



Koluman Otomotiv Endüstri Anonim Şirketi

Personal Data Protection and Processing Policy

Prepared by:

Koluman Otomotiv Endüstri Anonim Şirketi

Address:

Şahin Mh. Sait Polat Blv. No:386 / C Blok P.K.33800 Tarsus/Mersin/Türkiye

Phone: +90 324 651 00 20 **WEB:** www.kolumanotomotiv.com

All rights reserved.

A. INTRODUCTION

1. Purpose

This "Kulman Automotive Industry Joint Stock Company" ("Company") Personal Data Processing and Protection Policy ("Policy") regulates the principles and guidelines adopted by our Company, which operates in the fields of motor vehicles, construction and engineering, infrastructure production, marketing and foreign trade, for the processing and protection of personal data regulated and protected under the Law No. 6698 on the Protection of Personal Data ("Law"). The Policy ensures compliance with the legal framework for the processing and protection of personal data.

2. Scope

This Policy covers all personal data processed by our Company, whether through automatic means or as part of any data recording system, of our customers, suppliers, their employees, our employees, job candidates, shareholders, representatives, visitors, and third parties.

Furthermore, the principles and guidelines adopted under this Policy apply to all employees, job candidates, employees of our Company's affiliated companies, and their representatives who process personal data, have access to personal data, provide personal data to the Company, or receive data from the Company.

3. Definitions

The terms used in this Policy refer to the meanings defined in Article 3 titled 'Definitions' of the Law.

B. PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA

Our Company adheres to the following principles, which are defined and adopted in compliance with the Constitution's Article 20 and the Law, as well as other relevant legislation, in the processing of personal data.

1. Fundamental Principles for the Processing of Personal Data

In processing personal data, our Company complies with the following principles in accordance with Article 4 of the Law:

- Compliance with the law and the principle of integrity,
- Ensuring that personal data is accurate and, where necessary, kept up to date,
- Processing personal data for specified, legitimate, and lawful purposes,
- Processing personal data in a way that is adequate, relevant, and limited to what is necessary for the purpose of processing,
- Retaining personal data for the period required by relevant legislation or the purpose for which it was processed.

In this context, our Company determines that, but is not limited to, the purposes and the duration of data processing before the processing of personal data begins. The Company does not perform processing activities based on potential future circumstances. Additionally, the Company carries out data minimization efforts, determines the retention periods for personal data according to the legislation, or if there is no legal retention period, sets the maximum duration based on the purpose of processing. After the expiration of these periods, personal data is deleted, destroyed, or anonymized. Furthermore, in order to ensure that these fundamental principles are effectively implemented, the Company monitors current technologies and conducts periodic checks for necessary updates.

2. Conditions for Processing Personal Data

According to the 3rd paragraph of Article 20 of the Constitution: "Personal data can only be processed in cases explicitly foreseen by law or with the explicit consent of the individual."

The conditions for processing personal data by our Company, in accordance with the relevant provision of the Constitution, are (i) the explicit consent of the data owner or (ii) the processing of personal data as regulated by the Law.

The conditions for processing personal data are regulated in Article 5 of the Law. In paragraph 1 of Article 5, the condition of explicit consent is reiterated; in paragraph 2, the other conditions are listed in seven subparagraphs. Personal data may be processed in accordance with one or more of these conditions.

2.1. Explicit Consent of the Data owner

The explicit consent of the data owner is one of the conditions for processing personal data, as outlined in the above-mentioned provision of the Constitution and paragraph 1 of Article 5 of the Law.

Our Company processes personal data only when the explicit consent of the data owner is obtained and in a manner that is connected to and proportional to the purpose and scope of the consent.

2.2. Explicit Provision in Laws

In cases explicitly foreseen by law, personal data may be processed without the explicit consent of the data owner.

For example, in accordance with Article 5 of the Regulation on the Measures Regarding the Prevention of Money Laundering and Financing of Terrorism.

2.3. Impossibility of Obtaining Explicit Consent Due to Physical Impossibility

If the data owner is unable to express their consent due to physical impossibility or if the individual's consent is not legally valid, personal data may be processed without the explicit

consent of the data owner in cases where it is necessary for the protection of the life or bodily integrity of the individual or another person.

For example, if a visitor to our Company suffers from a health issue and needs to be taken to the medical center, their contact details may be recorded.

