GÜROK TURİZM VE MADENCİLİK A.Ş.
PERSONAL DATA STORAGE AND

DESTRUCTION POLICY

April 2019
İstanbul

Table of Contents

I. Purpose and Scope of the Policy

Gürok Turizm ve Madencilik A.Ş., which was incorporated as a joint stock company pursuant to the Turkish Commercial Code No. 6102 (hereinafter referred to as "Gürok") and acting as a data controller, aims to fully comply with all kinds of legal regulations regarding the protection and lawful processing of personal data.

The purpose of this Personal Data Storage and Destruction Policy ("the Policy"), which is prepared within the scope of Article 16 of the Law on Protection of Personal Data No. 6698 and Article 5 of the Regulation on the Deletion, Destruction or Anonymization of Personal Data, is to determine the required storage periods and the minimum standards to be regarded in the destruction of personal data which is processed by Gürok and belong to customers purchasing/receiving products and services, employees, employee candidates and other third parties.

This Policy provides the basis for determining the maximum time required for the processing of data by data controller, Gürok, in line with the purpose of processing as well as for deleting, destroying and anonymizing the data.

This Policy will apply to all business units, processes and business relationships with other third parties. This Policy will apply to all Company executives, employees, consultants, service providers or service providers that may collect, process or access data (including personal data and/or qualified personal data).

This Policy will apply to all personal data and information collected by the Company. Electronic and non-electronic recording media and/or documents where personal data covered by this Policy are stored are as follows:

- Servers (domain, backup, e-mail servers, database, web, file sharing etc.)
- Software (office software, portal etc.)
- Information security devices (firewall, attack detection and blocking, log files, anti-virus software etc.)
- Personal computers (desktop, laptop)
- Mobile devices (smartphones, tablets etc.)
- Optical discs (CD, DVD, Blu-Ray etc.)
- Removable memories (USB, Memory Card, Portable Memory etc.)
- Printer, scanner, photocopy device.

- Information and documents in printed media,
- Video files and audio recordings,
- Data produced by physical access control systems.

II. Applicable Legislation and Other Documents

- Law No. 6698 on Protection of Personal Data
- Regulation on the Deletion, Destruction or Anonymization of Personal Data dated 28 October 2017
- Regulation on Registration of Data Controllers dated 30 December 2017
- Communiqué on Procedures and Principles to Be Followed in Fulfilling Obligation to Inform dated 10 March 2018

- Turkish Code of Obligations no. 6098
- Labor Law no. 4857
- Social Insurance and General Health Insurance Law no. 5510
- Occupational Health and Safety Law no. 6361
- Law no. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts

- Gürok Policy on Personal Data Protection and Processing
- Gürok Policy on Processing Qualified Personal Data
- Gürok Clear Desk & Clear Screen Policy
- Gürok Procedure on PPD Law - Data Subject Application
- Gürok Procedure on Employee Communication & Use and Inspection of IT Tools

III. Definitions

The terms in this Policy will have the meanings ascribed to them below.

Term	Definition
Recipient Group	The category of natural or legal persons to whom personal data is transferred by the data controller
Explicit Consent	Consent to a specific subject, based on information and explained with free will
Anonymization	Making the personal data unfeasible to be matched with an identified or identifiable real person's personal data
Data Subject	Real person whose personal data is processed
Data Processor	Persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller except for the person or unit responsible for the technical storage, protection and backup of the data
Destruction	Deleting, destroying or anonymizing personal data
Law or PPD Law	Law No. 6698 on Protection of Personal Data
Storage Media	Any medium where personal data processed by non-automated means are stored provided that they are fully or partially automated or as part of any data recording system
Personal Data	Any information about an identified or identifiable real person
Personal Data Processing Inventory	Inventory created associated to the personal data processing purposes, the data category, the recipient group transferred, and the data subject group in which data officers detail their personal data processing activities in line with their business processes by explaining the maximum time required for the purposes for which

	the personal data are processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security
Processing of Personal Data	Any action put into practice on the personal data such as the acquisition, recording, storage, retention, modification, reorganization, disclosure, transfer, acquisition, availability, classification or prevention of personal data by fully or partially automated means or by non-automated means provided that they are part of any data recording system.
Board	Personal Data Protection Board
Authority	Personal Data Protection Authority
Qualified Personal Data	Information related with individuals' race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and outfit, association, foundation or union membership, health status, sexual life, criminal conviction records and security measures as well as their biometric and genetic data
Periodic Destruction	It is the process of ex-officio and recurrently deleting, destroying or anonymizing the personal data in the event that all the conditions specified in the policy requiring the processing, storing and destroying of personal data in the law cease.
Company or Gürok	Gürok Turizm ve Madencilik Anonim Şirketi
Data Processor	Real or legal person who processes personal data on his/her behalf based on the authority provided by the data controller
Data Registration System	Registration system in which personal data is processed in accordance with certain criteria
Data Controller	Real or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data registration system

