

Kar Porselen Sanayi Ve Ticaret Anonim Şirketi	POLICY
	<u>Personal Data Retention and Destruction Policy</u> Version 2026/01 .../.../...

TABLE OF CONTENTS

1. PREAMBLE	2
2. PURPOSE AND SCOPE OF THE POLICY	2
3. DEFINITIONS	2
4. RECORDING MEDIUM REGULATED BY POLICY	3
5. REASONS REQUIRING THE RETENTION AND DESTRUCTION OF PERSONAL DATA	4
6. METHODS APPLIED FOR THE DESTRUCTION OF PERSONAL DATA AND TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE DESTRUCTION OF PERSONAL DATA IN ACCORDANCE WITH THE LAW	6
7. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE SECURE RETENTION OF PERSONAL DATA AND THE PREVENTION OF UNLAWFUL PROCESSING AND ACCESS TO IT	8
8. TITLES, DEPARTMENTS AND JOB DESCRIPTIONS OF THOSE INVOLVED IN THE RETENTION AND DESTRUCTION OF PERSONAL DATA	8
9. RETENTION AND DESTRUCTION PERIODS	9
10. PERIODIC DESTRUCTION PERIODS	9
11. EFFECTIVE DATE	10
12. APPENDIX - 1 VERSION HISTORY	11

KAR PORSELEN SANAYİ VE TİCARET ANONİM ŞİRKETİ PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. PREAMBLE

Protection of personal data is of great importance for Kar Porselen Sanayi Ve Ticaret Anonim Şirketi (hereinafter referred to as "**Kar Porselen**" and/or "**Company**") and our Company shows maximum sensitivity in this regard. Accordingly, the processing of personal data in a manner consistent with the expectations of individuals and in accordance with the law is one of the basic building blocks of our Company.

In this respect, our Company retains and destroys the personal data obtained during its activities in accordance with the general principles and regulations specified in this Personal Data Retention and Destruction Policy (hereinafter referred to as the "**Policy**"), which is prepared in accordance with the Constitution, the Personal Data Protection Law Nr. 6698 (hereinafter referred to as the "**Law**" and/or "**PDPL**"), the Regulation on Deletion, Destruction or Anonymisation of Personal Data (hereinafter referred to as the "**Regulation**"), and other relevant legislation.

2. PURPOSE AND SCOPE OF THE POLICY

With this Policy, the Company aims to fulfil the obligations determined by the legislation on these issues, including the general principles and principles of the Company regarding the retention and destruction of natural person data subject to personal data processing activities within the scope of PDPL.

This Policy covers all personal data subject to the Company's data processing activities within the scope of PDPL . In addition, unless otherwise stated in this Policy, the documents referred to by the Policy include both physical and digital copies.

3. DEFINITIONS

Unless the content of this Policy requires otherwise:

"Explicit consent": refers to consent on a specific subject, based on information and expressed with free will,

"Recipient Group" refers to the category of natural or legal person to whom personal data is transferred by the data controller,

"Constitution" refers to the Constitution of the Republic of Türkiye,

"Related User" refers to persons who process personal data within the organisation of the data controller or in accordance with the authority and instruction received from the data controller, except for the person or unit responsible for the technical

	retention, protection and backup of the data,
"Destruction"	refers to deletion, destruction or anonymisation of personal data,
"Recording Medium"	refers to all kinds of media containing personal data that are fully or partially automated or processed by non-automated means, provided that they are part of any data recording system,
"Personal data"	refers to any information relating to an identified or identifiable natural person (e.g. name-surname, Turkish ID Number, e-mail, address, date of birth, credit card number, bank account number - <i>Therefore, the processing of information on legal persons is not covered by the PDPL</i>),
"Person Concerned":	refers to the natural person whose personal data is processed,
"Processing of personal data":	refers to all kinds of operations performed on personal data, such as obtaining, recording, storing, retaining, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that they are part of any data recording system.
"Board":	refers to Personal Data Protection Board.
"Sensitive Personal Data"	refers to data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data,
"Periodic Destruction"	refers to the deletion, destruction or anonymisation process specified in this Policy and to be carried out ex officio at recurring intervals in the event that all of the conditions for processing personal data in the PDPL disappear,
"Data Controller"	refers to the person who determines the purposes and means of processing personal data and manages the place where the data is kept systematically (data recording system).