2.4. Necessity for the Establishment or Performance of a Contract

Personal data may be processed without the explicit consent of the data owner if it is necessary for the establishment or fulfilment of a contract, provided it directly relates to the parties involved in the contract.

For example, if an individual places an order for infrastructure from our Company, the contract is formed, and their information and signature related to the contract are collected.

2.5. Necessity for Fulfillment of Legal Obligation

Personal data may be processed without the explicit consent of the data owner when necessary for the fulfillment of legal obligations of our Company.

For example, responding to inquiries from judicial authorities like courts or prosecutors, or providing requested documents.

2.6. Personal Data Made Public by the Data owner

If the data owner has made their personal data public, such data may be processed without the explicit consent of the data owner.

For example, contacting an individual who has applied for a job with our Company.

2.7. Necessity for the Establishment or Protection of a Right

If the processing of personal data is necessary for the establishment, exercise, or protection of a right, personal data may be processed without the explicit consent of the data owner.

For example, obtaining information from individuals who have applied via our website in order to respond to their questions.

2.8. Necessity for the Legitimate Interest of the Company

Personal data may be processed without the explicit consent of the data owner when it is necessary for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the individual.

For example, maintaining visitor logs and taking video recordings for security purposes.

C. PRINCIPLES REGARDING THE PROTECTION OF PERSONAL DATA

The fundamental principles related to the protection of personal data are regulated in Article 12 of the Law.

Our Company adheres to the following principles, as defined by the relevant legislation, including this article, in the protection of personal data.

1. Data Security

Our Company takes technical, administrative, and physical measures regarding data security to prevent the unlawful processing of personal data, unlawful access to personal data, and to ensure the protection of personal data.

1.1. Technical Measures for Data Security

- As part of the Information Security Management System, activities are carried out systematically, with established rules, planned, manageable, sustainable, documented, approved by management, and based on international security standards to ensure the confidentiality, integrity, and continuous availability (accessibility) of information.
- For cybersecurity, measures are taken including, but not limited to, firewall and gateway protections; preventing employees from accessing threatening websites or online services; deleting unused software and services from computers; ensuring that software and hardware are up to date with the latest security patches.
- To track personal data security, measures are taken such as monitoring which software and services are operating on IT networks, determining if there is any unauthorized or unusual activity within the networks, and keeping logs of all user activities.
- To ensure the security of environments containing personal data, precautions are taken to prevent risks such as the theft, loss, or damage of devices or paper records containing personal data. Measures are implemented to prevent these risks, and, if they occur, to minimize any potential damage.
- When personal data is stored in the cloud, the security measures of the relevant cloud storage systems and providers are reviewed. Personal data to be uploaded to the cloud is encrypted using cryptographic methods, the cloud environment is encrypted, and the access to the cloud data storage by specific persons, locations, and internet networks is restricted and monitored.
- Within the procurement, development, and maintenance of information technology systems, control mechanisms are built into applications to ensure accurate data entry and prevent data corruption during processing. Measures are taken to prevent errors that may lead to data loss, and in case of hardware failures, actions are taken to prevent or manage the risk of sending data-storing parts to third-party companies.

1.2. Administrative Measures for Data Security

Our Company provides awareness training to its employees regarding the protection of personal data. Employees are informed that they cannot disclose personal data to third parties in violation of the Personal Data Protection Law (PDPL) or use it for purposes other than the processing purpose. Employees are also made aware that these obligations will continue even after they leave their position, and necessary commitments are obtained from them.

By following any changes in the legislation, necessary updates are made, special clauses for the protection of data owners' data are added to contracts when personal data is transferred, periodic audits are conducted to identify risks, efforts are made to minimize the amount of personal data stored, and other administrative measures are taken.

1.3. Physical Measures for Data Security

Our Company takes security measures in its facilities and buildings to protect personal data. Authorized access is granted to places where personal data is kept, such as cabinets, drawers, and archives, and security measures are taken to protect electronic devices containing personal data.

1.4. Measures to Be Taken in Case Personal Data Is Acquired by Unlawful Means

In case personal data is obtained by unlawful means, our Company, as the data controller, will report this situation to the concerned individual and the Personal Data Protection Authority (the Authority) as soon as possible. As a rule, our Company aims to notify the Authority within 72 hours of detecting such a breach.

