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.

GÜROK TURİZM VE MADENCİLİK A.Ş. RICHTLINIEN ZUR SPEICHERUNG UND VERNICHTUNG PERSÖNLICHER DATEN

April 2019
Istanbul

Inhalt

I. Zweck und Umfang der Richtlinie

Gürok Turizm ve Madencilik A.Ş., eine Aktiengesellschaft nach dem türkischen Handelsgesetz Nr. 6102. (im Folgenden "Gürok" genannt), ist als Datenverantwortlicher

bestrebt, alle gesetzlichen Bestimmungen zum Schutz und zur rechtlichen Verarbeitung

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 information	In order to establish a sales contract, the data acquired 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.

GÜROK TURİZM VE MADENCİLİK A.Ş. RICHTLINIEN ZUR SPEICHERUNG UND VERNICHTUNG PERSÖNLICHER DATEN

April 2019
Istanbul

Inhalt

I. Zweck und Umfang der Richtlinie

Gürok Turizm ve Madencilik A.Ş., eine Aktiengesellschaft nach dem türkischen Handelsgesetz Nr. 6102. (im Folgenden "Gürok" genannt), ist als Datenverantwortlicher bestrebt, alle gesetzlichen Bestimmungen zum Schutz und zur rechtlichen Verarbeitung personenbezogener Daten vollständig zu erfüllen.

Der Zweck dieser Richtlinie zur Aufbewahrung und Vernichtung persönlicher Daten ("Richtlinie"), die gemäß Artikel 16 des Gesetzes zum Schutz persönlicher Daten Nr. 6698 und Artikel 5 der Verordnung über die Löschung, Vernichtung oder Anonymisierung der persönlichen Daten erstellt wurde, besteht darin, die erforderlichen Aufbewahrungsfristen und die Vernichtung der von Gürok verarbeiteten persönlichen Daten zu bestimmen, die von Personen, Mitarbeitern, Kandidaten und anderen Dritten, die die Produkte oder Dienstleistungen von Gürok erhalten, erhalten wurden.

Diese Richtlinie bildet die Grundlage für die Bestimmung der maximalen Zeit, die für den Zweck, für den die personenbezogenen Daten von dem für die Datenverarbeitung Verantwortlichen Gürok verarbeitet werden, und für den Löschungs-, Vernichtungs- und Anonymisierungsprozess benötigt wird.

Diese Richtlinie gilt für alle Einheiten, Prozesse und Geschäftsbeziehungen mit anderen Drittparteien. Diese Richtlinie gilt für alle Führungskräfte, Mitarbeiter, Berater, Dienstleistungsanbieter oder Dienstleister des Unternehmens, die Daten (die persönliche Daten und/oder besondere persönliche Daten enthalten) sammeln, verarbeiten oder auf diese zugreifen können.

Diese Richtlinie gilt für alle persönlichen Daten und Informationen, die vom Unternehmen gesammelt werden. Elektronische und nicht-elektronische Aufzeichnungsmedien und/oder Dokumente, die mit dieser Richtlinie ausgegeben werden und persönliche Daten enthalten, sind wie folgt:

- Server (Domäne, Sicherung, E-Mail, Datenbank, Web, gemeinsame Dateinutzung usw.)
- Software (Bürosoftware, Portal usw.)
- Informationssicherheitsvorrichtungen (Firewall, Einbruchserkennung und -blockierung, Log-Datei, Antivirus usw.)
- Personal Computer (Desktop, Laptop)
- Mobile Geräte (Telefon, Tablett usw.)
- Optische Datenträger (CD, DVD, Blu-Ray usw.)
- Wechseldatenträger (USB, Speicherkarte, tragbarer Speicher usw.)
- Drucker, Scanner, Kopierer.
- Informationen und Dokumente in gedruckten Medien,
- Video- und Audioaufnahmen,
- Daten, die von physischen Zugangskontrollsystemen erzeugt werden.

II. Relevante Gesetzgebung und andere Dokumente

- Gesetz Nr. 6698 über den Schutz personenbezogener Daten
- Verordnung über die Löschung, Vernichtung oder Anonymisierung von persönlichen Daten vom 28. Oktober 2017
- Durchführungsverordnung über das Register der für die Verarbeitung Verantwortlichen vom 30. Dezember 2017
- Kommuniqué über die Verfahren und Grundsätze, die bei der Erfüllung der Beleuchtungsverpflichtung zu befolgen sind, vom 10. März 2018

- Türkisches Obligationenrecht Nr. 6098
- Arbeitsrecht Nr. 4857
- Sozialversicherungs- und allgemeines Krankenversicherungsgesetz Nr. 5510
- Arbeitsschutzgesetz Nr. 6361
- Gesetz Nr. 5651 über die Anordnung von Veröffentlichungen im Internet und die Bekämpfung der durch diese Veröffentlichungen begangenen Verbrechen

- Gürok Richtlinien zum Schutz und zur Verarbeitung personenbezogener Daten
- Gürok- Richtlinien der Verarbeitung besonders qualifizierter persönlicher Daten
- Gürok Sauberer Tisch und saubere Bildschirmrichtlinie
- Gürok- Antragsverfahren der betroffenen Person über das Gesetz zum Schutz personenbezogener Daten
- Gürok Mitarbeiter-Kommunikation & IT-Tools Nutzung und Kontrollverfahren

III. Definitionen

Die Begriffe in dieser Richtlinie beziehen sich auf die unten aufgeführten Bedeutungen.

Begriff	Erläuterung
Empfangende Gruppe	Die Kategorie der natürlichen oder juristischen Personen, an die personenbezogene Daten vom für die Datenverarbeitung Verantwortlichen übermittelt werden
Offene Zustimmung	Zustimmung, die auf Informationen zu einem bestimmten Thema beruht und die mit freiem Willen erklärt wurde.
Anonyme Kontaktaufnahme	Prozess des Abgleichs von persönlichen Daten mit anderen Daten, so dass diese nicht mit einer identifizierten oder identifizierbaren natürlichen Person in Verbindung gebracht werden.
Relevante Benutzer	natürliche Person, deren personenbezogene Daten verarbeitet werden Personen, die personenbezogene Daten innerhalb der Organisation des für die Datenverarbeitung Verantwortlichen oder gemäß der Genehmigung und Anweisung des für die Datenverarbeitung Verantwortlichen verarbeiten, mit Ausnahme der Person oder Einheit, die für die technische Speicherung, den Schutz und die Sicherung der Daten verantwortlich ist.
Vernichtung	Löschung, Vernichtung oder Anonymisierung persönlicher Daten
Gesetz oder Gesetz zum Schutz persönlicher Daten	Gesetz Nr. 6698 über den Schutz personenbezogener Daten
Registrierungs-Umgebung	Jede Umgebung, in der personenbezogene Daten mit Mitteln verarbeitet werden, die vollständig oder teilweise automatisiert oder nicht automatisiert sind, sofern sie Teil eines Datenaufzeichnungssystems sind.
Persönliche Daten	Alle Informationen über eine identifizierte oder identifizierbare natürliche Person.
	Das Inventar, das die Datenverantwortlichen auf der Grundlage ihrer Geschäftsvorgänge erstellen, indem sie ihre Tätigkeiten zur Verarbeitung personenbezogener Daten mit den Zwecken der Verarbeitung personenbezogener Daten, der Datenkategorie, der Gruppe der übermittelten Empfänger und der Gruppe der betroffenen Daten in Verbindung bringen und die maximale Zeit für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie das von den Datenverantwortlichen detaillierte Inventar angeben, in dem die für die Übermittlung ins Ausland vorgesehenen personenbezogenen Daten und die Maßnahmen in Bezug auf die Datensicherheit erläutert werden.