4. RECORDING MEDIUM REGULATED BY POLICY

The Company stores all personal data subject to data processing activities within the scope of PDPL in the following environments where personal data processed by fully or

partially automated or non-automated means, provided that they are part of any data recording system:

ELECTRONIC MEDIA:

- XMAIL SERVER (cloud)
- MICRO ACCOUNTING/PAYROLL
- FILE SERVER
- DC
- My Portal
- Micros POS

Physical media:

- Unit Cabinets
- Archive (In-house and with service procurement)

Our Company databases, third party databases, email accounts, desktop computers, Company employees' vehicles (e.g. mobile phones), backup areas, paper files, etc.

5. REASONS REQUIRING THE RETENTION AND DESTRUCTION OF PERSONAL DATA

The following principles are taken as basis by Kar Porselen during the performance of personal data processing activities:

- Compliance with the law and the rule of honesty,
- Ensuring that personal data is accurate and up-to-date when necessary,
- Processing for specific, explicit and legitimate purposes,
- Being relevant, limited and proportionate to the purpose for which they are processed,
- Retention for the period stipulated in the relevant legislation or required for the purpose for which they are processed.

Kar Porselen stores and uses personal data in accordance with the above-mentioned principles, for the purposes of personal data processing in the relevant articles of the Kar Porselen Personal Data Protection and Processing Policy and in accordance with the conditions for the processing of personal data in Articles 5 and 6 of the PDPL specified below, and in the event that all of these conditions disappear, it destroys personal data ex officio or upon the request of the personal data subject.

Pursuant to Articles 5 and 6 of the PDPL, personal data are processed and stored in the following cases:

(a) Explicit Consent of the Personal Data Subject

The first condition for processing personal data is the explicit consent of the data subject. The explicit consent of the personal data subject must be related to a specific subject, based on information and with free will.

(b) Explicitly stipulated in the Laws

The personal data of the data subject may be processed in accordance with the law

without obtaining his/her explicit consent, if expressly stipulated in the Laws.

(c) Failure to Obtain Explicit Consent of the Personal Data Subject Due to Actual Impossibility

The personal data of the data subject may be processed if it is mandatory to process the personal data of the person who is unable to disclose his/her consent due to actual impossibility or whose consent cannot be recognised as valid, in order to protect his/her or another person's life or physical integrity.

(d) Direct Relevance to the Establishment or Performance of the Contract

Provided that it is directly related to the establishment or performance of a contract, it is possible to process personal data if it is necessary to process personal data belonging to the parties to the contract.

(e) Legal Liability

If data processing is mandatory for our company to fulfil its legal obligations, the data of the personal data subject may be processed.

(f) Publicization of Personal Data by the Personal Data Subject

If the data subject has made his/her personal data public by himself/herself, the relevant personal data may be processed limited to publicization.

(g) Data Processing is Mandatory for the Establishment or Protection of a Right

Personal data of the data subject may be processed if data processing is mandatory for the establishment, exercise or protection of a right.

(h) Data Processing is Mandatory for the Legitimate Interest of our Company

Provided that it does not harm the fundamental rights and freedoms of the personal data subject, the personal data of the data subject may be processed if data processing is mandatory for the legitimate interests of our Company.

Accordingly, the basis of the personal data processing activity may be only one of the above-mentioned conditions, or more than one of these conditions may be the basis of the same personal data processing activity.

