Policy on Storage, Destruction and Anonymization of Personal Data

Document Name:	Policy on Storage, Destruction and Anonymization of Personal Data
Contents of the Document:	The purpose of this Policy is to set forth the main principles regarding the storage, destruction and anonymization of personal data by Nemil Turizm Tekstil A.Ş
Legal Basis:	6698 no. Law on Protection of Personal Data, The Regulation on Deletion, Disposal or Anonymization of Personal Data

PREPARED BY

Küçük&Küçük Attorneys at Law

In the case of any discrepancy or inconsistency between the Turkish version and any other translated version of this Policy, the original Turkish version shall take precedence.

CONTENTS

1) POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

1.1. This Policy on Storage, Destruction and Anonymization of Personal Data (“Policy”) shall apply to all Company departments, employees, officers and third parties which is involved in processing of personal data by any means.

1.2. This Policy applies to all annihilation activities conducted by Nemil and it shall be implemented whenever an destruction of personal data is deemed necessary.

1.3. This Policy shall not be applied to non-personal data.

1.4. In case of any new regulations or revisions regarding contents of this Policy, Nemil shall revise this Policy in accordance with the concerned regulations.

1.5. In case there is any legal obstacle which prevents the implementation of this Policy by Nemil, Nemil shall redefine the steps it will take if deemed necessary.

2) For the purposes of this Policy the following definitions shall apply:

Explicit consent	Freely given, specific and informed consent
Anonymizing	Rendering personal data impossible to link with an identified or an identifiable natural person, even through matching them with other data
Recipient Group	The group of natural persons or legal entities, to whom the personal data are transferred by the data controller
Anonymized data	Personal data which is impossible to link with an identified or an identifiable natural person, even through matching them with other data
Destruction	Deletion, destruction or anonymization of personal data.
Concerned user	People who process personal data within the data manager organization or under the authority and instruction of the data manager apart from the person or unit who is responsible for technically storing, protecting and backing up data.
Law/KVKK	Law on Protection of Personal Data no. 6698
Recording medium	Any medium containing personal data processed by means which are completely or partially automatic or non-automatic as part of any data recording system.
Special Categories of Personal Data	Personal data relating to race, ethnic origin, political opinions, philosophical or religious beliefs, being part of a sect, other beliefs, dressing style, membership of an association, foundation or a trade-union, physical or mental health, sexual life or sexual orientation, criminal conviction and security measures, genetic or biometric data

Personal data	Any information relating to an identified or identifiable natural person. Such as; a name, an identification number, e-mail, location data, date of birth, credit card number etc.
Data processor	The natural or legal person who processes personal data on behalf of the controller upon his/her/their authorization
Commission	Committee responsible for the implementation of the Law on Protection of Personal Data Procedures to be applied in accordance with this Policy.
Board	The Personal Data Protection Board
Authority	The Personal Data Protection Authority
Data Registry System	The registry of data controllers that is maintained by the Personal Data Protection Board
Data Inventory	The inventory where Nemil details its data processing activities in accordance with business processes and that has the following information; the details of the personal data being processed, the data categories, the recipient group and the data subject group.
Deletion	Deletion of personal data; making personal data inaccessible and non-reusable in any way for Concerned Users.
Data Controller representative	The employee who is elected from the committee and appointed by the decision of the Board of Directors, and conducts the Company's relations with the Board.

3) PURPOSE AND SCOPE

3.1. The purpose of this Policy is to determine the principles and procedures which shall be applied to natural persons or legal entities who is in charge of the retention and destruction of personal data and to determine the principles and procedures Nemil and third parties authorized by Nemil shall comply with for the fulfilment of the obligations on as required by the Regulation on the Deletion, Destruction or Anonymization of Personal Data, issued based on the Article 7 of Law No. 6698 on the Protection of Personal Data.

3.2. In compliance with Regulation, as a Data Controller who is obliged to be registered in Data Controllers' Registry; Nemil is obliged to prepare and comply with a Policy regarding maintaining and deletion, disposal or anonymization of personal data if deemed necessary in accordance with Data Inventory. Nemil has prepared this Policy in order to fulfill these obligations within this scope.

3.3. Following principles shall apply in storage and annihilation of personal data:

3.3.1. Nemil shall comply with the general principles of Law on Protection of Personal Data Article 4 and Article 7 of the regulation.
3.3.2. Nemil acknowledges that the preparation of this Policy alone does not imply that Personal Data is deleted, destroyed or anonymized in accordance with Law and related regulation.
3.3.3. Nemil declares that it shall store, delete, destroy or anonymize personal data in accordance with the security measures under Article 12 of Law and concerned regulations. We, as Nemil Turizm Tekstil A.Ş, are well aware of our responsibility for the security and legal protection of personal data which is regulated as a constitutional right and we place a great importance on the confidentiality and security of your personal data processes within our Company.