2. Database Systems

Our Company establishes and manages database systems that allow analysis of through which channels and by what methods data is collected, how long it is retained, with whom it is shared, and how an individual's data is processed in the records based on this analysis. These systems also enable the execution of deletion, destruction, and anonymization activities.

Generally, this data recording system serves the following purposes:

- A database system that shows and controls which data is kept by which departments, for what purposes, and for how long,
- Enabling the data controller to analyze the data in its possession and operate the deletion process for unnecessary data,
- Managing the processes of deleting, destroying, or anonymizing data,
- Responding to data owner information requests (i.e., answering questions such as how a person's data is stored in the controller's records, from which sources it was collected, who can access it, with whom it is shared, how long it is retained, whether the data owner was provided with an information notice, and whether consent was obtained),
- Responding to requests from data owners regarding deletion, destruction, anonymization of their data, and prohibition of sharing with third parties.

3. Processes for Deletion, Destruction, and Anonymization of Data

Regarding the processes of deleting, destroying, and anonymizing personal data:

- Identifying unnecessary or unlawfully retained data in our Company's records, determining who can access these data and through which channels, and closing these channels,
- If services are provided by third-party providers such as cloud storage providers, verifying whether these providers have the technical capability to restore data after deletion,
- Ensuring that data stored on portable data recording devices is encrypted and can be deleted,
- Destruction involves more than just deleting from records; storage media must also be rendered unrecoverable through demagnetization, physical deformation, overwriting, or similar methods,
- Anonymization involves removing or altering all direct and/or indirect identifiers to prevent association with the relevant individual.

4. Collection and Management of Data owner Applications and Requests

The Law grants data owners the right to apply to the data controller, and requires the controller to respond within 30 days and conclude the requests.

Accordingly, data owners whose personal data are processed by our Company have the rights, under Article 11 of the Law, to apply to our Company to:

- Learn whether their personal data is processed,
- Request information if their personal data has been processed,
- Learn the purpose of processing and whether their data is used appropriately,
- Know third parties domestically or abroad to whom their data has been transferred,
- Request correction of incomplete or inaccurate data, and demand that the correction be notified to third parties to whom data has been transferred,
- Request deletion or destruction of personal data under conditions stated in Article 7 of the Law (e.g., when the reasons requiring processing no longer exist despite lawful processing) and request that the deletion be notified to third parties,
- Object to outcomes arising solely from automatic processing of data,
- Request compensation if damaged due to unlawful processing of personal data.

Exceptions stipulated in Article 28 of the Law are reserved.

Data owners can submit their requests by filling out the “Application Form” available at <https://www.kulamanotomotiv.com/en/corporate> and using the methods specified in the form.

Requests are processed free of charge as soon as possible and no later than thirty (30) days, except in cases where additional costs are required, in which case a fee determined by the Personal Data Protection Board is charged.

D. PRINCIPLES REGARDING THE PROCESSING AND PROTECTION OF SPECIAL CATEGORY PERSONAL DATA

Article 6 of the Law regulates special category personal data as data related to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and appearance, membership in associations, foundations or unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

The unlawful processing of special category personal data may cause more serious harm or discrimination to individuals. Our Company, aware of this, exercises the highest level of care in the processing and protection of these types of data in accordance with the special importance attributed by the Law.

1. Principles Regarding the Processing of Special Category Personal Data

Our Company processes special category personal data under the following conditions:

- If there is explicit consent from the data owner,
- If explicitly stipulated by laws,
- If the person is unable to give consent due to factual impossibility or the consent is not legally valid, and processing is mandatory to protect the life or physical integrity of the data owner or another person,
- If the data is related to personal data made public by the data owner and processing is consistent with the disclosure intention,
- If required for the establishment, exercise or enforcement of a right,
- If necessary for public health protection, preventive medicine, medical diagnosis, treatment and care services, and planning, management and financing of health services by persons under confidentiality obligations or authorized institutions and organizations,
- If necessary for the fulfillment of legal obligations in employment, occupational health and safety, social security, social services and social assistance,
- If related to associations, foundations, and other non-profit organizations established for political, philosophical, religious or union purposes, provided that processing is in accordance with applicable legislation and purposes, limited to their fields of activity, not disclosed to third parties, and concerns current or former members or persons regularly in contact with these organizations.

