compliance with the current resolutions of the KVK Board; and in the event of unlawful disclosure of personal data, action is taken in accordance with the measures stipulated under the Law.

The data security measures set out in this section are the minimum measures to be taken by the Company in the processing of sensitive personal data. These measures have been determined in compliance with the KVK Board's Resolution dated 31/01/2018 and numbered 2018/10 on

"Adequate Measures to be Taken by Data Controllers in the Processing of Sensitive Personal Data" and will be updated in the event of new resolutions published by the KVK Board on this matter.

Standard technical and administrative data security measures already implemented by the Company in its other processes will continue to be applied to the extent appropriate for processes involving the processing of sensitive personal data.

8. ADMINISTRATIVE AND TECHNICAL MEASURES IN THE PROCESSING OF SENSITIVE PERSONAL DATA

Technical and administrative measures aimed at ensuring an appropriate level of security as set out in the Personal Data Security Guide published on the KVK Authority's website are taken by the Company in the processing of sensitive personal data. While audits on technical measures are carried out by the department responsible for information security within the Company, it is essential that these measures are implemented by the relevant business unit processing the data, and that requests are made to the department responsible for information security where necessary.

In the event that sensitive personal data are unlawfully obtained by unauthorised persons within the scope of the sensitive personal data processing activities carried out by the Company, the situation will be reported to the KVK Board within at most 72 (seventy-two) hours in compliance with the KVK Board's resolution dated 24.01.2019 and numbered 2019/10, and the relevant data subjects affected by the breach will be notified as soon as possible.

In addition, the following additional technical and administrative measures determined by the KVK Board are also taken:

For employees involved in sensitive personal data processing processes:

- Regular training is provided on sensitive personal data security.
- Confidentiality clauses are executed within the scope of employment contracts and disciplinary procedures to be applied in the event of a breach are established.
- The scope of access authorisations and their duration for users with access to data are clearly defined.
- Periodic access reviews are conducted.
- The authorisations of employees who change roles or leave employment in this area are immediately revoked and the inventory allocated to them is retrieved.

Where the environment in which sensitive personal data are processed, retained and/or accessed is an electronic environment:

- Data is retained using cryptographic methods.
- Cryptographic keys are kept in secure and separate environments.
- Transaction logs of all operations carried out on data are securely logged.
- Security updates for the environments where the data is located are continuously monitored, necessary security tests are conducted regularly and test results are recorded.
- Where data is accessed through software, user authorisations for the relevant software are performed, security tests for such software are conducted regularly and test results are recorded.

- Where remote access to data is required, a minimum two-factor authentication system is provided.

Where the environment in which sensitive personal data are processed, retained and/or accessed is a physical environment:

- It is ensured that adequate security measures (against situations such as electrical leakage, fire, flood, theft, etc.) are in place depending on the nature of the environment in which the sensitive personal data are located.
- Physical security of the relevant physical environments is ensured and unauthorised access is prevented.

In cases where sensitive personal data are transferred:

- Where data needs to be transferred via e-mail, it is transferred in encrypted form using a corporate e-mail address or a Registered Electronic Mail (KEP) account.
- Where transfer via portable memory devices, CDs, DVDs or similar media is required, the data is encrypted using cryptographic methods and the cryptographic key is kept in a separate environment.
- Where transfer is carried out between servers in different physical environments, data transfer is performed by establishing a VPN between the servers or using the sFTP method. This ensures network security and reduces cyber risks during transfer.
- Where transfer of data via paper is required, the necessary measures are taken against risks such as theft, loss or viewing by unauthorised persons and the document is sent in "confidential document" format.

9. RELATED DOCUMENTS

This Policy should be read in conjunction with all other Policies and Procedures in force within the Company, including in particular the following policies and procedures relating to the protection and processing of personal data:

- Anadolu Group IT Standards Guide
- Personal Data Protection and Processing Policy
- Personal Data Retention and Disposal Policy

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.