Verarbeitung personenbezogener Daten	Jede Handlung, die an Daten vorgenommen wird, wie z.B. das Verhindern der Erfassung, Aufzeichnung, Speicherung, Aufbewahrung, Änderung, Reorganisation, Erläuterung, Übertragung, Übernahme, Bereitstellung, Klassifizierung oder Verwendung von personenbezogenen Daten durch automatische oder teilweise Automatisierung oder durch nicht- automatisierte Mittel, sofern sie Teil eines Datenaufzeichnungssystems sind.
Ausschuss	Ausschuss für den Schutz personenbezogener Daten
Behörde	Behörde für den Schutz personenbezogener Daten
Besonders qualifizierte persönliche Daten	Daten über Rasse, ethnische Herkunft, politisches Denken, philosophische Überzeugungen, Religion, Sekte oder andere Glaubensrichtungen, Verkleidung und Kleidung, Mitgliedschaft in einer Vereinigung, Stiftung oder Gewerkschaft, Gesundheit, Sexualleben, strafrechtliche Verurteilung und Sicherheitsmaßnahmen sowie biometrische und genetische Daten einer Person.
Periodische Vernichtung	Prozess der Löschung, Vernichtung oder Anonymisierung der persönlichen Daten, der von Amts wegen in regelmäßigen, in der Richtlinie der Speicherung und Vernichtung von persönlichen Daten festgelegten Abständen durchgeführt wird, wenn alle gesetzlich vorgeschriebenen Bedingungen für die Verarbeitung der persönlichen Daten beseitigt sind.
Firma oder Gürok	Gürok Turizm ve Madencilik Anonim Şirketi
Datenverarbeiter	Eine natürliche oder juristische Person, die personenbezogene Daten in ihrem Namen auf der Grundlage der Genehmigung des Datenbeauftragten verarbeitet
Datenaufzeichnungs-System	Registrierungssystem, in dem persönliche Daten nach bestimmten Kriterien verarbeitet werden
Daten-Verantwortlicher	Natürliche oder juristische Person, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt und für die Einrichtung und Verwaltung des Datenaufzeichnungssystems verantwortlich ist.
Informationssystem für das Register der Datenbeauftragten (VERBİS)	Informationssystem, auf das über das Internet zugegriffen werden kann und das von der Behörde erstellt und verwaltet wird und das die Datenverantwortlichen für die Registrierung und andere damit zusammenhängende Transaktionen der Registrierung verwenden werden.
Verordnung	Verordnung vom 28. Oktober 2017 über die Löschung, Vernichtung oder Anonymisierung von personenbezogenen Daten

IV. Allgemeine Aufbewahrungsprinzipien

Aufbewahrungsfristen

Das Unternehmen definiert und aktualisiert die Zeitdefinition für Dokumente und elektronische Aufzeichnungen, die während der Aufbewahrungszeit persönlicher Daten in der Tabelle der Aufbewahrungs- und Vernichtungszeiten in Anhang-1 aufbewahrt werden sollten.

Sofern in dieser Richtlinie und ihren Anhängen nichts anderes angegeben ist, werden die in den Datenkategorien des Inventars der Firma zur Verarbeitung personenbezogener Daten enthaltenen personenbezogenen Daten in der Regel in den in Anhang-1 angegebenen Zeiträumen ab dem Zeitpunkt der Beschaffung der relevanten personenbezogenen Daten gespeichert.

Ausnahmsweise können die Aufbewahrungsfristen in den folgenden Fällen verlängert werden:

- Wenn dies für Untersuchungen oder Ermittlungen offizieller Behörden gefordert wird und/oder wenn es die gesetzliche Verpflichtung oder die gesetzlichen Rechte des Unternehmens erfordern;
- In Fällen, in denen es notwendig ist, die Rechte nach der geltenden Gesetzgebung in dem Verfahren oder in anderen rechtlichen Verfahren auszuüben.

Bei der Festlegung der maximalen Aufbewahrungsdauer, die für den Zweck, zu dem die personenbezogenen Daten verarbeitet werden, erforderlich ist, werden die folgenden Punkte berücksichtigt;

- Im Rahmen des Zwecks der Verarbeitung der betreffenden Datenkategorie wird der Zeitraum als allgemeine Praxis in dem Sektor, in dem das Unternehmen tätig ist, akzeptiert,
- Die Dauer des mit der betreffenden Person begründeten Rechtsverhältnisses, das die Verarbeitung personenbezogener Daten in der betreffenden Datenkategorie erfordert,
- Je nach dem Zweck der Verarbeitung der betreffenden Datenkategorie gilt der Zeitraum, in dem das berechtigte Interesse des Unternehmens in Übereinstimmung mit dem Gesetz und den Regeln der Integrität gewahrt werden muss,
- Die Dauer, während der die Risiken, Kosten und Verantwortlichkeiten der Speicherung der entsprechenden Datenkategorie je nach dem Zweck der Verarbeitung legal weiterbestehen,
- ob die zu bestimmende Höchstdauer geeignet ist, die betreffende Datenkategorie bei Bedarf genau und aktuell zu halten.
- Der Zeitraum, in dem das Unternehmen gemäß seiner gesetzlichen Verpflichtung personenbezogene Daten in der entsprechenden Datenkategorie speichern muss,
- Die vom Unternehmen festgelegte Zeitspanne für die Inanspruchnahme eines Rechts auf der Grundlage persönlicher Daten in der betreffenden Datenkategorie,

Bei der Festlegung und Anwendung der maximalen Fristen, die für den Zweck, für den die persönlichen Daten verarbeitet werden, erforderlich sind, überwacht das Unternehmen die Einhaltung dieser Fristen mit den Informationen, die im Inventar der Verarbeitung persönlicher Daten des Unternehmens enthalten sind, und ob die maximalen Fristen überschritten werden. Informationen über die persönlichen Daten, die von der Firma im Rahmen ihrer Aktivitäten verarbeitet werden, sind in den folgenden Dokumenten enthalten:

- Aufbewahrungsfristen auf der Grundlage der personenbezogenen Daten für alle personenbezogenen Daten im Rahmen der durchgeführten Aktivitäten in Abhängigkeit von den Prozessen im Inventar der Verarbeitung personenbezogener Daten;
- Aufbewahrungsfristen auf der Grundlage von Datenkategorien werden in VERBIS erfasst;
- Prozessbasierte Aufbewahrungsfristen in der Richtlinie zur Aufbewahrung und Vernichtung personenbezogener Daten

Falls erforderlich, werden Aktualisierungen der betreffenden Aufbewahrungsfristen vorgenommen. Für persönliche Daten, deren Aufbewahrungsfristen abgelaufen sind, wird der Prozess der Löschung, Vernichtung oder Anonymisierung automatisch angewendet.

Aufbewahrungsregeln und Vorsichtsmaßnahmen

Bei der Speicherung von Personendaten wird die Möglichkeit des Verschleißes des Datenträgers (schriftlich, digital, etc.), der zur Speicherung oder Archivierung der betreffenden Personendaten verwendet wird, berücksichtigt. Wird die Speicherung von Personendaten durch elektronische Speichermethode gewählt, ist der Zugriff zwischen den Netzwerkkomponenten während der Speicherzeit begrenzt und nur autorisiert.

Personenbezogene Daten, die in der Geräte- oder Papierumgebung des Unternehmens gespeichert sind, werden durch physische Sicherheitsmaßnahmen gegen Bedrohungen wie Diebstahl oder Verlust dieser Geräte und Papiere geschützt. Ebenso werden physische Umgebungen, die persönliche Daten enthalten, durch geeignete Methoden vor externen Risiken (Feuer, Überschwemmung usw.) geschützt. Die Ein-/Ausgänge zu diesen Umgebungen werden unter Kontrolle gehalten.

Maßnahmen auf gleicher Ebene werden auch für Papiermedien, elektronische Medien und Geräte ergriffen, die sich außerhalb des Unternehmens befinden und persönliche Daten enthalten, die dem Unternehmen gehören.

Die von der Firma getroffenen Vorkehrungen für die Sicherheit der verarbeiteten persönlichen Daten sind wie folgt:

- Die notwendigen Vorkehrungen werden vom Unternehmen getroffen, indem es die Risiken, Bedrohungen, Schwächen und Lücken der Informationssysteme, falls vorhanden, mit Eindringtests aufdeckt.
- Die Risiken und Bedrohungen, die die Kontinuität der Informationssysteme beeinträchtigen werden, sind vom Unternehmen ständig zu überwachen.
- Der Zugang zu Informationssystemen und die Autorisierung von Benutzern erfolgt über eine Zugangs- und Autorisierungsmatrix und Sicherheitsdefinitionen.
- Es werden die notwendigen Maßnahmen für die physische Sicherheit der Ausrüstung, Software und Daten der Informationssysteme des Unternehmens getroffen.
- Hardware (Zugangskontrollsystem, das nur autorisiertem Personal den Zugang zum Systemraum ermöglicht, 24/7-Überwachungssystem, das die physische Sicherheit der Edge- Switches, die das lokale Netzwerk bilden, gewährleistet, Feuerlöschsystem, Klimaanlage usw.) und Software (Firewalls, Angriffsverhinderungssysteme, Netzwerkzugangskontrolle, Systeme, die bösartige Software verhindern, usw.) Maßnahmen werden ergriffen, um die Sicherheit der Informationssysteme gegen Umweltbedrohungen zu gewährleisten.
- Zur Verhinderung der illegalen Verarbeitung personenbezogener Daten werden Risiken identifiziert, technische Maßnahmen ergriffen, um die Einhaltung dieser Risiken zu gewährleisten, und es werden technische Kontrollen für die ergriffenen Maßnahmen durchgeführt.
- Durch die Einrichtung von Zugangsverfahren innerhalb des Unternehmens werden Berichts- und Analysestudien über den Zugang zu persönlichen Daten durchgeführt.
- Der Zugriff auf Speicherbereiche mit persönlichen Daten wird aufgezeichnet und unzulässige Zugriffe oder Zugriffsversuche werden unter Kontrolle gehalten.
- Das Unternehmen trifft die notwendigen Vorkehrungen, um die gelöschten persönlichen Daten für die betroffenen Benutzer unzugänglich und wiederverwendbar zu machen.
- Falls die persönlichen Daten illegal von anderen Personen beschafft werden, wurde das Verfahren in ANHANG-2 von der Firma vorbereitet und ein System und eine Infrastruktur geschaffen, um die hiervon betroffene Person und den Vorstand entsprechend zu informieren.
- Es werden geeignete Sicherheits- Patches installiert, indem Sicherheitslücken verfolgt werden, und die Informationssysteme werden auf dem neuesten Stand gehalten.