2. Principles Regarding the Protection of Special Category Personal Data

Even if the processing conditions explained above are met, adequate measures determined by the Board must also be taken in the processing of special category personal data.

For employees involved in the processing of special category personal data, regular training is provided, confidentiality agreements are signed, the scope and duration of access rights of authorized users are clearly defined, periodic access controls are carried out, and when

employees change roles or leave, their access rights are immediately revoked and allocated inventory is returned.

In terms of electronic environments where special category personal data is processed, stored and/or accessed, the following measures are taken:

- Data is secured by cryptographic methods,
- Cryptographic keys are stored securely and separately,
- All operations on the data are securely logged,
- Security updates for these environments are continuously monitored,
- Regular security testing is performed and recorded,
- User authorization is managed for software accessing the data,
- Software undergoes regular security testing and results are recorded,
- If remote access is needed, at least two-factor authentication is ensured.

For physical environments where special category personal data is processed, stored, and/or accessed, adequate security measures are taken against risks such as power failures, fire, flooding, theft, etc., and unauthorized access is prevented.

During the transfer of special category personal data:

- If transfer is via email, it is encrypted and sent through corporate email or Registered Electronic Mail (KEP),
- If transfer is via portable media such as USB drives, CDs, DVDs, it is encrypted with cryptographic methods and cryptographic keys are stored separately,
- If transfer occurs between servers in different physical locations, it is done through VPN or sFTP,
- If transfer is via paper documents, necessary precautions are taken against risks like theft, loss or unauthorized viewing, and documents are sent as “confidential documents.”

E. INFORMING THE PERSONAL DATA OWNER AND OBTAINING CONSENT WHEN NECESSARY

According to Article 20 of the Constitution, everyone has the right to be informed about personal data concerning them. Article 11 of the Law also imposes an obligation on data controllers to inform data owners. This obligation must be fulfilled at the time the personal data is obtained or, if the data is not collected directly from the data owner, within a reasonable time and in any case no later than the first communication.

In this context, our Company, within the legally prescribed period and in accordance with the Law, informs personal data owners about the following, in its capacity as data controller:

- The identity of our Company as the data controller,
- The purpose for which personal data will be processed,
- To whom and for what purposes the processed personal data may be transferred,
- The method and legal basis for collecting personal data,
- And the rights of the personal data owner.

Furthermore, in cases where the processing of personal data requires the explicit consent of the data owner, comprehensive information is provided to ensure that their consent is given for a specific purpose and based on free will.

F. TRANSFER OF PERSONAL DATA

According to the definitions section of the Law, the transfer of personal data is also considered as an "activity of personal data processing." Therefore, the explanations provided under Sections B and C above are valid when transferring personal data. On the other hand, the provisions of Articles 8 and 9 of the Law are strictly followed during the transfer of data. In this context, our Company transfers data to third parties (affiliated companies, business partners, employees, contractors or suppliers, public institutions) in accordance with the purpose of data processing and after taking the necessary security measures.

Article 8, Paragraph 3 of the Law specifies exceptions for data transfer situations in accordance with the provisions of other laws.

Transfer of Personal Data Abroad

Our Company transfers personal data abroad when necessary and in compliance with the conditions of the Law, ensuring the transfer is in line with the purpose of processing and appropriate security measures are taken. The Company conducts transfers abroad under the following conditions:

- If one of the conditions specified in Articles 5 and 6 of the Law is met, and there is an adequacy decision regarding the country, sectors within the country, or international organizations to which the data will be transferred,
- If there is no adequacy decision, the transfer is conducted if one of the conditions mentioned in Articles 5 and 6 is met and if the data owner has the ability to exercise their rights and access effective legal remedies in the country to which the transfer is made. In this case, the parties must ensure the provisions of Article 9, Paragraph 4 of the Law are met.

If there is no adequacy decision and none of the safeguards specified in Paragraph 4 are provided, data may be transferred if one of the situations described in Paragraph 6 is applicable. Personal data may also be transferred abroad, with the permission of the Personal Data Protection Authority (DPA), in situations where there is a serious risk to Turkey's or the data owner's interests, and if the relevant institution or organization's opinion is taken into consideration.

