# KONYA KAĞIT SAN. VE TİC. A.Ş.

**PERSONAL DATA STORAGE and DESTRUCTION POLICY**

**TABLE OF CONTENTS**

## 1. PURPOSE

**KONYA KAĞIT SANAYİ VE TİCARET A.Ş. (Konya Kağıt)** has issued this Personal Data Storage and Destruction Policy ("**Storage and Destruction Policy**") in order to regulate the technical and administrative protection of personal data in accordance with the Law No. 6698 on the Protection of Personal Data ("**Law**"), and to regulate the implementation of the provisions of the Regulation on the Deletion, Destruction or Anonymisation of Personal Data ("**Regulation**") published in the Official Gazette dated 28/10/2017 in the event that the conditions for the processing of personal data disappear.

## 2. RECORDING MEDIA WHERE PERSONAL DATA ARE STORED

Personal data belonging to data subjects are securely stored by Konya Kağıt in the environments listed below in accordance with the relevant legislation, especially the provisions of the Law:

**Electronic media:**

- Server
- Virtual Server
- Nas Storage
- Microsoft Office Programmes and DB
- Firewall and DLP Devices
- Image Recorders

**Physical environments:**

- Unit Cabinets
- Folders
- Archive

## 3. EXPLANATIONS ON THE REASONS REQUIRING RETENTION

**Personal data belonging to data subjects, especially by Konya Kağıt:**

a. Sustainability of activities,
b. Fulfilment of legal obligations,
c. Planning and fulfilment of employee rights and benefits,
d. For the purpose of managing business relations, it is stored securely in the physical or electronic media mentioned above within the limits specified in the Law and other relevant legislation.

**Reasons requiring concealment:**

a. Personal data are directly related to the establishment and performance of contracts,
b. The establishment, exercise or protection of a right of personal data,
c. Provided that personal data does not harm the fundamental rights and freedoms of individuals, Konya Kağıt has a legitimate interest,
d. Fulfilment by Konya Kağıt of any legal obligation of personal data,
e. The legislation clearly stipulates the storage of personal data,
f. Explicit consent of data subjects in terms of storage activities that require the explicit consent of data subjects.

Pursuant to the Regulation, personal data of data subjects shall be deleted, destroyed or anonymised by Konya Kağıt ex officio or upon request in the following cases

a. Amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing or storage of personal data,
b. The purpose requiring the processing or storage of personal data disappears,
c. The disappearance of the conditions requiring the processing of personal data in Articles 5 and 6 of the Law.
d. In cases where the processing of personal data is carried out only on the basis of explicit consent, the person concerned withdraws his/her consent,
e. The application of the data subject for the deletion, destruction or anonymisation of his/her personal data within the framework of his/her rights under paragraphs 2 (e) and (f) of Article 11 of the Law is accepted by the data controller,
f. In cases where the data controller rejects the application made by the data subject with the request for deletion, destruction or anonymisation of his/her personal data, his/her response is found insufficient or he/she does not respond within the period stipulated in the Law; a complaint is filed to the Board and this request is approved by the Board,
g. Although the maximum period required for the storage of personal data has elapsed, there are no circumstances justifying the storage of personal data for a longer period of time.

**4. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA**

In accordance with Article 12 of the Law, Konya Kağıt takes the necessary technical and administrative measures to ensure the appropriate level of security to prevent unlawful processing of personal data, to prevent unlawful access to data and to ensure the preservation of data, and to carry out or have the necessary audits carried out within this scope. In the event that the processed personal data is obtained by third parties through unlawful means even though all technical and administrative measures have been taken, Konya Kağıt notifies the relevant units as soon as possible.

**4.1 Technical Measures**

Technical Measures

- Network security and application security are ensured.
- Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
- Data masking measures are applied when necessary.
- Confidentiality undertakings are made.
- The authorisations of employees who change their duties or leave their jobs in this area are removed.
- Up-to-date anti-virus systems are used.
- Closed system network is used for personal data transfers via network.
- Key management is implemented.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- Security of personal data stored in the cloud is ensured.
- There are disciplinary regulations that include data security provisions for employees.
- Training and awareness raising activities on data security are carried out at regular intervals for employees.
- Authorisation matrix has been created for employees.
- Access logs are kept regularly.
- Firewalls are used.
- Signed contracts contain data security provisions.
- Extra security measures are taken for personal data transferred via paper and the relevant document is sent in confidentiality-grade document format.
- Personal data security policies and procedures have been determined.
- Personal data security problems are reported quickly.

- Personal data security is monitored.
- Necessary security measures are taken for entry and exit to physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- The security of environments containing personal data is ensured.
- Personal data is minimised as much as possible.
- Personal data are backed up and the security of backed up personal data is also ensured.
- User account management and authorisation control system is implemented and these are also monitored.
- In-house periodic and/or random audits are carried out and carried out.
- Log records are kept without user intervention.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- If sensitive personal data is to be sent via electronic mail, it is sent encrypted and using KEP or corporate mail account.
- Secure encryption / cryptographic keys are used for sensitive personal data and managed by different units.
- Attack detection and prevention systems are used.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is performed.
- Sensitive personal data transferred in portable memory, CD, DVD media are encrypted.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers on data security is ensured.
- Data loss prevention software is used.