- Starke Passwörter werden in elektronischen Umgebungen verwendet, in denen persönliche Daten verarbeitet werden.
- In elektronischen Umgebungen, in denen personenbezogene Daten verarbeitet werden, werden sichere Aufzeichnungs- (Protokollierungs-)Systeme verwendet.
- Datensicherungsprogramme werden verwendet, um sicherzustellen, dass persönliche Daten sicher gespeichert werden.
- Der Zugang zu persönlichen Daten, die in elektronischen oder nicht-elektronischen Umgebungen gespeichert sind, wird nach Zugangsprinzipien eingeschränkt.
- Für die Sicherheit persönlicher Daten wurde eine eigene Richtlinie mit der Bezeichnung **" Richtlinien zur Verarbeitung besonders qualifizierter persönlicher Daten "** festgelegt.

V. Maßnahmen zur Informationssicherheit

Die folgenden Richtlinien und Verfahren bezüglich Informationssicherheitsmaßnahmen, Vorsichtsmaßnahmen und zu ergreifende Schritte wurden innerhalb des Unternehmens herausgegeben und vom Verwaltungsrat des Unternehmens genehmigt und in Kraft gesetzt:

Richtlinien:

1- Richtlinie zur Informationssicherheit
2- Richtlinie zur Zugangskontrolle
3- Netzwerk-Richtlinien
4- Kryptographische Kontrollen und Schlüsselverwaltungsrichtlinie
5- Richtlinie zur sicheren Systementwicklung
6- Richtlinie zur Fernarbeit
7- Ausrüstungs- und Mediensicherheitsrichtlinien
8- Akzeptable Nutzungsrichtlinien
9- Richtlinie zum Informationsaustausch
10- Richtlinie zur Passwortverwaltung
11- Richtlinie zur physischen und ökologischen Sicherheit
12- Richtlinie zur Verwaltung von Privilegienrechten

Verfahren

1- Verfahren der Vermögensverwaltung
2- Verfahren zum Management von Vorfallverletzungen
3- IT- Projektmanagement- Verfahren
4- Verfahren zur Nutzung von Sozialmedien

Formulare und andere Dokumente

1- Formular zur Datenvernichtung
2- Zugangsberechtigungs-Matrix
3- Firmencomputer-Zuweisung und Nutzungsanweisungen
4- Anleitung zur Zuweisung und Nutzung von Firmenleitungen und Telefonen

VI. Vernichtung von persönlichen Daten

Allgemeine Bedingungen über die Vernichtung von persönlichen Daten

Wenn die Gründe, die die Verarbeitung personenbezogener Daten erfordern, beseitigt sind, werden die personenbezogenen Daten von der Firma von Amts wegen oder auf Antrag der betreffenden Person gelöscht, vernichtet oder anonymisiert. Dementsprechend sollten personenbezogene Daten in den folgenden Situationen gelöscht, vernichtet oder anonymisiert werden;

- Der Vertrag zwischen dem Unternehmen und der Person ist nie zustande gekommen, der Vertrag ist nicht gültig, der Vertrag wird spontan beendet, der Vertrag wird aufgelöst oder der Vertrag wird zurückgegeben,
- Der Zweck, der die Verarbeitung personenbezogener Daten erfordert, verschwindet,
- Die Verarbeitung personenbezogener Daten verstößt gegen das Gesetz oder die Ehrlichkeitsregel,
- In Fällen, in denen die Verarbeitung personenbezogener Daten nur unter der Bedingung einer ausdrücklichen Zustimmung erfolgt, ist die Rücknahme der Zustimmung durch die hiervon betroffene Person erforderlich,
- Das Unternehmen akzeptiert den Antrag der betreffenden Person bezüglich der Verarbeitung von persönlichen Daten im Rahmen der Rechte des Artikels 11 (e) und (f) des Gesetzes,
- In Fällen, in denen das Unternehmen den Antrag mit der Bitte um Löschung oder Vernichtung der persönlichen Daten durch die hiervon betroffene Person ablehnt, ist die Antwort, die er gegeben hat, unangemessen oder reagiert nicht innerhalb der vom Gesetz vorgesehenen Frist; Beschwerden an den Vorstand und dieser Antrag wird vom Vorstand genehmigt,

- Die Tatsache, dass es keine Bedingungen gibt, die es rechtfertigen würden, die persönlichen Daten länger aufzubewahren, obwohl die maximale Zeitspanne, die die Speicherung von persönlichen Daten erfordert, abgelaufen ist
  Das Verschwinden der Bedingungen, die in den Artikeln 5 und 6 des Gesetzes die Verarbeitung personenbezogener Daten vorschreiben,

Techniken zur Vernichtung persönlicher Daten

Die Löschung von persönlichen Daten ist der Prozess, der diese persönlichen Daten für die betroffenen Benutzer unzugänglich und unbrauchbar macht. Das Unternehmen stellt sicher, dass die gelöschten persönlichen Daten für die jeweiligen Nutzer nicht zugänglich und wieder- verwendbar sind.

Bei der Löschung personenbezogener Daten durch das Unternehmen wird der folgende Prozess angewendet:

- Identifizierung der persönlichen Daten, die Gegenstand der Löschung sein werden;

- Identifizierung der relevanten Benutzer für die einzelnen persönlichen Daten unter Verwendung der Zugangsberechtigungs- und Kontrollmatrix oder eines ähnlichen Systems;

- Bestimmung der Befugnisse und Methoden der relevanten Benutzer wie Zugriff, Abruf und Wiederverwendung;

- Die Schließung und Beseitigung der Zugriffs-, Wiederherstellungs- und Wiederverwendung- Befugnisse und -methoden der relevanten Benutzer im Rahmen der persönlichen Daten.

Je nach Aufzeichnungsmedium werden personenbezogene Daten wie folgt gelöscht:

- Für diejenigen, deren Gültigkeitsdauer durch die in den Servern enthaltenen persönlichen Daten abläuft, sollte der Systemadministrator die zu speichernde Zeitspanne durch Entfernen der Zugriffsrechte der betreffenden Benutzer löschen.

- Von den persönlichen Daten, die in der elektronischen Umgebung enthalten sind, werden diejenigen, deren Speicherzeit abgelaufen ist, in keiner Weise für andere Mitarbeiter (relevante Benutzer) zugänglich und wiederverwendbar gemacht, außer für den Datenbankverwalter.

- Von den persönlichen Daten, die in der physischen Umgebung enthalten sind, werden diejenigen, deren Speicherzeit abgelaufen ist, in keiner Weise für andere Mitarbeiter (relevante Benutzer) zugänglich und wiederverwendbar gemacht, außer für den für das Dokumentenarchiv verantwortlicher Abteilungsleiter. Darüber hinaus wird eine Schwärzung durch Zeichnen/Malen/Löschen in unlesbarer Weise vorgenommen.
- Von den persönlichen Daten, die in der tragbaren Medien enthalten sind, werden diejenigen, deren Speicherzeit abgelaufen ist, vom Systemadministrator verschlüsselt und nur dem Systemadministrator zugänglich gemacht und in sicheren Umgebungen mit Verschlüsselungsschlüsseln gespeichert.

Vernichtung; bedeutet, dass alle physischen Aufzeichnungsmedien, auf denen Informationen gespeichert sind, nicht zurückgebracht und wieder verwendet werden können.

Je nach Aufzeichnungsmedium werden personenbezogene Daten wie folgt vernichtet:

- Von den persönlichen Daten, die in Papiermedien enthalten sind, werden diejenigen, deren Speicherzeit abgelaufen ist in Papierklippern irreversibel zerstört.