G. MANAGEMENT OF PROCESSES RELATED TO THE PROTECTION AND PROCESSING OF PERSONAL DATA

Our Company follows the fundamental processes below to manage the processes of personal data protection and processing and to fulfill all other requirements of the Law:

- Preparing and implementing the fundamental policies and amendments regarding the protection and processing of personal data,

- Deciding how the policies will be applied and monitored, and assigning responsibilities within the Company,
- Increasing awareness within the Company regarding the protection and processing of personal data, designing and ensuring the implementation of training programs,
- Identifying risks and ensuring that necessary precautions are taken,
- Tracking and resolving data owner requests,
- Managing communication with the Personal Data Protection Authority (DPA) and the necessary notification processes.

H. IMPLEMENTATION AND EFFECTIVENESS

The matters regulated in this Policy are subject to the Law and secondary regulations. In case of a conflict between the provisions of this Policy and the regulations, the provisions of the regulations will apply. This Policy is published on www.kolumanotomotiv.com and is effective as of the date of publication.

ANNEX 1 - Purposes of Personal Data Processing

Types Of Personal Data Processed	Purposes Of Processing Personal Data	Maximum Retention Period
Identity	<p>Creation and Tracking of Visitor Records, Management Activities Execution, Providing Information to Authorized Persons, Institutions, and Organizations, Execution of Talent/Career Development Activities, Execution of Investment Processes, Foreign Personnel Work and Residence Permit Processes, Ensuring the Security of Data Controller Operations, Execution of Compensation Policy, Execution of Supply Chain Management Processes, Ensuring the Security of Movable Property and Resources, Tracking Requests/Complaints, Execution of Contract Processes, Execution of Storage and Archiving Activities, Execution of Performance Evaluation Processes Organization and Event Management, Execution of Goods/Services Production and Operations Processes, Execution of Goods/Services Sales Processes, Execution of Goods/Services Purchase Processes, Execution of Logistics Activities, Execution of Business Continuity Activities, Receiving and Evaluating Suggestions for Improving Business Processes, Execution of Occupational Health and Safety Activities, Execution/Control of Business Activities, Planning of Human Resources Processes, Execution of Communication Activities, Execution of Internal, Auditing/Investigation/Intelligence Activities</p> <p>Tracking and Execution of Legal Affairs, Execution of Assignment Processes, Ensuring Physical Security of the Facility, Execution of Financial and Accounting Affairs, Execution of Activities in Compliance with Regulations, Management of Access Rights, Execution of Training Activities, Execution of Auditing/Ethical Activities, Execution of Fringe Benefits and Employee Welfare Processes,</p>	Legal Relationship + 10 Years

	Fulfillment of Employment Contracts and Legal Obligations for Employees, Execution of Employee Satisfaction and Engagement Processes, Execution of Employee Candidate Application Processes, Execution of Employee Candidate/Intern/Student Selection and Placement Processes, Execution of Information Security Processes, Execution of Emergency Management Processes	
Communication	<p>Creation and Tracking of Visitor Records,</p> <p>Execution of Management Activities,</p> <p>Providing Information to Authorized Persons, Institutions, and Organizations,</p> <p>Execution of Talent / Career Development Activities,</p> <p>Execution of Investment Processes,</p> <p>Work and Residence Permit Procedures for Foreign Personnel,</p> <p>Ensuring the Security of Data Controller Operations,</p> <p>Execution of Wage Policy,</p> <p>Execution of Supply Chain Management Processes,</p> <p>Ensuring the Security of Movable Property and Resources,</p> <p>Tracking Requests / Complaints,</p> <p>Execution of Strategic Planning Activities,</p> <p>Execution of Contract Processes,</p> <p>Execution of Retention and Archiving Activities,</p> <p>Execution of Performance Evaluation Processes,</p> <p>Organization and Event Management,</p> <p>Execution of Goods / Services Production and Operations Processes,</p> <p>Execution of Goods / Services Sales Processes,</p> <p>Execution of Goods / Services Procurement Processes,</p> <p>Execution of Logistics Activities,</p> <p>Execution of Business Continuity Activities,</p> <p>Receiving and Evaluating Suggestions for Business Process Improvement,</p> <p>Execution of Occupational Health and Safety Activities,</p> <p>Execution / Audit of Business Activities,</p> <p>Planning of Human Resources Processes,</p> <p>Execution of Communication Activities,</p> <p>Execution of Internal Audit / Investigation / Intelligence Activities,</p> <p>Follow-up and Execution of Legal Affairs,</p> <p>Execution of Assignment Processes,</p> <p>Ensuring Physical Space Security,</p> <p>Execution of Financial and Accounting Affairs,</p> <p>Execution of Activities in Compliance with Legislation,</p> <p>Execution of Access Authorization Processes,</p> <p>Execution of Training Activities,</p> <p>Execution of Audit / Ethical Activities,</p> <p>Execution of Processes Related to Fringe Benefits and Employee Benefits,</p> <p>Fulfillment of Employment Contracts and Legal Obligations for Employees,</p>	Legal Relationship + 10 Years