4) RECORDING MEDIA

4.1. Nemil, hereby agrees to include the personal data in the following environments in addition to any other media which may contain personal data within the scope of this Policy:

4.1.1. Computer and servers which are used on behalf of Nemil,
4.1.2. Network devices,
4.1.3. Shared / non-shared disk drives used for storing data on the network,
4.1.4. Cloud systems,
4.1.5. Mobile phone memory,
4.1.6. Paper,
4.1.7. Microfiche,
4.1.8. Peripheral units such as printer, fingerprint reader,
4.1.9. Flash disks,
4.1.10. Manuel data recording systems (survey forms, visitor register books)
4.1.11. Any printed and visual media.

5) CONDITIONS REQUIRING STORAGE AND DISPOSAL OF PERSONAL DATA

5.1. Personal data of data subjects are stored securely in the physical or electronic media mentioned above within the limits specified in Law and other relevant legislation by Nemil for the purposes mentioned below:

(I) For the fulfillment of legal obligations,

(ii) In the interest of commercial activities,

(iii) Planning and performing of employee rights and benefits,

(iv) Managing customer relations.

The personal data we acquire is stored safely in physical or electronic environment for an appropriate period to allow Tekfen Holding perform its business activities

Conditions that requires storage are as follows:

a.If it is necessary to process the personal data belonging to the parties to the contract, provided that it is directly related to the formation or enforcement of a contract.
b. If the storage of personal data is deemed necessary for the establishment, use and protection of a right,
c. If it is necessary to process data for the legitimate interests of Nemil
provided that it does not damage the fundamental rights and freedoms of the data subject..
d. If it is mandatory for Nemil to fulfill its legal obligations,
e. If it is explicitly stipulated in the Law,
f. Explicit consent of the personal data subject for the processing of its personal data in circumstances requiring explicit consent

5.2. In case of a violation occurring within the scope of the issues stated below, Nemil shall consider this as a security violation and take the necessary measures. Nemil shall take any kind of technical and administrative measures in order to ensure safe storage of personal data and to prevent unlawful processing of and access to personal data.

5.2.1.In case of illegality

Nemil undertakes that it will not process any personal data in contradiction with the manner specified in the Law. Unless "Conditions for Processing of Personal Data and Special Categories of Personal Data" under Article 5 & 6 of Law applies:

a. Nemil shall not preserve personal data without obtaining the explicit consent of the data subject unless it is expressly permitted by Law.
b. In cases where special categories of personal data are processed, Nemil shall process this data in compliance with concerned regulations within the knowledge of Commission. Within this scope, Nemil shall take the adequate measures designated by the Board in accordance with Article 6/4 of the Law.

5.2.1.Disappearance of Reasons Which Require the Processing of Data

Nemil is obliged to be up-to-date regarding data processing conditions and it shares this responsibility with all its employees. Employees shall not process data if all of the conditions for processing personal data have ceased to exist. Nemil Information Technologies Department is obliged to delete, destroy or anonymize personal data in accordance with this Policy if such conditions cease to exist. Nemil acknowledges that conditions requiring processing of personal data are no longer valid in the following circumstances and circumstances specified within Regulation:

a.Amendment or repeal of the provisions of the relevant legislation which constitute the legal basis for processing personal data
b.In case the contract between the parties has never been established, the contract is invalid, the contact terminates automatically or in case of termination of the contract.
c.The personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
d.It does not comply with principles of bona fides (good faith) and lawfulness.
e.In case of data subject revoking their consent if the processing of personal data occurs only with the explicit consent of the person concerned,
f. Nemil accepting the referral made by the relevant person for deleting or terminating his personal data being processed based on rights she/he owns according to Article 11 of KVK Law
g.Following the application of the above-mentioned person, the person concerned complains to the Council due to the conditions specified in the law and the Council approves the request of the person concerned
h.Maximum period requiring storage of personal data to be expired and being no purpose-conditions to enforce longer storage of personal data

In accordance with Regulation, the personal data of Data Subject shall be deleted, destructed or anonymized in the cases mentioned above by Nemil ex officio or upon the request of Data Subject.

6) MEASURES TAKEN FOR STORING, PROCESSING AND DISPOSAL OF PERSONAL DATA

In order to ensure personal data is lawfully maintained, processsed and accessed; Nemil is taking any technical and administrative measures depending on the personal data, technological capability and implementation cost.