6. METHODS APPLIED FOR THE DESTRUCTION OF PERSONAL DATA AND TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE DESTRUCTION OF PERSONAL DATA IN ACCORDANCE WITH THE LAW

Our company deletes, destroys or anonymises personal data by the following methods in the event that all of the conditions for processing personal data specified in Articles 5 and 6 of the PDPL disappear. Our Company shows utmost care and diligence in the destruction of personal data. In this context, our Company takes the necessary technical and administrative measures in accordance with the provisions of Article 12 of the PDPL and the Regulation, the general principles stated above, this Policy and the decisions of the Personal Data Protection Board, according to the technological possibilities and the cost of implementation regarding the following issues. All transactions carried out within the scope of destruction are recorded by our Company and these records are kept for 10 years, excluding other legal obligations. Unless otherwise decided by the Personal Data Protection Board, our Company chooses the appropriate method of ex officio deletion, destruction or anonymisation of personal data according to technological possibilities and implementation cost, and explains the justification of the appropriate method upon request of the personal data subject.

(a) Methods of Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the users concerned. Our Company takes all necessary technical and administrative measures according to the technological possibilities and the cost of implementation in order to ensure that the deleted personal data is not accessed and reused for the relevant users.

In this context, our Company applies the following methods for the deletion of personal data:

[The organisation should explain the deletion methods it applies within the scope of deletion activities and the technical and administrative measures it applies to ensure that deletion is carried out securely]

(b) Methods of Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Our Company takes all necessary technical and administrative measures for the destruction of personal data according to the technological possibilities and the cost of implementation.

In this context, our Company applies the following methods for the destruction of personal data:

- **De-magnetisation:** It is the method of distorting the data on the magnetic media in an unreadable way by passing it through special devices where it will be exposed to high magnetic fields. It should be noted that if destruction by this method is not successful, the destruction process can only be completed by physically destroying

the media.

- Physical Destruction: Personal data may also be processed by non-automatic means, provided that they are part of any data recording system. When destroying such data, the system of physically destroying the personal data in such a way that it cannot be used later is applied. The destruction of data on paper and microfiche media must also be carried out in this way, as it is not possible to destroy them in any other way.
- Overwriting: Overwriting is a data destruction method that makes it impossible to read and recover old data by writing random data consisting of 0s and 1s at least seven times on magnetic media and rewritable optical media by means of special software.

During the realisation of the above-mentioned situations, the Company fully complies with the provisions of the PDPL, the Regulation and other relevant legislation in order to ensure data security and takes all necessary administrative and technical measures.

[The organisation should explain the destruction methods it applies within the scope of destruction activities and the technical and administrative measures it applies to ensure that destruction is carried out safely]

(c) Methods of Anonymisation of Personal Data

Anonymisation of personal data means making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even if the personal data is matched with other data. In order for personal data to be anonymised; personal data must be rendered unassociated with an identified or identifiable natural person, even through the use of techniques suitable for the recording medium and the relevant field of activity, such as reversal and matching of data with other data by our Company, recipient or recipient groups. Our Company takes all necessary technical and administrative measures regarding the anonymisation of personal data according to technological possibilities and implementation cost.

In this context, our Company applies the following methods for anonymising personal data:

- Secure Deletion from Software: When deleting data processed by fully or partially automated means and stored in digital media; methods are used to delete the data from the relevant software in such a way as to make it inaccessible and non-reusable in any way for the Related Users.
- Deleting the relevant data in the cloud system by giving a delete command; removing the access rights of the relevant user on the file or the directory where the file is located on the central server; deleting the relevant rows in databases with database commands or deleting the data on portable media, i.e. flash media, using appropriate software can be considered within this scope.

However, if the deletion of personal data will result in the inaccessibility of other data

within the system and the inability to use this data, personal data will also be deemed deleted if the personal data is archived by making it unassociated with the person concerned, provided that the following conditions are met.

- ✓ It is not accessible to any other institution, organisation or person.
- ✓ Taking all necessary technical and administrative measures to ensure that personal data is accessed only by authorised persons.
- ✓ Secure Deletion by Expert: In some cases, he or she may hire an expert to delete personal data on his or her behalf. In this case, the personal data shall be securely erased by the person specialised in this field in such a way that it cannot be accessed and reused in any way for the Related Users.
- ✓ Obfuscation of Personal Data in Paper Media: In order to prevent the misuse of personal data or to delete the data requested to be deleted, it is the method of physically cutting the relevant personal data and removing it from the document or making it invisible by using fixed ink so that it cannot be reversed and cannot be read with technological solutions.