	Execution of Employee Satisfaction and Engagement Processes, Execution of Application Processes for Job Candidates, Execution of Selection and Placement Processes for Candidates / Interns / Students, Execution of Information Security Processes, Execution of Emergency Management Processes	
Location	Ensuring the Security of Movable Property and Resources Execution / Audit of Business Activities Execution of Assignment Processes Execution of Audit / Ethical Activities Execution of Processes Related to Fringe Benefits and Employee Benefits Execution of Emergency Management Processes	2 Years
Personnel	Execution of Management Activities Providing Information to Authorized Persons, Institutions and Organizations Execution of Talent / Career Development Activities Processing Work and Residence Permits for Foreign Employees Execution of Remuneration Policy Ensuring the Security of Movable Property and Resources Follow-up of Requests / Complaints Execution of Contract Processes Execution of Storage and Archiving Activities Execution of Performance Evaluation Processes Organization and Event Management Execution of Goods / Services Production and Operational Processes Execution of Business Continuity Activities Receiving and Evaluating Suggestions for Business Process Improvement Execution of Occupational Health / Safety Activities Execution / Audit of Business Activities Planning of Human Resources Processes Execution of Communication Activities Execution of Internal Audit / Investigation / Intelligence Activities Follow-up and Execution of Legal Affairs Execution of Assignment Processes Execution of Financial and Accounting Affairs Execution of Activities in Compliance with Legislation Management of Access Authorizations Execution of Training Activities Execution of Audit / Ethical Activities Execution of Fringe Benefits and Employee Benefits Processes Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Employee Satisfaction and Engagement Processes Execution of Job Application Processes for Candidates Execution of Selection and Placement Processes for Candidates / Interns / Students	Legal Relationship + 10 Years

Legal Act	<p>Execution of Management Activities Providing Information to Authorized Persons, Institutions and Organizations Execution of Supply Chain Management Processes Ensuring the Security of Movable Property and Resources Execution of Contract Processes Execution of Storage and Archiving Activities Execution of Goods / Services Sales Processes Execution of Goods / Services Procurement Processes Execution of Occupational Health / Safety Activities Execution / Audit of Business Activities Planning of Human Resources Processes Execution of Internal Audit / Investigation / Intelligence Activities Follow-up and Execution of Legal Affairs Execution of Financial and Accounting Affairs Execution of Activities in Compliance with Legislation Execution of Training Activities Execution of Audit / Ethical Activities Fulfillment of Employment Contract and Legal Obligations for Employees Execution of Job Application Processes for Candidates</p>	Legal Relationship + 10 Years
Customer Operations	<p>Execution of Management Activities Provision of Information to Authorized Persons, Institutions, and Organizations Execution of Contract Processes Execution of Storage and Archiving Activities Execution of Goods / Services Sales Processes Execution of Goods / Services Procurement Processes Execution / Audit of Business Activities Monitoring and Execution of Legal Affairs Execution of Finance and Accounting Operations Ensuring Activities Are Conducted in Compliance with Regulations</p>	Legal Relationship + 10 Years
Physical Site Security	<p>Creation and Tracking of Visitor Records Execution of Management Activities Provision of Information to Authorized Persons, Institutions, and Organizations Ensuring the Security of Movable Property and Resources Conducting Retention and Archiving Activities Execution of Goods / Services Production and Operational Processes Execution of Business Continuity Activities Execution of Occupational Health and Safety Activities Execution / Supervision of Business Activities Execution of Internal Audit / Investigation / Intelligence Activities Ensuring Physical Space Security Execution of Audit / Ethics Activities Execution of Information Security Processes</p>	6 Months