6.1.Technical and Administrative Measures

In accordance with the Law on Protection of Personal Data Article 12; To ensure maintenance of personal data, to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure disposal of personal data lawfully, Nemil is taking the measures listed below:

6.1.a.Administrative Measures:

Administrative measures taken by Nemil are listed below:

a.1. Limiting internal access to personal data stored within Nemil with only the employees who are required to access it depending on their job description. Nemil shall also take the importance and nature (whether it is sensitive data or not) of personal data into consideration when restricting access to said data.
a.2. In case of acquisition of personal data processed by others unlawfully, informing the concerned and the Board of this issue as soon as possible,
a.3. In connection with disclosure of personal data, signing data security agreements with whom personal data is disclosed to or ensuring data security through the provisions it shall include in such agreements.
a.4. Employing personnel experienced and knowledgeable about personal data processing and provides its personnel with necessary Law on Protection of Personal Data training,
a.5. Conducting necessary internal controls in order to ensure the enforcement of the provisions of the Law in its own establishments and organizations and taking necessary action in case of any confidentiality and security gap.

6.1.b.Technical Measures:

Technical measures taken by Nemil are listed below:

b.1. Conducting necessary internal controls under the systems established,
b.2. Conducting risk analysis, data classification, IT risk assessment and business impact analysis processes under the systems established,
b.3. Providing of the technical infrastructure that shall prevent and/or monitor leakage of personal data out of house and creation of relevant matrices,
b.4. Providing control of system vulnerabilities by taking penetration test service regularly and whenever it is deemed necessary,
b.5. Ensuring controlling of authorizations of employees of information technologies units to personal data.
b.6. Ensuring personal data is destroyed in a way that cannot be retrieved or leaves no audit trail.
b.7. Protection of any digital media in which personal data stored by encrypted or cryptographic methods to ensure information security requirements in compliance with Article 12 of Law.

6.2. Audit of the Measures Taken to Protect Personal Data

In compliance with Article 12 of Law, Nemil carries out the necessary audits or has the necessary audits performed by the Committee established within the organization. The audit results are reported to the relevant department within the scope of the internal operation of the Company and necessary actions are taken to improve the measures taken.

7) UNAUTHORIZED DISCLOSURE OF PERSONAL DATA

Nemil shall follow the procedure determined in this Policy in the event of a breach of personal data security obligations which is specified in Law, concerned regulations and this Policy.

7.1. Violations Emergent within Nemil

If a Nemil employee detects a violation or encounters a potential violation, he/she immediately informs the relevant department director of the situation and informs the department manager about how the violation was discovered and where it originated. The Department director shall take the first steps to stop the breach if it is ongoing and to determine the extent to which it has ended, and shall notify Commission President of the situation. Commission President gets support from the IT department to take action against the breach and contacts the legal department. reports the extent, scope and consequences of the breach and shares it with the Board of Directors and the Authority.

7.2. Violations by Third Partie

Commission President shall contact the legal department and, if necessary, the IT department within 12 hours following the notification if a third party with whom Nemil works detects a breach or encounters a

possible breach. Commission President reports the information obtained from the other party about the extent, scope and consequences of the breach and shares it with the Board of Directors and the Authority.

8) DISPOSAL OF PERSONAL DATA

Disposal of Personal Data may be attained with three different methods which is: Erasure, Destruction and Anonymization. The purpose of the destruction process is not to be able to identify the real person with the remaining data in any manner.

Nemil shall take all manner of technical and administrative measures in order to ensure the erasure, destruction or anonymization of personal data is conducted in accordance with Regulation.

8.1.Erasure of Personal Data

Deletion of personal data which is processed by fully or partially automatic means is the process of making personal data inaccessible to and not-usable by the relevant users. Data Controller shall explain how the conditions set out in Article 7(3) of the Regulation are met in relevant policies and procedures. Deletion of Personal Data that forms part of any Data Recording System and processed by non-automated means and the process of making Personal Data Anonymous, which is not required in paper form, which is transferred to the electronic media by scanning or without digitization, are done in cases where Nemil processes the data completely or automatically; when Nemil deletes Personal Data, it makes the data inaccessible or reusable in any way. Nemil guarantees that the data cannot be accessed or reused by any user while performing this operation. This warranty is under the responsibility of Nemil.

Deletion methods listed above are subject to the Regulation and it is the responsibility of Nemil to update them in the relevant cases.

8.2.Destruction of Personal Data

Destruction methods shall apply in cases personal data is processed in physical recording media. Nemil is obliged to ensure this data inaccessible, not-reusable and impossible to recover. During the destruction process, Nemil employees and the related departments are obliged to inform the Commission of the relevant data to be destroyed. Following this, Nemil shall take any necessary technical and administrative measures.