- Von den persönlichen Daten, die optischen und magnetischen Datenträgern enthalten sind, werden diejenigen, deren Speicherzeit abgelaufen ist, hysisch zerstört, z.B. durch Verbrennung oder Verstaubung. Darüber hinaus werden die magnetischen Medien durch ein spezielles Gerät geführt und einem hochwertigen Magnetfeld ausgesetzt, wodurch die Daten darauf unlesbar werden.

Anonymisieren persönlicher Daten bedeutet, persönliche Daten von einer identifizierten oder identifizierbaren natürlichen Person zu trennen, selbst wenn sie mit anderen Daten abgeglichen werden. Wenn in diesem Zusammenhang nachvollziehbar ist, wem die Daten gehören, nachdem sie mit anderen Daten abgeglichen und durch eine Überwachung der Daten unterstützt wurden, kann nicht akzeptiert werden, dass diese Daten anonymisiert wurden.

Anonymisierte Daten unterliegen nicht den Bestimmungen des Gesetzes, da sie nicht mehr als personenbezogene Daten qualifiziert sind. Da die Datensätze so lange persönliche Datenqualitäten haben, bis sie anonymisiert werden, wird jede Transaktion, die mit diesen Daten durchgeführt wird, als Verarbeitung persönlicher Daten betrachtet.

Alle Transaktionen bezüglich der Löschung, Vernichtung und Anonymisierung von persönlichen Daten werden aufgezeichnet und diese Aufzeichnungen werden unter Ausschluss anderer gesetzlicher Verpflichtungen mindestens drei Jahre lang aufbewahrt.

Periodische Vernichtung

Personenbezogene Daten, die in Gürok verarbeitet werden, werden gemäß Artikel 11 der Verordnung über die Löschung, Zerstörung oder Anonymisierung personenbezogener Daten regelmäßig alle 6 (sechs) Monate ab dem ersten Tag des betreffenden Kalenderjahres vernichtet.

Personenbezogene Daten werden bei der ersten periodischen Vernichtung nach dem Datum der Verpflichtung zur Löschung, Vernichtung oder Anonymisierung von personenbezogenen Daten gemäß dieser Richtlinie gelöscht, vernichtet oder anonymisiert.

Falls die hiervon betroffene Person die Löschung oder Vernichtung ihrer persönlichen Daten beantragt, indem sie sich gemäß Artikel 13 des Gesetzes zum Schutz persönlicher Daten an das Unternehmen wendet, werden die folgenden Verfahren durchgeführt:

- Wenn alle Bedingungen für die Verarbeitung personenbezogener Daten verschwunden sind, löscht, vernichtet oder anonymisiert das Unternehmen die personenbezogenen Daten, die Gegenstand des Antrags sind. Das Unternehmen schließt den Antrag der Person spätestens innerhalb von dreißig Tagen ab und informiert die betroffene Person.
- Wenn alle Bedingungen für die Verarbeitung personenbezogener Daten beseitigt sind und die personenbezogenen Daten, die Gegenstand der Anfrage sind, an Dritte weitergegeben wurden, teilt das Unternehmen dies dem Dritten mit. Sie stellt sicher, dass notwendige Maßnahmen im Rahmen dieser Richtlinie und der damit verbundenen Gesetzgebung vor der dritten Partei ergriffen werden.
- Wenn nicht alle Bedingungen für die Verarbeitung der persönlichen Daten verschwunden sind, kann dieser Antrag von der Gesellschaft in Übereinstimmung mit dem dritten Absatz des Artikels 13 des Gesetzes abgelehnt werden, und die Ablehnungsantwort wird der betreffenden Person spätestens innerhalb von dreißig Tagen schriftlich oder elektronisch mitgeteilt.

VII. Die Verantwortlichen der Richtlinie

Die Einheiten und das damit verbundene Personal, die die Systeme, in denen personenbezogene Daten aufbewahrt, verarbeitet und/oder übertragen werden, nutzen/verwalten, sind für die Vorbereitung, Aktualisierung und Umsetzung dieser Richtlinie verantwortlich. In diesem Zusammenhang unterstützen alle Einheiten und Mitarbeiter des Unternehmens die verantwortlichen Einheiten aktiv bei der ordnungsgemäßen Umsetzung der technischen und administrativen Maßnahmen, die von den verantwortlichen Einheiten im Rahmen der Richtlinie ergriffen werden. Alle Einheiten und Mitarbeiter unterstützen die verantwortlichen Einheiten auch aktiv mit dem Ziel, die Ausbildung und das Bewusstsein der Mitarbeiter der Einheit zu erhöhen, sie zu überwachen und kontinuierlich zu kontrollieren, die Datensicherheit in allen Umgebungen, in denen personenbezogene Daten verarbeitet werden, zu gewährleisten, um die illegale Verarbeitung personenbezogener Daten zu verhindern, den illegalen Zugang zu personenbezogenen Daten zu verhindern und sicherzustellen, dass personenbezogene Daten rechtmäßig aufbewahrt werden.

Insbesondere ist die Personalabteilung dafür verantwortlich, dass die Mitarbeiter des Unternehmens in Übereinstimmung mit der Richtlinie handeln, die Abteilung für Informationstechnologien ist für die Bereitstellung der technischen Lösungen verantwortlich, die für die Umsetzung der Richtlinie benötigt werden, und beide Abteilungen sind auch für die Entwicklung, Umsetzung, Veröffentlichung und Aktualisierung der Richtlinie autorisiert und verantwortlich.

VIII.Einhaltung der Richtlinie

Alle Mitarbeiter des Unternehmens sind verpflichtet, die Bestimmungen der Richtlinie bei der Verarbeitung und Speicherung von persönlichen Daten vollständig und ordnungsgemäß einzuhalten, und die oben genannte Richtlinie ist ein integraler Bestandteil der Arbeitsverträge der Mitarbeiter.

Bei konkreten Anzeichen von Verstößen gegen die Bestimmungen dieser Richtlinie untersucht das Führungsgremium des Unternehmens vermutete Verstöße gegen die Richtlinie und ergreift die erforderlichen Maßnahmen. Die Nichteinhaltung dieser Richtlinie kann eine Vielzahl negativer Konsequenzen nach sich ziehen, einschließlich, aber nicht beschränkt auf, den Verlust des Kundenvertrauens, Rechtsstreitigkeiten, Prestigeverlust, finanzielle Verluste und den Ruf des Unternehmens oder persönlichen Schaden. Daher kann die Nichteinhaltung dieser Richtlinie in irgendeiner Weise zu disziplinarischen Untersuchungen oder zur Beendigung von Geschäften oder Verträgen mit Mitarbeitern des Unternehmens oder anderen betroffenen Personen führen. Der Verstoß kann auch zu rechtlichen Schritten gegen die an dem Verstoß beteiligten Personen führen.

IX. Inkrafttreten

Diese Richtlinie, die mit dem Ziel der vollständigen Einhaltung der geltenden Gesetzgebung bei der Verarbeitung personenbezogener Daten ausgearbeitet wurde, wurde durch den Beschluss des Verwaltungsrates von Gürok Turizm ve Madencilik Anonim Şirketi vom... /... / 2019 genehmigt.

Die Richtlinie wird in zwei verschiedenen Medien veröffentlicht: in gedruckter Form und in elektronischen Medien. Sie wird den Mitarbeitern, die in einer elektronischen Umgebung arbeiten, die speziell für die interne Kommunikation bestimmt ist, offengelegt, und ein gedrucktes Exemplar wird in der Personalabteilung aufbewahrt. Die Richtlinie wird bei Bedarf überarbeitet und die entsprechenden Abschnitte werden bei Bedarf aktualisiert.