**4.2 Administrative Measures:**

- Employees are trained on the technical measures to be taken to prevent unlawful access to personal data.
- Access to personal data and authorisation processes are designed and implemented within Konya Kağıt in accordance with the legal compliance requirements for processing personal data on a business unit basis. In limiting access, whether the data is of special nature or not and the degree of importance are also taken into consideration.
- Konya Kağıt has included records in all documents containing personal data that regulate the relationship between Konya Kağıt and its employees, stating that in order to process personal data in accordance with the law, the obligations stipulated by the Law must be complied with, personal data must not be disclosed, personal data must not be used unlawfully, and the confidentiality obligation regarding personal data continues even after the termination of the employment contract with Konya Kağıt.
- Employees are informed that they cannot disclose the personal data they have learnt to others in violation of the provisions of the Law and cannot use them for purposes other than processing, and that this obligation will continue even after they leave their duties, and necessary commitments are obtained from them in this direction.
- In the contracts concluded by Konya Kağıt with the persons to whom personal data are transferred in accordance with the law, provisions are added stating that the persons to whom personal data are transferred will take the necessary security measures to protect personal data and ensure that these measures are complied with in their own organisations.
- In case the processed personal data is obtained by others through unlawful means, it notifies the relevant person and the Board as soon as possible.

- When necessary, it employs personnel who are knowledgeable and experienced in the processing of personal data and provides training to its personnel within the scope of personal data protection legislation and data security.
- Konya Kağıt carries out and has carried out the necessary audits to ensure the implementation of the provisions of the Law. It eliminates the confidentiality and security weaknesses that arise as a result of the audits.

**5. MEASURES TAKEN REGARDING THE DESTRUCTION OF PERSONAL DATA**

Although Konya Kağıt has been processed in accordance with the provisions of the relevant law, it may delete or destroy personal data based on its own decision or upon the request of the personal data owner in the event that the reasons requiring its processing disappear. Following the deletion of personal data, the relevant persons will not be able to access and use the deleted data again in any way. Konya Kağıt will manage an effective data tracking process for defining and tracking the destruction processes of personal data. The process carried out will be the identification of the data to be deleted, the identification of the relevant persons, the identification of the access methods of the persons and the deletion of the data immediately afterwards.

Konya Kağıt may use one or more of the following methods to destroy, delete or anonymise personal data, depending on the medium in which the data is recorded:

**5.1 Methods for Deletion, Destruction and Anonymisation of Personal Data**

**5.1.1 Deletion of Personal Data**

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. Konya Kağıt may use one or more of the following methods as a method of deleting personal data:

✓ Personal data on paper will be processed by drawing, painting, cutting or erasing by blackout method.
✓ User(s) access right(s) for office files in the central file will be eliminated.
✓ The rows or columns containing personal information in the databases will be deleted with the 'Delete' command.

It will be safely deleted with the help of an expert when necessary.

**5.1.2 Destruction of Personal Data**

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and non-reusable by anyone in any way by the following methods.

Physical Destruction
Destruction with Paper Shredder
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.

**5.1.3. 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 by matching them with other data. Konya Kağıt may use one or more of the following methods to anonymise personal data:

**Masking**: Data masking is a method of anonymising personal data by removing the basic identifying information of personal data from the data set.

**De-recording:** In the de-recording method, the data line containing singularity among the data is removed from the records and the stored data is anonymised.

**Regional Hiding:** In the regional hiding method, anonymisation is ensured by hiding the relevant data if it is determinative due to the fact that a single data creates a combination that can be seen very little.

**Global Coding:** With the data derivation method, a more general content is created from the content of the personal data and it is ensured that the personal data cannot be associated with any person. For example; specifying ages instead of dates of birth; specifying the region of residence instead of open address.

**Adding Noise**: The method of adding noise to the data, especially in a data set where numerical data is predominant, anonymises the data by adding some deviations in the plus or minus direction to the existing data at a determined rate. For example, in a data set with weight values, a deviation of (+/-) 3 kg is used to prevent the display of real values and anonymise the data. The deviation is applied equally to each value.

In accordance with Article 28 of the Law; anonymised personal data may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the Law and the explicit consent of the personal data owner will not be sought.

Konya Kağıt may take an ex officio decision regarding the deletion, destruction or anonymisation of personal data and may freely determine the method to be used according to the category it has chosen. In addition, within the scope of Article 13 of the Regulation, if the data subject selects one of the categories of deletion, destruction or anonymisation of his/her personal data during the application, Konya Kağıt will be at liberty regarding the methods to be used in the relevant category.