Data Controller Registry Information System (VERBİS)	Information system which can be accessed over the internet that is created and managed by the Authority to be used in applying for and other transactions related to the registry.
Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data dated 28 October 2017

IV. General Storage Principles

Storage Period

The company defines and updates the relevant storage period for documents and electronic records that should be stored during the personal data storage period pursuant to the Storage and Destruction Period Table in Annex-1.

Unless otherwise stated in this Policy and its annexes, the Company, as a rule, stores the personal data included in the data categories defined in the Personal Data Processing Inventory for the periods specified in Annex-1 as of the date when the relevant personal data is collected.

Data storage periods may exceptionally be extended if:

- requested by any research or investigations carried out by official authorities. and/or where required by the Company's legal obligation or legal rights;

- it is necessary to exercise the rights under applicable legislation as part of the proceedings or other legal processes.

While determining the maximum storage period required for the purpose for which the personal data is processed;

- The period accepted as a general practice in the industry in which the company operates regarding the purpose of processing the relevant data category,

- The duration of the legal relationship established with the data subject which requires the processing of personal data in the relevant data category,

- The period that the legitimate interest to be obtained by the Company will be valid in accordance with the law and the rules of integrity depending on the purpose of processing the relevant data category,

- The period during which the risks, costs and responsibilities of data storage will legally continue depending on the purpose of processing the relevant data category,

- Whether the maximum period to be determined is suitable for keeping the relevant data category accurate and up-to-date when necessary,

- the period during which the Company has to store personal data in the relevant data category due to its legal obligations,

- The timeout period determined by the Company to assert a right based on personal data in the relevant data category,

are all taken into consideration.

The Company will monitor whether the information contained in the Personal Data Processing Inventory complies with the period required in line with the purpose of processing personal data and whether the maximum periods have been exceeded. Regarding the personal data processed within the scope of its activities, the Company will give place:

- to the storage periods related to all personal data within the scope of activities performed in Personal Data Processing Inventory based on the nature of personal data;
- to the storage periods on the basis of data categories in VERBİS;
- to the storage periods on the basis of processes in the Policy on Storage and Destruction of Personal Data

These storage periods are updated, if necessary. Personal data, whose storage period have expired, are ex officio deleted, destroyed or anonymized.

Storage Rules and Precautions

In the process of storing personal data, the possibility of wearing out of the data medium (printed, digital, etc.) used for storage or archiving of relevant personal data should be taken into consideration. If it is preferred to store personal data electronically, access to network components is granted only to the authorized persons, provided that this authorization is limited with the storage period.

Personal data stored in corporate devices or in the form of paper are protected against threats such as theft or loss of these devices and papers via physical security measures. Likewise, physical environments in which personal data are stored are protected against external risks (fire, flood etc.) by appropriate methods. Entries/exits to these areas should be subject to control measures.

Precautions of the same level are also put into effect for papers, electronic media and devices that are physically outside the Company but contain personal data belonging to the Company.

The precautions that are taken to ensure the security of personal data processed by the Company include the following:

- With penetration tests, the Company exposes risks, threats, weaknesses and vulnerabilities, if any, to the information systems and takes necessary measures.

- The risks and threats that will affect the sustainability of the information systems are constantly monitored by the Company.

- Access to information systems and authorization of users is provided through access and authorization matrix in line with security definitions.

- Necessary measures are taken for ensuring the physical security of the company's information systems, equipment, software and data.

- In order to ensure the security of information systems against environmental threats, both hardware based (access control system that allows only

authorized personnel to access the system room, 7/24 personnel monitoring system, ensuring the physical security of the edge switches forming the local area network, fire extinguishing system, air conditioning system etc.) and software based (firewalls, hacker prevention systems, network access control, systems that prevent harmful software etc.) measures are taken.

- Risks that may cause unlawful processing of personal data are identified; appropriate technical measures to prevent these risks are executed and duly monitored.

- Data access procedures are established within the Company and regular reporting and analysis on access to personal data are carried out.

- Access to storage areas where personal data are kept is recorded, improper access or access attempts are kept under control and reported.

- The company takes the necessary precautions to ensure that the deleted personal data inaccessible and not reusable for the users concerned.