8.3.Anonymization of Personal Data

The anonymization of personal data which is processed by Nemil by fully or partially automatic means is to make it impossible for such data to be associated with any identified or identifiable person in any way, even if the personal data is matched with other data.

Anonymization of personal data is the task of the business unit having the data within the Nemil. The business unit having the data may get support from different departments of Nemil, provided that the audit is done by itself for the destruction of the data. Nemil may apply the methods within this Policy regarding anonymization of Personal Data. The Commission should be consulted in cases where the accuracy of the procedure cannot be guaranteed.

9) DISPOSAL PROCESS AND METHODS OF PERSONAL DATA

Although it is processed according to the related law clauses, in the case of the disappearance of reasons which require processing, based upon our Company's own decision or on the demand of the owner of the personal data, personal data is deleted, destructed or anonymize in accordance with the related regulations with the methods stated below.

9.1.Personal Data Deletion Methods

General principles regarding the methods of deletion of personal data by Nemil is listed below:

Secure Deletion from Software	While deleting the data which is processed with entirely or partially automatic methods and stored in digital media; methods concerning the deletion of the data from the software in a way which will make it inaccessible and non-reusable for related users, are used.

Secure Erase by an Expert	In some cases, it can agree with an expert to delete the private data on its behalf. In this case, private data is security deleted by a person who is expert at it in a way that makes it inaccessible and non-reusable anyways for Related Users.
Darkening of Personal Data on Paper (Black-out method)	It is the method of removing the related private data physically from the document by cutting or making it invisible by using a constant ink in a way that cannot be recycled and cannot be read with technologic solutions in order to prevent the misuse of private data or to delete the data which is requested to be deleted.

Secure Deletion from Software; deletion the personal data in its cloud system by giving the delete command; removal of the user's access rights on the file or directory on the central server; deletion of related rows in database by database commands or deleting the data on the portable media, ie flash media, when using the appropriate software can be considered within this scope.

9.2.Personal Data Destruction Methods

Nemil employees shall perform destruction of personal data by selecting the appropriate method within the methods listed below:

Overwriting	The overwriting method is a data disposal method that aims to render the old data unrecoverable and achieve data sanitization by using zeros and ones (at least seven times) to overwrite data on magnetic media and rewritable optical media by means of special software.
Magnetizing	It is the process of placing the magnetic media in a high value magnetic field in order to make the data on it unreadable. It should be noted that if this method does not succeed, the only way to complete the destruction progress is to destroy the data in a physical manner.
Physical Destruction	Private data, on the condition of being a part of a data recording system, can also be processed with non-automatic ways. While these kinds of data are being purged, system of purging private data physically in a way that cannot be used later is applied.
Cloud Systems	It is the process of destroying all copies of the encryption keys of Personal Data after notification of the destruction of Personal Data held on cloud systems is made to the contracted service provider.
Destruction of Personal Data in Environmental Systems	Printer, door entry turnstile, network devices, mobile phones et cetera. It is used for the destruction of personal data contained in such environments. Such disposal must be carried out before the devices are subjected to backup, maintenance and similar operations.

Destruction of Personal Data in Paper and Microfiche Media	The main media is destroyed because the personal data in those media is permanently and physically overwritten. During this process, the media is divided into small pieces of an incomprehensible size with paper Destruction or clipping machines, if possible horizontally and vertically, so that it cannot be combined back.

9.3.Personal Data Anonymizing Methods

General principles regarding the methods of anonymization of personal data by Nemil is listed below:

Anonymization Methods That Do Not Provide Value Irregularity	Anonymization Methods That Provides Value Irregularity	Statistical Methods To Strengthen Anonymization
1.Removing Variables It is an anonymizing technique provided by deleting one or more of the variables from the table completely. In this case, the entire column in the table will be removed completely.	**1. Micro Combination** In this method, all the records in the data set are first sorted in a meaningful order and then the whole set is divided into a certain number of subsets. Then, by averaging the value of each subset of the specified variable, the value of the subset of that variable is replaced by the mean value. Thus, the average value of that variable that applies to the entire dataset will not change either.	**1.K-Anonymity** K-Anonymity has been developed to prevent the disclosure of information specific to individuals who show singular characteristics in certain combinations by enabling the identification of more than one person, with specific fields in a dataset. If there are more than one record of a combination created by combining some of the variables in a data set, the probability of identifying the individuals corresponding to this combination is reduced.
2. Removing Records In this method, anonymity is strengthened by removing a line containing a singularity in the data set and the possibility of producing assumptions about the data set is reduced.	**2. Data Exchange** The data exchange method is record changes obtained by exchanging values of a subset of variables between pairs selected from among records. This method is mainly used for categorizable variables, and the main idea is to transform the database by changing the values of variables between records or individuals.	**2.L-Diversity** L-diversity method is formed upon the studies on weaknesses of K-anonymity method. The L-diversity method takes the diversity of sensitive variables corresponding to the same variable combinations into consideration thus excelling K-anonymity.
3.Regional Concealment In the regional concealment method, the goal is to make the dataset more secure and reduce the risk of predictability. If the combination of values of a particular record creates a very little visible situation, and this can likely cause that person to become distinguishable in the group concerned, the value that creates the exceptional situation shall be changed to “unknown”.	**3. Noise Injection** With this method, additions and subtractions are made to provide distortions in a selected variable to the specified extent. This method is most often applied to datasets that contain numeric values. Distortion is applied equally at each value.	**3.T-Closeness** The process of calculating the degree of closeness of personal data, values and anonymizing the data set into subclasses according to these closeness degrees is called the T-closeness method.