[The organisation should explain the anonymisation methods it applies within the scope of anonymisation activities and the technical and administrative measures it applies to ensure that anonymisation is carried out securely]

7. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE SECURE RETENTION OF PERSONAL DATA AND THE PREVENTION OF UNLAWFUL PROCESSING AND ACCESS TO IT

Our Company shows the utmost care and diligence in the safe retention of personal data and the prevention of unlawful processing and access, and takes the necessary technical and administrative measures in accordance with the technological possibilities and implementation cost regarding the following issues in accordance with Article 12 of the PDPL and the provisions of the Regulation, the general principles mentioned above, this Policy and the decisions of the Personal Data Protection Board:

[Technical and Administrative Measures Taken by the Organisation Should Be Entered]

8. TITLES, DEPARTMENTS AND JOB DESCRIPTIONS OF THOSE INVOLVED IN THE RETENTION AND DESTRUCTION OF PERSONAL DATA

Persons involved in the processes of storing and destroying personal data within our company are informed and trained on the Personal Data Protection Legislation and the processing of personal data in accordance with the law. In this context, the employees of our Company and persons who learn personal data due to their duties store and destroy such information in accordance with the provisions of PDPL and other relevant legislation. This obligation continues after the termination of the existing relationship with

the Related Persons.

9. RETENTION AND DESTRUCTION PERIODS

Our company retains and destroys personal data only for the period specified in the legislation that it is obliged to comply with or for the period required for the purpose for which they are processed.

In the event that the personal data subject requests the destruction of his/her personal data by applying to our Company, our Company;

- (a) If all the conditions for processing personal data have disappeared:
 - (i) Finalises the request of the personal data subject within thirty days at the latest and informs the personal data subject; and
 - (ii) If the personal data subject to the request has been transferred to third parties, it notifies this situation to the third party; ensures that necessary actions are taken before the third party.
- (b) If all the conditions for processing personal data have not disappeared, the request of the personal data subject may be rejected by explaining the reason in accordance with the third paragraph of Article 13 of the PDPL and notifies the personal data subject in writing or digitally within thirty days at the latest.

10. PERIODIC DESTRUCTION PERIODS

Our Company destroys personal data in the first periodic destruction process following the date on which the obligation to destroy personal data arises. In this context, our Company subjects personal data to destruction in 3-month periods if the obligation to destroy personal data arises. The said period does not exceed the maximum periodic destruction period specified in Article 11 of the Regulation in any case and under any circumstances.

The approximate retention and destruction periods of the data processed by the Company are written as follows and are included in the inventory organised by the Company.

Data Subject	Retention Period	Destruction Period
Employee	10 years following the termination of the employment relationship	Within 30 days following the data subject's application for destruction
Employee	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period

Employee	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Employee Candidate	For a maximum of 2 years, as long as the CV will be out of date	Within 180 days following the end of the retention period
Business Partner/Solution Partner/Consultant	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Visitor	2 YEARS	Within 180 days following the end of the retention period
Occupational Health and Safety Practices	10 years following the termination of the employment relationship	Within 180 days following the end of the retention period
Log/Recording/Tracking Systems	2 YEARS	Within 180 days following the end of the retention period
Visitor Registration Information	10 YEARS	Within 180 days following the end of the retention period
Website Visitors	2 YEARS	Within 180 days following the end of the retention period
Potential Guest	2 YEARS	Within 180 days following the end of the retention period
Suppliers, Manufacturers, Support Firms	10 YEARS	Within 180 days following the end of the retention period

11. EFFECTIVE DATE

This Policy entered into force on **[Insert Date]**. The Policy may be updated from time to time in order to adapt to changing conditions and legislation. Updated Policy shall enter into force on the date of its publication on <https://karporselen.com/>. In case of any conflict between this Policy and the provisions of PDPL, Regulation and Kar Porselen Sanayi ve Ticaret Anonim Şirketi Personal Data Protection and Processing Policy, the provisions of