- In the event that personal data are illegally acquired by others, the procedure in Annex 2 has been adopted by the Company and a system and infrastructure has been created accordingly in order to report this situation both to the data subject and the Board.

- Security vulnerabilities are monitored, appropriate security patches are installed and information systems are kept up-to-date.

- Strong passwords are used in electronic environments where personal data are processed.

- Secure logging systems are used in electronic environments where personal data are processed.

- Data backup programs which ensure the safe storage of personal data are used.

- Access to personal data stored in electronic or non-electronic environments is restricted in accordance with access principles.

- A specific policy titled "**Policy on Processing Qualified Personal Data**" has been adopted for the security of qualified personal data.

V. Information Security Measures

The following policies and procedures regarding information security measures, precautions and steps to be taken have been adopted in the Company and put into effect upon approval by the Board of Directors:

Policies:

1- Information Security Policy
2- Access Control Policy
3- Network Policy
4- Cryptographic Controls and Key Management Policy
5- Safe System Development Policy
6- Remote Work Policy
7- Equipment and Media Security Policy
8- Acceptable Use Policy
9- Information Exchange Policy
10- Password Management Policy
11- Physical and Environmental Security Policy
12- Privileged Access Rights Management Policy

Procedures

1- Asset Management Procedure
2- Incident Violation Management Procedure
3- IT Projects Management Procedure
4- Social Media Usage Procedure

Forms and Other Documents

1- Data Destruction Form
2- Access Authorization Matrix

3- Company Computer Allocation and Usage Instruction
4- Corporate Phone Line and Telephone Allocation and Usage Instruction

VI. Destruction of Personal Data

General Conditions for the Destruction of Personal Data

In cases the purposes that require the processing of personal data cease, personal data are ex officio deleted, destroyed or anonymized by the Company in line with the instructions of the Data Subject. Therefore; in the event that

- relevant legislation provisions that constitute the basis for processing personal data are either amended or annulled,
- the contract between the Company and the Data Subject has never been established, the contract is not valid, the contract ends automatically, the contract is reneged on,
- the purpose requiring the processing of personal data cease,
- processing personal data is against the law or the integrity rule,
- data subject withdraws his/her former consent which has been duly obtained in order to process personal data occurs only on the condition of explicit consent, the relevant person's withdrawal of his consent,
- the Company accepts the objection of the Data Subject regarding the processing of personal data within the framework of the rights granted as of Article 11 (e) and (f) of the Law,
- tha Data Subject submits the complaints to the Board on the grounds that he/she had objected the Company with a request on the deletion or destruction of his/her personal data however the Company had refused such an objection or claiming that the reply by the Company is evaluated as not satisfactory or the Company failed to respond within the period stipulated by Law, and this request is approved by the Board,

- the conditions justifying the storage of personal data have already ceased although the maximum period for the storage of personal data has not yet expired,

- The elimination of the conditions stipulated in Articles 5 and 6 of the Law that require the processing of personal data,

personal data should be deleted, destroyed or anonymized.

Personal Data Destruction Techniques

Deletion of Personal Data; is the process of making relevant personal data inaccessible and unusable for the users concerned. The Company ensures that the deleted personal data is no longer accessible and reusable by the respective users.

The process of deletion of personal data by the Company is as follows:

- Identifying the personal data to be deleted;

- Identifying the relevant authorized users for each personal data using the access authorization and control matrix or a similar system;

- Identifying whether the relevant users have the authority and opportunity to access, retrieve or reuse the data;

- The cancellation and termination of the access, retrieval, reuse authorization and methods of the relevant users to the personal data.

Depending on the media in which they are recorded, the personal data are deleted as follows:

- For the personal data stored on the servers whose required storage period has expired, the system administrator terminates the authorized access of the users and deletes such data.

- For the personal data stored on electronic media whose required storage period has expired, the personal data is made inaccessible and unusable for all employees (relevant users) except for the database manager.

- For the personal data stored on physical media whose required storage period has expired, the personal data is made inaccessible and unusable for all employees except for the archiving manager. In addition, obscuration is applied by scratching/covering/ erasing the data in an unreadable manner.

- For the personal data stored on a portable media whose required storage period has expired, data is encrypted by the system administrator and access is granted to the system administrator only or stored in secure environments with encryption keys.

Destruction; is the process to destroy all physical recording media where the information is stored and is suitable for further data storage in a way so that such data cannot be retrieved and used again.

Depending on the media in which they are stored, the personal data are destroyed as follows:

- For the personal data stored on a printed media whose required storage period has expired, data is irreversibly destroyed via paper clippers.