Ek-1: Tabelle der Aufbewahrungs- und Vernichtungszeiten

Relevante Prozess- und Datenkategorie	Aufbewahrungs- Zeit	Erläuterung
Persönliche Gesundheitsdaten von Mitarbeitern	5 Jahre ab dem Ende der Geschäftsbeziehung	Es wird 5 Jahre lang im Falle einer möglichen Berufskrankheit/eines möglichen Arbeitsunfalls nach dem Arbeitsvertrag und seiner Adresse aufbewahrt.
Dateien für die Einstellung von Mitarbeitern, persönliche Daten	20 Jahre nach dem Ende der Geschäftsbeziehung	Die für den Vertragsabschluss verwendeten Daten werden 20 Jahre lang nach der Fortsetzung des Dienstleistungsvertrags und auf Antrag der Sozialversicherungsanstalt auf der Grundlage eines möglichen Antrags auf Dienstleistungs-/Gebührenermittlung aufbewahrt.
Bewerbungsformulare für Mitarbeiter-Kandidaten, Lebenslauf	1 Jahr ab dem Datum der Antragstellung	Er wird höchstens 2 Jahre lang aufbewahrt, für die Zeit, in der Ihr Lebenslauf und Ihre Bewerbungsformulare veraltet sind.
Persönliche Daten, die im Rahmen der Arbeitsschutzpraxis gewonnen wurden	**15 Jahre nach dem Ende der Geschäftsbeziehung**	Im Rahmen der Verantwortung, die der Arbeitsvertrag den Parteien auferlegt, wird er für einen Zeitraum von 15 Jahren ab dem Datum der Beendigung der Geschäftsbeziehung im Falle eines gesundheitlichen Problems aufbewahrt.
Informationen über potentielle Kunden	2 Jahre ab dem Datum des Erhalts von Informationen	Um einen Kaufvertrag abzuschließen, werden die von den Interessenten erhaltenen Daten 2 Jahre lang aufbewahrt.
Daten, die während des Kundennachfrage- und Beschwerdemanagements gewonnen wurden	1 Jahr ab dem Datum der ersten Registrierung	Persönliche Daten, die zum Zweck der Fortführung des Dienstes, der Verbesserung der Qualität und der Bewertung der Anforderungen des Empfängers gesammelt wurden, werden für 1 Jahr ab dem Datum der ersten Registrierung aufbewahrt.
Aufzeichnungen von Finanz-/ Zahlungstransaktionen	10 Jahre nach dem Ende der Geschäftsbeziehung	Die Daten, die zur Auszahlung der Löhne und Gehälter an die Beschäftigten im Rahmen der vertraglichen Verpflichtungen erhalten werden, werden 10 Jahre lang gespeichert.
Informationsaustausch mit Unternehmen / Institutionen in Zusammenarbeit mit Gürok Turizm ve Madencilik Anonim Şirketi	10 Jahre ab und bis zum Ende des Arbeitsvertrages	Die während des Arbeitsvertrages übertragenen Daten werden 10 Jahre lang, die als Vertragsauszeit angegeben werden, während der entsprechenden Arbeitsperiode und ab dem Ende aufbewahrt.
Persönliche Daten des Unterlieferanten/ Mitarbeiter des Unterlieferanten	10 Jahre ab dem Ende des entsprechenden Vertrags	Die persönlichen Daten der Mitarbeiter der Unternehmen, die mit dem Unternehmen als Auftragnehmer/Unterauftragnehmer zusammenarbeiten, werden gemäß dem Vertragsverhältnis 10 Jahre lang aufbewahrt.

Vom Kaufvertrag abgedeckte persönliche Daten	10 Jahre nach dem Ende der Geschäftsbeziehung	Im Falle von Streitigkeiten, die sich aus dem Vertrag ergeben können, werden sie für die Dauer des Vertrags aufbewahrt.
Persönliche Daten aus Verträgen mit Dritten	10 Jahre ab dem Ende des Vertrags	wird aufgrund des Vertragsverhältnisses für 10 Jahre aufbewahrt
Aufzeichnungen von Sicherheitskameras	180 Tage	Um die Sicherheit am Arbeitsplatz zu gewährleisten, wird sie unter Berücksichtigung der Dauer der Beschwerde sechs Monate lang aufbewahrt.
Registrierung von Besuchern und Versammlungs-Teilnehmern	2 Jahre nach dem Ende der Veranstaltung	Die empfangenen Daten werden 2 Jahre lang aufbewahrt, was eine unfaire Verb-Auszeit gegen ungünstige Situationen hat, die aufgrund der Sicherheit innerhalb des Unternehmens auftreten können.
Daten, die im Rahmen der Zuweisung von Fahrzeugen an Mitarbeiter erhalten wurden	5 Jahre nach dem Ende des Arbeitsvertrags	Personenbezogene Daten, die zur Lieferung von Fahrzeugen an Mitarbeiter zur Erfüllung der Verpflichtungen aus der Geschäftsbeziehung erhalten wurden, werden 5 Jahre lang aufbewahrt, was die Frist für Lohnforderungen darstellt.
Daten zur Nutzung drahtloser Internetdienste	2 Jahre ab dem Datum der ersten Registrierung	Die für die Bereitstellung des Internetzugangsdienstes erhaltenen Daten werden, wie gesetzlich vorgeschrieben, 2 Jahre lang aufbewahrt.
Daten, die unter Protokollierungssystemen aufbewahrt werden	2 Jahre ab dem Datum der Registrierung	Persönliche Daten, die zum Zweck der Bereitstellung eines Internetzugangsdienstes in einer sicheren Umgebung erhalten wurden, werden, wie gesetzlich vorgeschrieben, 2 Jahre lang aufbewahrt.
Informationen von Gästen der Gül Palas und Ali Bey Hotels & Resorts zur Hotelreservierung/ Registrierung erhalten	10 Jahre nach dem Ende des Dienstverhältnisses	Die im Rahmen der Unterkunftsvermittlung erhaltenen Identitäts- und Kontaktdaten werden 10 Jahre lang aufbewahrt, wobei der Vertrag abläuft.
Daten, die von Gästen von Gül Palas und Ali Bey Hotels & Resorts für Hotelunternehmen erhalten wurden	10 Jahre nach dem Ende des Dienstverhältnisses	Die im Rahmen des Vertrags erhaltenen Daten werden für einen Zeitraum von 10 Jahren aufbewahrt, um den Ansprüchen der Hotelgäste mit den angebotenen Dienstleistungen gerecht zu werden.

Ek-2: Verfahren zur Meldung von Verletzungen der personenbezogenen Daten

Paragraph (5) des Artikels 12 des Gesetzes besagt: "Wenn die verarbeiteten persönlichen Daten von anderen auf illegale Weise erlangt werden, informiert der Datenbeauftragte den Betroffenen und den Vorstand so schnell wie möglich ...". Der Ausdruck "so bald wie möglich" in der Bestimmung wird als 72 Stunden interpretiert.

In diesem Zusammenhang wird Gürok die Verletzung unverzüglich und spätestens innerhalb von 72 Stunden ab dem Datum, an dem er davon Kenntnis erlangt hat, dem Verwaltungsrat melden. Nach der Feststellung der von der genannten Datenverletzung betroffenen Personen durch Gürok werden die betroffenen Personen direkt informiert, wenn die Kontaktadresse innerhalb kürzester Zeit erreicht werden kann. Falls diese Information nicht verfügbar ist, erfolgt die Benachrichtigung durch geeignete Methoden, wie z.B. die Veröffentlichung dieser Information durch den für die Datenverarbeitung Verantwortlichen über die firmeneigene Website.

Wenn die Firma Gürok - auf begründeter Basis - den Verwaltungsrat nicht innerhalb von 72 Stunden benachrichtigt, werden die Gründe für die Verzögerung zusammen mit der zu erfolgenden Benachrichtigung dem Verwaltungsrat erläutert.

Das "Meldeformular für die Verletzung von personenbezogenen Daten" auf der Website des Ausschusses wird in der an den Ausschuss zu richtenden Meldung verwendet. In den Fällen, in denen es nicht möglich ist, die Informationen im Formular gleichzeitig zu übermitteln, werden diese Informationen dem Vorstand schrittweise und ohne Verzögerung zur Verfügung gestellt.

Informationen, Auswirkungen und Vorsichtsmaßnahmen bezüglich Datenverstöße durch Gürok werden aufgezeichnet und für die Überprüfung durch den Vorstand bereitgehalten.

Wenn die personenbezogenen Daten in den Datenverarbeitern im Auftrag von Gürok auf illegale Weise von anderen Personen beschafft werden, werden Regelungen getroffen, die es dem Datenverarbeiter ermöglichen, Gürok unverzüglich über diese Angelegenheit zu informieren.

Im Falle von Datenverstößen informiert die Abteilung Informationstechnologien die von der Verstößen betroffenen Unternehmenseinheiten und erstellt einen Bericht über die möglichen Ergebnisse. Sie erstellt einen Aktionsplan für die zu ergreifenden Maßnahmen und Schritte und ergreift Maßnahmen.