4.Generalization It is the process of converting personal data from a customized value to a more general value. The new values obtained as a result of the generalization process show the total values or statistics of a group, making it impossible to identify the person concerned.		
5. Lower and upper bound coding The upper and lower bound encoding method defines a category for a given variable, and combines the values left in the grouping created by that category. In general, the lower or higher values in a particular variable are gathered together and these values are progressed by making a new definition.		
6.Global Coding The Global encoding method is a grouping method used in datasets where lower and upper bound encoding is not feasible, does not contain numeric values, or has values that cannot be sorted numerically. It is generally used in cases where certain values are grouped together, making it easier to make predictions and assumptions. All records in the data set are replaced with this new definition by creating a common and new group for the selected values.		
7.Sampling The sampling method describes or shares a subset taken from the cluster instead of the whole dataset. This reduces the risk of producing accurate estimates of individuals because it is not known whether a person who is known to be involved in the whole data set is included in the described or shared sample subset. Simple statistical methods are used to determine the subset of sampling.		

10) RETENSION AND DISPOSAL PERIODS

10.1. Periodical Destruction and Legal Retention Durations

Physical and digital data that expires the legal retention periods are periodically destroyed within the intervals stipulated by the legislation.

Nemil shall delete, destruct or anonymize the personal data in the first periodic demolition process following the date of its obligation to delete, destruct or anonymize the personal data. Periodic destruction shall be carried out at 6-month intervals for all personal data.

Legal destruction and retention periods which shall be taken as the basis during the periodical destruction are defined in Annex 1 of this Policy. Nemil reserves the right to store Personal Data arising from other legal obligations.

10.2. Deletion and Disposal Process upon Data Subject's Request

When a data subject requests for the deletion or destruction of his/her personal data by applying to Nemil, Nemil shall evaluate the current state of the conditions for processing Personal Data and takes related actions accordingly.

If all of the conditions for processing personal data have ceased to exist; the data controller deletes, destroys, or anonymizes the personal data subject to the request. Nemil finalizes the request of Data Subject within thirty days at the latest and inform Data Subject.

If all of the conditions for processing personal data have ceased to exist and personal data of the data subject has been transferred to a third party, Nemil shall notify the third party of this situation; and make sure that the third party shall carries out the necessary procedures within the scope of Regulation.

If all of the processing conditions of the personal data have not ceased to exist, data subject's request may be rejected by Nemil explaining the reasons in accordance with the third paragraph of Article 13 of the Law. Data Controller shall send a response to the data subject within 30 days of the request in written or electronic form.

11) AMENDMENT TO THE POLICY

11.1 In case of any official amendments to the relevant legislation, Nemil may make amendments to this Policy with the approval of the Board of Directors in accordance with these changes. In case of any discrepancy between the KVKK, the provisions of other relevant legislation and this Policy, the KVKK and the provisions of other relevant legislation shall prevail.
11.2. Nemil shall share the updated version of the Policy and any amendments to the Policy with its employees via e-mail corporate network in a reviewable manner.

12) EFFECTIVE DATE OF THE POLICY

This version of the Policy on Storage, Destruction and Anonymization of Personal Data prepared by Nemil is effective as of 01/11/2019 upon the approval of the Board of Directors of Nemil Turizm Tekstil A.Ş.

13) OTHER ISSUES

In the case of any discrepancy or inconsistency between Law on Protection of Personal Data and other related regulations and this Policy, Law on Protection of Personal Data and related regulations shall take precedence.

This policy prepared by Nemil entered into effect as per separate decisions taken by the Board of Directors of Nemil Turizm Tekstil A.Ş.