- For the personal data stored on an optical or magnetic media whose required storage period has expired, the data is physically destroyed by melting, burning or pulverizing. In addition, the data on it is rendered unreadable by putting it through a device specific to magnetic media and exposing it to a high degree magnetic field.

Anonymization of personal data; is a process where it is rendered unrelated to an identified or identifiable real person even if it is matched with other data. In this context, if the data still matches with other data and if the data subject can still be understood even after the transaction, this data cannot be considered as anonymous.

Anonymized data will no longer be subject to the provisions of the Law as it will no longer have personal data qualifications. Since the data sets have personal data qualifications until the moment they are subjected to an anonymization any transaction to be performed on these data will be considered as the processing of personal data.

All actions regarding the deletion, destruction and anonymization of personal data are recorded and such records are kept confidential for at least three years except for the requirements of other legal obligations.

Periodic Destruction

Personal data processed by Gürok are subject to periodic destruction every 6 (six) months as of the first day of the relevant calendar year in accordance with Article 11 of the Regulation on the Deletion, Destruction or Anonymization of Personal Data.

As of the first periodic destruction transaction following the date on which the obligation to delete, destroy or anonymize personal data is due, personal data are deleted, destroyed or anonymized pursuant to this Policy.

In the event that Data Subject requests the deletion or destruction of his/her personal data by applying to the Company pursuant to their rights as per Article 13 of the PPD Law;

- If all the conditions requiring the processing of personal data have ceased, the company deletes, destroys or anonymizes the personal data in line with the data subject's request. The company finalizes the request of the Data Subject within thirty days at the latest and duly informs the Data Subject.

- If all the conditions requiring the processing of personal data have ceased however the personal data subject to the request have been transferred to third parties, the Company reports this situation to the third party and ensures the execution of necessary actions within the scope of this Policy and related legislation on behalf of the third party.

- If all the conditions requiring the processing of personal data have not ceased, this request may be rejected by the Company by explaining its justification

pursuant to the third paragraph of Article 13 of the Law and the negative response is then notified to the Data Subject in writing or electronically within thirty days at the latest.

VII. Policy Owners

Units and related employees using/managing the systems in which the personal data are kept, processed and/or transferred are responsible for the preparation, updating and implementation of this Policy. In this context, all units and employees of the Company actively support responsible units to appropriately execute the technical and administrative measures taken by the responsible units under the Policy, to train and raise awareness of unit employees, to prevent unlawful processing of personal data through monitoring and continuous supervision, to prevent personal data from being illegally accessed and take technical and administrative measures to ensure data security in all environments where personal data is processed in order to ensure that personal data are stored in a lawful manner.

Human Resources Department, in particular, is obliged to ensure that employees comply with the policy and IT Department is responsible for providing the technical solutions needed for the implementation of the policy. Both of these units are also authorized and responsible for the development, implementation, publication and updating of the Policy.

VIII.Compliance with the Policy

All Company employees are obliged to fully and properly comply with the provisions of the Policy during the processing and storage of personal data, and the aforementioned policy is an integral part of the employment contracts of employees.

In case there are concrete signs that indicate any breach of the provisions in this Policy, the Company's executive body investigates suspected cases of breach and takes necessary measures. Failure to comply with this Policy may result in various unfavorable consequences, including but not limited to, loss of customer confidence, litigation, loss of prestige, financial loss and damage to Company reputation or any personal damage. For this reason, failure to comply with this Policy in any way

howsoever may result in disciplinary investigations or termination of business or employment contract concluded with Company employees or other interested persons. Such breach may also lead to legal proceedings against those involved.

IX. Enforcement

This Policy, which is prepared with a view to ensure full compliance with the applicable legislation in the processing of personal data, was approved by the resolution of Board of Directors of Gürok Turizm ve Madencilik Anonim Şirketi on ... /… / 2019 and entered into force accordingly.

The policy is published in two different media: printed paper and electronic media. Electronic copy is communicated internally to the employees electronically, while the printed copy is kept in the Human Resources Department. The policy is revised as needed and relevant sections are updated when necessary.