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГЮРОК» ТУРИЗМ И ГОРНО-РУДНИКОВЫЕ РАБОТЫ («ГЮРОК ТУРИЗМ ВЕ МАДЕНДЖИЛИК АНОНИМ ШИРКЕТИ» GÜROK TURİZM VE MADENCİLİK A.Ş.) ПОЛИТИКА ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Апрель 2019
Стамбул

Содержание

I. Цель и сфера политики

В соответствии со Ст.№ 6102 Турецкого Коммерческого Кодека, Акционерное Общество «Гюрок» -
Туризм и Горно-Рудниковые Работы, (именуемое в дальнейшем «Гюрок»), в качестве контроллера данных, обязуется полностью соблюдать все юридические меры по защите и обработке персональных данных.
Цель данной политики хранения и уничтожения персональных данных («Политика»), в соответствии со Ст.№ 6698, П. 16 о защите, удалении и уничтожении персональных данных и П. 5 о анонимности персональных данных, определить максимальные стандарты, которые будут применяться при хранении, удалении и уничтожении персональных данных, обрабатываемых «Гюрок», для лиц, получающим продукт или услуги, сотрудникам, кандидатам в работники и другим третьим лицам.
Настоящая «Политика» является основой для процесса определения максимального времени обработки персональных данных, обрабатываемых «Гюрок», а также для удаления, уничтожения и анонимизации.
Эта «Политика» распространяется на все подразделения, процессы и деловые отношения с третьими сторонами. Настоящая «Политика» применяется ко всем руководителям

«Гюрок», сотрудникам, консультантам, поставщикам услуг, которые могут собирать, обрабатывать или получать доступ к данным (содержащим персональные данные и / или специальные персональные данные).
Настоящая «Политика» распространяется на все персональные данные и информацию, собираемую «Гюрок». Собранные данные хранятся в документах или на електронных носителях таких как:

- Серверы (домены, резервные копии, электронная почта, базы данных, веб-сервера, обмен файлами и т. д.)
- Программное обеспечение (офисное программное обеспечение, порталы и т. д.)
- Устройства защиты информации (брандмауэр, обнаружение и блокировка вторжений, файл журнала, антивирус и т. д.)
- Персональные компьютеры (настольные компьютеры, ноутбуки)
- Мобильные устройства (телефоны, планшеты и т. д.)
- Оптические диски (CD, DVD, Blu-Ray и т. д.)
- Устройства переносной памяти (USB, карта памяти, оперативная память и т. д.)
- Принтер, сканер, копировальная машина.
- Информация и документы в печатных средствах массовой информации.
- Видео и аудио записи.
- Данные, полученные с помощью систем контроля и управления доступом.

II. Соответствующее законодательство и документы

- Ст. № 6698 о защите персональных данных.
- Постановление от 28 октября 2017 года об удалении, уничтожение или анонимизации персональных данных.
- Постановление от 30 декабря 2017 года о реестре контроллеров данных.
- Постановление от 10 марта 2018 года о выполнении обязательств по предоставлению информации владельцам персональных данных о целях, способах сбора и процедурах, которым необходимо следовать при выполнении обязательств.

- Ст. № 6098 Кодекса Обязательств Турции
- Ст. № 5510 Кодекса о социальном страховании и общем медицинском страховании
- Ст. № 6361 Кодекса о безопасности и охране здоровья.
- Ст. № 5651 Кодекса о регулировании интернет-изданий и о борьбе с преступлениями, совершаемыми с помощью таких публикаций.

- Политика «Гюрок» о защите и обработке персональных данных.
- Политика «Гюрок» об обработке специальных квалифицированных персональных данных.
- Политика «Гюрок» «Чистый стол и чистый экран».

- Процедура «Гюрок» о подаче заявления согласно с Закон о Защите Персональных Данных (ЗЗПД).
- Процедура «Гюрок» по использованию и контролю инструментов связи с общественностью и информационных технологий сотрудников.

III. Определения

Значения терминов употребляемых в «Политике» приведенны ниже:

Термин	Значение
Группа Покупателей	Физические или юридические лица, которые передают персональные данные ответственным за эти данные
Открытое согласие	согласие на конкретную тему, основанное на информировании и выраженное добровльно
Анонимизация	Методы сопоставление персональных данных с другими данными позволяющие сделать персональные данные не связанными с реальным идентифицируемым физическим лицом
Клиент	Физическое лицо, чьи персональные данные обрабатываются
Пользователь	Лицо, которое обрабатывает персональные данные в рамках организации, ответственной за данные в соответствии с полномочиями и инструкциями, полученными от ответственного за данные, за исключением лица или

Уничтожение	подразделения, ответственного за техническое хранение, защиту и резервное копирование данных
Закон или ЗЗПД	Удаление, уничтожение или анонимизация персональных данных
Носители записей	Ст. № 6698 о защите персональных данных
Персональные данные	Все виды сред, в которых хранятся персональные данные, которые обрабатываются автоматическими или полуавтоматическими способами при условии, что они являются частью любой системы записи данных
Инвентаризация обработки персональных данных	Любая информация, относящаяся к физическому лицу, личность которого определена или может быть определена Операции по обработке персональных данных, которые выполняются ответственными за эти данные на продолжительности определённого времени; цель обработки персональных данных, категория данных, максимальное время, необходимое для целей, создания и обработки персональных данных, которые создаются путем связывания передаваемой информации от группы или субъекта данных

Обработка персональных данных	Получение персональных данных полностью или частично автоматизированными или не автоматизированными способами, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу, распространение, предоставление, доступ, обезличивание, блокирование, удаление, уничтожение,при условии, что они будут являться частью любой системы регистрации данных.
Компания	Компания, ответственная за защиту персональных данных
Руководящий орган	Руководящий орган, ответственный за защиту персональных данных
Специальные квалифицированные персональные данные	Персональные данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, одежды, членства в ассоциациях, фондах или профсоюзах, состояния здоровья, интимной

Периодическое Уничтожение	жизни, судимости, данные о мерах безопасности, биометрические или генетические данные
Компания или «Гурок»	Это процесс удаления, уничтожения или анонимизации персональных данных, который будет выполняться с повторяющимися интервалами, указанными согласно закону о политике хранения и уничтожения персональных данных
Обработчик данных	Акционерное Общество «Гюрок», Туризм и Горно-Рудниковые Работы
Система регистрации данных	Физическое или юридическое лицо, которое обрабатывает персональные данные от своего имени на основе полномочий, предоставленных ответственным за данные
Ответственный за данные	Система регистрации, в которой персональные данные обрабатываются в соответствии с определенными критериями
Информационная система реестра для сотрудников	Физическое или юридическое лицо, которое определяет цели и средства обработки персональных данных и несет ответственность за создание и управление системой регистрации данных
Положение-правила	Информационная система, доступ к которой осуществляется через Интернет, созданная и управляемая Руководящим Органом, где данные будут использовать для регистрации и других связанных транзакций
	Положение от 28 октября 2017 года об удалении, уничтожении или анонимизации персональных данных

IV. Общие Принципы Хранения

Срок Хранения

Компания в течение периода хранения персональных данных, сама определяет время для хранения или обновления документов и электронных записей (смотрите Приложение-1)

Если в настоящей «Политике» и в приложениях к ней не указано иное, персональные данные, включенные в категорию Инвентаризации и обработки персональных данных Компанией, хранятся, как правило, в течение периодов, указанных в Приложении-1, с даты получения соответствующих персональных данных.

Исключительные случаи, в которых время хранения данных может быть продлено:

- В случаях запроса Официальными Органами на проведение расследования или исследования, и/или в случае, если этого потребуют юридические обязательства или правовые законны Компании;

- В случаях, когда необходимо осуществление правовых действий в соответствии с действующим законодательством в ходе разбирательств или других правовых, судебных процессах.

Определение максимального срока хранения, необходимого для цели обработки персональных данных:

- Цель обработки соответствующей категории данных, соответствует со сроками, принятыми в соответствии с общими требованиями сектора, в котором работает Компания,
- Обработка персональных данных заинтересованного лица будет продолжаться в соответствующей категории на продолжительности правовых отношений
- Период срока хранения, будет действителен в соответствии с Законодательством и Кодексом Честности, в зависимости от цели обработки соответствующей категории данных, в течение которого Компания будет иметь законный интерес,
- Время , в течение которого персональные данные, требующие обработки, будут храниться, риски, затраты и обязанности связанные с хранением, будет продолжаться на законых основаниях,
- Максимальное время будет определяться для поддержания точности и актуальности соответствующей категории,

- Юридическое обязательство Компании хранить персональные данные в соответствующей категории данных на период их обработки,
- Период хранения устанавлевается Компанией для утверждения права, связанного с персональными данными, включенными в соответствующую категорию данных,

что берется во внимание.
Компания устанавливает и применяет максимальное время, необходимое для целей обработки персональных данных, также отслеживает соответствие периодов и соответствие хранения информации, содержащихся в Инвентареизации персональных данных Компании и не превышены ли максимальные периоды.
Персональные данные обрабатываются Компанией в рамках ее деятельности;

- Сроки хранения персональных данных, относятся ко всем персональным данным, определяются в зависимости от процессов и в рамках выполняемой деятельности, описанных в Инвентаризации обработки персональных данных;
- Периоды хранения, на основе категорий данных , записываются в Информационной системе реестра для сотрудников;

- Сроки хранения персональных данных включены в политику хранения и уничтожения персональных данных.