**6. STORAGE AND DESTRUCTION PERIODS OF PERSONAL DATA**

Konya Kağıt retains personal data for the purposes for which they are processed for the periods specified in Annex-1. If a period of time is stipulated in the legislation regarding the storage of the personal data in question, this period shall be complied with. In the absence of a period stipulated in the legislation, personal data will be retained for the maximum period for the storage of personal data in the table in Annex-1. These periods have been determined by evaluating Konya Kağıt's data categories and data subject groups; ensuring that the data obtained as a result of this evaluation will ensure the fulfilment of the obligations under the law and taking into account the maximum statute of limitations (10 years) in the Turkish Code of Obligations.

In the event that the obligation to delete, destroy or anonymise arises due to the expiration of these periods, Konya Kağıt deletes, destroys or anonymises personal data in the first periodic destruction process following this date.

All transactions regarding the deletion, destruction and anonymisation of personal data are recorded and such records are kept for at least three years, excluding other legal obligations.

**7. PERIODIC DESTRUCTION PERIODS**

Pursuant to Article 11 of the Regulation, the period of periodic destruction is determined as 6 months. Accordingly, periodic destruction process is carried out in June and December every year in the Agency. In the systems in question, the information will be deleted from the documents, files, CDs, floppy discs, hard discs, if any, where the data is saved, in a way that the information will not be recovered again.

**8. PERSONEL**

Within the scope of the Law, Konya Kağıt, as the data controller, based on paragraph 1 of Article 11 of the Regulation, the titles, units and job descriptions of the personnel whose obligations will be fulfilled in terms of the implementation of the data storage and destruction process of the Law are determined by the table in Annex-2 of the Storage and Destruction Policy.

These persons, whose boundaries have been determined, are responsible for the transactions and actions that take place within their limits of authority within the scope of the Turkish Commercial Code, the Code of Obligations and the Turkish Penal Code. In particular, the Chairman of Konya Kağıt Personal Data Protection Committee has been elected to represent Konya Kağıt in law enforcement, prosecution offices, public institutions and courts and to be authorised to testify. Each department responsible will be obliged to supervise whether the relevant users in the departments act in accordance with the Storage and Destruction Policy and Personal Data Policy prepared within the framework of the Law and Regulation. All department supervisors will report the transactions carried out in accordance with this Storage and Destruction Policy within the specified periodic destruction periods to the Chairman of Konya Kağıt Personal Data Protection Committee. The decision resulting from the results of the work carried out for these reports will be put into practice.

**9. REVISION AND REPEAL**

If the Storage and Destruction Policy is amended or repealed, the new regulation will be announced on Konya Kağıt's website.

**10. ENFORCEMENT**

This Storage and Destruction Policy enters into force on the date of its publication.

**ANNEXES**

**Annex 1- Data Storage and Destruction Periods**
**Annex 2- Table of Personnel in Charge of Personal Data Storage and Destruction**

**Annex 1- Data Storage and Destruction Periods**

| Data Category | Storage Period | Destruction Period |
|---|---|---|
| **Identity** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Contact** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Location** | 2 years from the transaction date | At the first periodic destruction period following the end of the storage period |
| **Personnel** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Legal Action** | 10 years following the date of the legal proceedings | At the first periodic destruction period following the end of the storage period |
| | If a lawsuit has been filed, 5 years starting from the year following the finalisation of the decision | At the first periodic destruction period following the end of the storage period |
| **Customer Transaction** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Physical Space Security** | 33 days | At the first periodic destruction period following the end of the storage period |
| **Process Security** | 2 years from the transaction date | At the first periodic destruction period following the end of the storage period |
| **Risk Management** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Finance** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Professional Experience** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Marketing** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Audio and Visual Recordings** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Association Membership** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Health Information** | 15 years starting from the year following the end of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Criminal Conviction and Security Measures** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Family Information** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Operation Data** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Website Usage** | 2 years from the transaction date | At the first periodic destruction period following the end of the storage period |

| | | |
|---|---|---|
| **Request / Complaint Management Information** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Reputation Management Knowledge** | 2 years starting from the year following the date of the transaction or termination of the legal relationship | At the first periodic destruction period following the end of the storage period |
| **Event Management Knowledge** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Signatures** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Insurance Information** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |
| **Vehicle Information** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Compliance Information** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Audit and Inspection** | 10 years starting from the year following the date of the transaction or termination of the legal relationship subject to the legislation | At the first periodic destruction period following the end of the storage period |
| **Foreign Residence Permit Information** | 10 years starting from the year following the termination of the labour relationship | At the first periodic destruction period following the end of the storage period |

**Annex 2- Table of Personnel in Charge of Personal Data Storage and Destruction**

| PERSONNEL | TASK | RESPONSIBILITY |
|---|---|---|
| Personnel Manager | Application manager | Management of the personal data destruction process in accordance with the periodic destruction period by ensuring the compliance of the processes within the task with the storage period |
| Administrative and Financial Affairs Officer | Application manager | Management of the personal data destruction process in accordance with the periodic destruction period by ensuring the compliance of the processes within the task with the storage period |
| Information Processing | Application manager | Management of the personal data destruction process in accordance with the periodic destruction period by ensuring the compliance of the processes within the task with the storage period |

Note: Destruction is determined by the Management during the Storage Periods