Annex-1: Table on Storage and Destruction Period

Related Process and Data Category	Storage Period	Explanation
Personal health status of employees	5 years following the end of the business/employment relationship	They are kept during the term of employment and for a period of 5 years following the expiry of employment contract in the event of detecting and reporting possible occupational diseases/occupational accidents.
Employee recruitment files, personal data	20 years following the end of the business/employment relationship	The data used to establish any business/employment Contract are kept throughout the employment relationship or for 20 years following the end of the business/employment relationship based on a request for determining a possible service/fee and a claim from the Social Security Institution.
Employee, candidate application forms, resumes	For 1 year as of the date of application	They are kept for as long as the CVs and application forms will be outdated; in any way for a maximum of 2 years.
Personal data acquired within the scope of occupational health and safety practices	15 years following the end of the business/employment relationship	They are kept for 15 years following the end of the business/employment relationship against any claim of health problem within the scope of the responsibilities imposed by the employment contract to the parties.
Potential customer information	For 2 years as of the date of acquiring such	In order to establish a sales contract, the data acquired

	information	from prospective customers are kept for 2 years.
Data acquired through managing customer claims and complaints	For 1 year as of the date of the first registration	Personal data acquired in order to improve the quality of the service and to assess customer claims are stored for 1 year as of the date of the first registration.
Records of Financial Transactions/Payments	10 years following the end of the business/employment relationship	Data acquired in order to pay wages to employees in line with the obligations imposed by employment contracts are kept for 10 years.
Information disclosed to companies/ institutions in cooperation with Gürok Turizm ve Madencilik Anonim Şirketi	Throughout the employment relationship and 10 years following the expiry of the employment relationship	The data disclosed throughout the employment contract are kept throughout the employment relationship and for 10 years, which is specified as the contract timeout, following the expiry of the employment relationship.
Personal data of subcontractor employees	10 years following the expiry of the business contract	The personal data of the employees of the companies that have a contractor/subcontractor relationship with the Company are kept for 10 years in accordance with the contractual relationship.
Personal data included in a sales contract	10 years following the expiry of the business relationship	Data are kept throughout the time-out period against any disputes that may arise from the Contract.
Personal data acquired in line with the contracts signed with third parties	10 years following the expiry of the business contract	Data are kept throughout the 10-year time-out period based on the contractual relationship.
Security camera records	180 days	They are kept for six months, taking into account the duration of the complaint, in order to ensure workplace

		safety.
Visitors' and meeting participants' registries	2 years following the end of the event	The acquired data are kept for 2-year time-out period for wrongful acts against any adverse situations that may occur within the company due to security issues.
Data acquired as part of allocating vehicles to employees	5 years following the expiry of the employment contract	Personal data acquired within the scope of allocating vehicles to employees in order to fulfill their obligations arising from the business relationship are kept for 5 years, which is a time-out period in wage claims.
Data on wireless internet service usage	For 2 year as of the date of the first registration	Data acquired for the provision of internet access service is kept for 2 years as required by law.
Data kept under tracking systems for log records	For 2 years as of the date of acquiring such logs	Personal data obtained for the purpose of providing internet access service in a secure environment is kept for 2 years as required by law.
Information acquired from Gül Palas and Ali Bey Hotels & Resorts guests for hotel reservation/registration purposes	10 years following the expiry of the service procurement relationship	ID and contact information acquired within the scope of accommodation services are kept for 10-year contractual time-out period.
Information acquired from Gül Palas and Ali Bey Hotels & Resorts guests for hotel organization purposes	10 years following the expiry of the service procurement relationship	The data acquired in order to meet the demands of the hotel guests with the services provided within the context of the contract are kept for a period of 10 years.

Annex-2: Notification Procedure for any Breach of Personal Data

The phrase "as soon as possible" stipulated in the provision of paragraph (5) of Article 12 of the Law, which reads as "*In the event that the processed personal data are obtained by others in illegal ways, the data officer will notify this situation both to the Data Subject and the Board as soon as possible….*", will be interpreted as 72 hours.

In this context, Gürok will notify the Board without delay and within 72 hours at the latest after being aware of the breach. The relevant people will also be notified as soon as reasonably possible following the determination of the persons affected by the said data breach, either directly in case the contact address of the Data Subject can be reached, if not, by appropriate methods such as publishing the said data through the data officer's website.

In case Gürok fails to notify the Board within 72 hours on a justified basis, the reasons for the delay will simultaneously be explained to the Board along with the notification.

"Notification Form for any Breach of Personal Data", which can be accessed on the website of the Board, will be used in notifying the Board. In cases where it is not possible to submit the information in the form simultaneously, this information will incrementally be provided to the Board without delay.

Information, effects and precautions regarding data breaches will be recorded by Gürok and made available for review by the Board.

If the personal data held by the data processors processing data on behalf of Gürok are acquired by others in an illegal way, arrangements will be made in order to require the data processors to notify Gürok without any delay.

In the event of a Data Breach, the IT Department informs the business units affected by the breach and prepares a report on possible outcomes. It prepares an action plan for the necessary measures and steps to be taken and puts them into effect.