При необходимости в сроки хранения могут вносится обновления. К персональным данным, срок хранения которых истек, применяется автоматический процесс удаления, уничтожения или анонимизации этих данных.

Правила Хранения И Меры Предосторожности

Так как для хранения или архивирования персональных данных используются носители данных (письменные, цифровые и т. д.), то в процессе хранения персональных данных учитывается возможность износа этих носителей. Если человек выбрал хранение персональных данных в электронном виде, то эти данные ограничены в хранении и доступе между компонентами сети и доступны только ответственным лицам.

Персональные данные, хранящиеся на устройствах или в бумажном виде, защищены путем принятия мер физической защиты от таких угроз, как кража или потеря этих устройств и документов. Также, физические среды, в которых хранятся личные данные, защищены от внешних рисков (пожаров, наводнений и т. д.) соответствующими методами. Входы / выходы в эти среды берутся под контроль. Такиеже меры принимаются и для хранения персональных данных, которые хранятся на устройствах или в бумажном виде за пределами Компании, но принадлежащие Компании.

Меры предосторожности, принятые Компанией для обеспечения безопасности обрабатываемых персональных данных, приведены ниже:

- Компания предпринимает все необходимые меры предосторожности, подвергая информационные системы проверкам для выявления слабых мест на возможность проникновения рисков, угроз и устраняет слабости, если таковые имеются.
- Компания постоянно контролирует все информационные системы на риски и угрозы, которые могут повлиять на непрерывность работы.
- Доступ к информационным системам и авторизация пользователей осуществляется через матрицу доступа и авторизации, которая и обеспечивает безопасность.
- Также принимаются необходимые меры предосторожности для обеспечения физической безопасности оборудования, программного обеспечения и данных информационных систем Компании.
- Для обеспечения защиты информационных систем от экологических угроз, используются аппаратное обеспечение (система контроля доступа, позволяющая доступ в системное помещение только ответственному персоналу, система круглосуточного мониторинга 7/24, обеспечивающая физическую

безопасность комутаторов, образующих локальную сеть, системы пожаротушения, системы кондиционирования и т. д.) и программное обеспечение (брандмауэры, системы предотвращения атак,системы контроля доступа к сети, системы, предотвращающие вредоносные программы и т. д.).

- Для предотвращения незаконной обработки персональных данных, применяются регулярные технические проверки и принятые меры периодически обновляются.
- Внутри Компании проводятся отчетные и аналитические работы, связанные с созданием процедур доступа к персональным данным .
- Доступ к хранилищам персональных данных регистрируется, а несанкционированные доступы или попытки доступа находятся под контролем.
- Компания предпринимает все необходимые меры предосторожности, чтобы сделать удаленные персональные данные недоступными и непригодными для повторного использования и для других лиц.
- Если персональные данные получены незаконно другими лицами, Компания разработала процедуру (смотрите Приложение-2) и систему для оповещения пострадавшего лица и Компании.
- Информационные системы регулярно обновляются, пробелы в безопасности устанавливаются, исправляются и устраняются.

- В цифровых электронных средах, где обрабатываются персональные данные, используются надежные пароли.
- Системы безопасного ведения записей (регистрации) заполняются в цифровых электронных средах, где эти персональные данные обрабатываются.
- Используются программы резервного копирования данных, которые обеспечивают безопасное хранение персональных данных.
- Доступ к персональным данным, которые хранятся в электронной или неэлектронной среде, ограничен в соответствии с принципами доступа.
- Для обеспечения безопасности специальных персональных данных используется отдельная политика под названием «Обработка специальных персональных данных».

V. Меры информационной безопасности

Ниже указанные политики и процедуры были разработаны для мер информационной безопасности, предосторожности и продвижения, которые необходимы для нашей Компании и были утверждены и введены в действие Советом директоров нашей Компании:

Политики

1. Политика информационной безопасности
2. Политика контроля доступа
3. Сетевая политика
4. Политика Контроля Криптографии и управления ключами
5. Политика развития безопасной системы
6. Политика Удаленной Работы
7. Политика безопасности оборудования и средств массовой информации
8. Политика допустимого использования
9. Политика обмена информацией
10. Политика управления паролями
11. Политика физической и экологической безопасности
12. Политика управления привилегированных прав

Процедуры

1. Процедура управления активами
2. Процедура устранения нарушений
3. Процедура управления проектами Информационных Технологий
4. Процедура использования социальных сетей

Формы и другие документы

1- Форма уничтожения данных.
2- Матрица доступа.
3- Руководство по размещению и эксплуатации компьютеров в Компании.
4- Руководство по использованию телефона и телефонной линии.

VI. Уничтожение персональных данных

Общие условия удаления персональных данных

В случае, если причины, требующие обработки персональных данных, устраняются, персональные данные удаляются, уничтожаются или анонимизируются Компанией или по запросу заинтересованного лица. Согласно этому, если:

- Поправка или актуальность соответствующих законодательных положений, составляющих основу для обработки персональных данных;
- В случае, если договор между Компанией и заинтересованным лицом не был заключен, договор недействителен, договор самопроизвольно прекращается, договор расторгается или отменяется;
- В случае, если отсутствует цель, по причине которой требуется обработка персональных данных,
- В случае, если обработка личных данных противоречит закону или добросовестности;
- В случаях, когда обработка персональных данных происходит только на основании открытого согласия заинтересованного лица;

- В случае, если принятие заявления заинтересованного лица в отношении обработки персональных данных осуществляется в рамках прав, предусмотренных «e» и «f» подпунктами 11-ой статьи Законодательства;
- В случаях, если Компания отклоняет заявление, поданное заинтересованным лицом с просьбой об удалении или уничтожении его персональных данных, или в случае, если ответ, который он дал, является неадекватным или ответ не поступил в течение срока, установленного Законодательством, в случае отправления жалоб в Правление, и одобрение данного запроса Правлением;

- Несмотря на завершение максимального срока, в течение которого требуется хранение персональных данных и отсутствуют условия, оправдывающие более длительное хранение персональных данных;
- Отмена условий, требуемых для обработки персональных данных, указанных в 5-ой и 6-ой статьях Законодательства;

то в этом случае личные данные должны быть удалены, уничтожены или переведены в анонимный статус.

Методы уничтожения персональных данных

Удаление персональных данных является процессом перевода указанных персональных данных в недоступные и непригодные для использования заинтересованными пользователями. Компания гарантирует, что удаленные персональные данные не будут доступны и не смогут использоваться повторно соответствующими пользователями.
В процессе удаления персональных данных, Компанией применяются следующие процедуры:

- Идентификация персональных данных, подлежащих удалению;
- Определение заинтересованных пользователей по каждой персональной информации с использованием матрицы авторизации и контроля доступа или аналогичной системы;

- Определение таких полномочий и методов заинтересованных пользователей, как доступ, поиск, повторное использование;
- Закрытие и устранение доступа, поиска, повторного использования полномочий и методов заинтересованных пользователей в рамках персональных данных.

В зависимости от носителей записи персональные данные удаляются следующим образом:

- Для лиц, срок данных которых истекает на серверах хранения, системный администратор может ограничить и удалить авторизацию доступа заинтересованного лица;
- Срок, истекающий для хранения персональных данных в электронной среде, становится недоступным и закрытым для других сотрудников (заинтересованных пользователей), за исключением менеджера базы данных.

- Данные лиц, чье время, требующее для хранения персональных данных, хранящихся в физической среде истекает, кроме руководителя подразделения, ответственного за архив документов, никоим образом не являются доступными и не могут быть использованы другими сотрудниками. Кроме этого, используется закрашивание информации путем затемнения / закрашивания / стирания.
- Период, истекающий для хранения персональных данных на переносном носителе, зашифровывается системным администратором и предоставляется только для системного администратора, а также, хранится в защищенной среде с использованием ключей шифрования.

Уничтожение означает, что все физические носители записи, пригодные для хранения данных, где хранится информация, не могут быть возвращены и использованы снова.

В зависимости от носителя, бумажные персональные данные уничтожаются следующим образом:

- Период, истекающий для хранения персональных данных, содержащихся на бумаге, необратимо уничтожается в машинах для резки бумаги;
- Применяется такое физическое уничтожение, как плавление, сжигание или стирание требующих хранения бумажных персональных данных, содержащихся на оптических и магнитных носителях, срок годности которых истекает. Кроме того, магнитный носитель пропускается через специальное устройство и

подвергается воздействию сильного магнитного поля, что делает данные на нем нечитаемыми.