Process Security	Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Ensuring the Security of Data Controller Operations Ensuring the Security of Movable Property and Resources Monitoring Requests / Complaints Conducting Retention and Archiving Activities Execution of Activities in Compliance with Legislation Managing Access Authorizations Execution of Information Security Processes	2 Years
Finance	Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Execution of Wage Policy Execution of Supply Chain Management Processes Execution of Contract Processes Conducting Retention and Archiving Activities Execution of Goods / Services Production and Operational Processes Execution of Goods / Services Sales Processes Execution of Goods / Services Procurement Processes Execution / Supervision of Business Activities Planning of Human Resources Processes Monitoring and Execution of Legal Affairs Execution of Assignment Processes Execution of Finance and Accounting Affairs Execution of Activities in Compliance with Legislation Execution of Employee Benefits and Welfare Processes Fulfillment of Employment Contract and Statutory Obligations for Employees	Legal Relationship + 10 Years
Professional Experience	Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Execution of Talent / Career Development Activities Processing Work and Residence Permits for Foreign Personnel Conducting Retention and Archiving Activities Execution / Supervision of Business Activities Planning of Human Resources Processes Monitoring and Execution of Legal Affairs Execution of Activities in Compliance with Legislation Execution of Training Activities Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Application Processes for Job Candidates Execution of Candidate / Intern / Student Selection and Placement Processes	Legal Relationship + 10 Years

Audio-Visual Records	Creation and Monitoring of Visitor Records Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Processing Work and Residence Permits for Foreign Personnel Ensuring the Security of Movable Property and Resources Conducting Retention and Archiving Activities Execution of Goods / Services Production and Operational Processes Execution of Business Continuity Activities Execution of Occupational Health and Safety Activities Execution / Supervision of Business Activities Execution of Internal Audit / Investigation / Intelligence Activities Ensuring Physical Space Security Execution of Activities in Compliance with Legislation Execution of Audit / Ethics Activities Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Application Processes for Job Candidates Execution of Candidate / Intern / Student Selection and Placement Processes Execution of Information Security Processes	Legal Relationship + 10 Years
Dress and Appearance	Execution of Occupational Health and Safety Activities Planning of Human Resources Processes Execution of Activities in Compliance with Legislation Fulfillment of Employment Contract and Statutory Obligations for Employees	Legal Relationship + 10 Years
Health Data	Providing Information to Authorized Persons, Institutions, and Organizations Conducting Retention and Archiving Activities Execution of Goods / Services Procurement Processes Execution of Occupational Health and Safety Activities Planning of Human Resources Processes Monitoring and Execution of Legal Affairs Execution of Assignment Processes Execution of Activities in Compliance with Legislation Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Application Processes for Job Candidates Execution of Candidate / Intern / Student Selection and Placement Processes	Legal Relationship + 10 Years
Criminal Convictions and Security Measures	Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Planning of Human Resources Processes Monitoring and Execution of Legal Affairs Execution of Activities in Compliance with Legislation Execution of Audit / Ethics Activities Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Application Processes for Job Candidates	Legal Relationship + 10 Years

	Execution of Candidate / Intern / Student Selection and Placement Processes	
Biometric Data	Execution of Management Activities Ensuring the Security of Data Controller Operations Ensuring the Security of Movable Property and Resources Execution / Supervision of Business Activities Execution of Internal Audit / Investigation / Intelligence Activities Ensuring Physical Space Security Managing Access Authorizations Execution of Audit / Ethics Activities Fulfillment of Employment Contract and Statutory Obligations for Employees Execution of Information Security Processes	As Long as the Legal Relationship Continues
Other – Insurance Data	Execution of Management Activities Providing Information to Authorized Persons, Institutions, and Organizations Conducting Retention and Archiving Activities Planning of Human Resources Processes Execution of Activities in Compliance with Legislation Execution of Employee Benefits and Welfare Processes Fulfillment of Employment Contract and Statutory Obligations for Employees	Legal Relationship + 10 Years
Other – Vehicle Data	Providing Information to Authorized Persons, Institutions, and Organizations Execution of Goods / Services Production and Operational Processes Execution of Goods / Services Sales Processes Execution / Supervision of Business Activities Monitoring and Execution of Legal Affairs Execution of Activities in Compliance with Legislation	1 Year