Анонимизация персональных данных заключается в том, чтобы сделать персональные данные не связанными с идентифицированным или определенным физическим лицом, даже если они могут сопоставлятся с другими данными. В этом контексте, если путем мониторинга данных
можно понять, кому принадлежат данные после их сопоставления с другими данными,
нельзя признать, что эти данные имеют анонимный статус.

Анонимные данные не регулируются положениями Закона, так как они больше не классифицируются как персональные данные. Поскольку данные обладают классификацией персональных данных до тех пор, пока не будут подвергнуты процессам анонимизации, любая транзакция, выполняемая с этими данными, рассматривается как обработка персональных данных.

Все транзакции, касающиеся удаления, уничтожения и анонимизации персональных данных, регистрируются, и данные записи хранятся не менее трех лет, за исключением других юридических обязательств.

Периодическое удаление

Персональные данные, обрабатываемые в рамках «Гюрок», подлежат периодическому уничтожению каждые 6 (шесть) месяцев с первого дня календарного года в соответствии с 11-й статьей Положения об Удалении, Уничтожении или Анонимизации Персональных Данных.
В контексте настоящей Политики, при первом периодическом уничтожении после даты, когда возникла обязанность удалять, уничтожать или анонимизировать личные данные,
персональные данные обязаны быть удалены, уничтожены или анонимизированы.
В случае, если соответствующее лицо запрашивает удаление или уничтожение его персональных данных путем обращения в Компанию в соответствии с 13 статьей «Защита Персональных Данных»:

- В случае, если полностью отсутствуют условия для обработки персональных данных, Компания удаляет, уничтожает или анонимизирует персональные данные, подлежащие запросу. Компания принимает решение по запросу лица не позднее чем через тридцать дней и информирует заинтересованное лицо.
- В случае, если полностью отсутствуют условия для обработки персональных данных, а персональные данные, подлежащие запросу, были переданы третьим лицам, Компания уведомляет об этом третье лицо, обеспечивает принятие необходимых мер в рамках настоящей Политики и соответствующего Законодательства в отношентт третьей стороны.
- В случае, если условия для обработки персональных данных полностью не сняты, то запрос может быть отклонен Компанией в соответствии с третьим параграфом

13-й статьи Законодательства, и ответ об отказе будет сообщен соответствующему лицу в письменной или электронной форме не позднее чем через тридцать дней.

VII. Ответственные за Политику

Подразделения и связанные с ними сотрудники, использующие / управляющие системами, в которых хранятся, обрабатываются и / или передаются персональные данные, несут ответственность за подготовку, обновление и реализацию настоящей Политики. В этом контексте, в целях надлежащего осуществления технических и административных мер, принимаемых ответственными подразделениями, филиами и работниками Компании,повышение уровня подготовки и осведомленности сотрудников подразделения, мониторинг и постоянный надзор, а также предотвращение незаконной обработки персональных данных,предотвращение незаконного доступа к персональным данным и обеспечение сохранения персональных данных в соответствии с Законом, принятие технических и административных мер для обеспечения безопасности данных во всех сферах, где обрабатываются персональные данные, активно поддерживают соответствующие ответственные подразделения.

В частности, так как отдел кадров обеспечивает работу сотрудников в соответствии с Политикой, Подразделение Информационных Технологий отвечает за предоставление технических решений, необходимых для реализации Политики, и оба подразделения уполномочены и несут ответственность за разработку, внедрение, публикацию и обновление Политики в соответствующих условиях.

VIII. Соответствие Политике

Все сотрудники Компании обязаны полностью и надлежащим образом соблюдать положения Политики при обработке и хранении персональных данных, и вышеупомянутая Политика является неотъемлемой частью трудовых договоров с работниками.
В случае выявления конкретных признаков нарушения положений настоящей Политики, орган управления Компании проводит расследование предполагаемых нарушений Политики и принимает необходимые меры. Несоблюдение этой Политики может привести к различным негативным последствиям, включая, помимо прочего, потерю доверия клиентов, судебные разбирательства, потерю престижа, финансовые потери, а также репутацию Компании или личный ущерб. Следовательно, несоблюдение этой политики каким-либо образом может привести к дисциплинарному расследованию или прекращению бизнеса или заключению контракта с работниками Компании или другими заинтересованными лицами. Нарушение может, также, привести к судебному иску против тех, кто причастен к этому вопросу.

IX. Вступление в Силу

Настоящая Политика, подготовленная с целью полного соответствия действующему Законодательству в области обработки персональных данных, была утверждена

решением Совета директоров акционерного общества «Гюрок Туризм ве Маденджилик Аноним Ширкети» (Gürok Turizm ve Madencilik Anonim Şirketi) от… /… / 2019.
Политика публикуется в двух разных форматах (печатных и электронных). Политика разъясняется сотрудникам, работающим в электронной сфере, специфичной для внутренней коммуникации, а печатная копия хранится в отделе кадров. Политика пересматривается по мере необходимости, а соответствующие разделы обновляются при необходимости.

Приложение-1: Таблица хранения и уничтожение персональных данных

Процесс и категория данных	Срок Хранения	Описание
Персональные данные о здоровье сотрудников	5 лет со дня окончания трудовых отношений	Хранятся 5 лет на случай определения и уведомления возможных профессиональных заболеваний / несчастных случаев.
Файлы подбора персонала, персональные данные	20 лет со дня окончания трудовых отношений	Хранятся 20 лет на случай возможного запроса данных, использованных для заключения контракта, определения услуги / сбора и требования учреждения социального обеспечения.
Заявки кандидатов на работу, резюме	1 год со дня подачи заявления	Хранятся не более 2 лет, так как теряют силу вашего резюме и форм заявки.
Персональные данные полученные в области техники безопасности труда и гигиены	15 лет со дня окончания трудовых отношений	Хранятся 15 лет с даты прекращения деловых отношений в рамках обязанностей по трудовому договору, на случай если стороны предъявят претензии касательно здоровья.
Информация о потенциальных клиентах	2 года со дня получения информации	Данные, полученные от потенциальных клиентов, сохраняются в течение 2 лет с целью заключения договоров.
Данные, полученные от опроса клиентов – жалобы и	1 год со дня регистрации	Данные, полученные с целью улучшения обслуживания, повышения качества и оценки требований покупателя,

предложения	10 лет со дня окончания трудовых отношений	сохраняются в течение 1 года со дня регистрации.
Записи о финансовых / платежных операциях	10 лет со дня начала и окончания трудового договора	Данные, о выплате заработной платы работникам по обязательствам, наложенным на стороны, сохраняются в течение 10 лет.
Информация о фирмах / организациях, которые сотрудничают с «Гюрок Туризм ве Маденджилик Аноним Ширкети» (Gürok Turizm ve Madencilik Anonim Şirketi)	10 лет со дня истечения срока действия соответствующего договора	Данные, полученные во время трудового договора, хранятся в течение 10 лет, что указывается как срок действия договора.
Информация о персональных данных подрядчиков / субподрядчиков		Персональные данные сотрудников компаний, имеющих отношения подрядчика / субподрядчика с компанией, как того требуют договорные отношения, хранятся в течение 10 лет.

Персональные данные, указанные в договорах	10 лет со дня окончания трудовых отношений	Хранятся 10 лет на случай возможных споров и разногласий в течение срока действия договора.
Персональные данные, третьих лиц, подписавших договоры	10 лет со дня окончания договора	Хранятся 10 лет, в соответствии с требованиями договорных отношений.
Записи с камер наблюдения	180 дней	Хранятся в течение шести месяцев в целях обеспечения безопасности на рабочем месте, с учетом срока действия возможных жалоб.
Регистрация посетителей и участников собраний	2 года после окончания мероприятий	Хранятся 2 года на случай деликатных или неблагоприятных ситуаций, которые могут возникнуть, для безопоасности внутри Компании.
Данные, полученные при распределении транспортных средств	5 лет со дня окончания трудового договора	Данные сотрудников, полученные для распределения транспортных средств с целью выполнения обязательств, вытекающих из деловых отношений, хранятся 5 лет со дня окончания

сотрудникам	2 года со дня регистрации	трудового договора. Данные, полученные для предоставления услуги доступа в Интернет, хранятся в течение 2 лет, как того требует закон.
Данные об использовании беспроводного интернета	2 года со дня регистрации	Персональные данные, полученные с целью предоставления услуг, доступа в интернет в защищенной среде, хранятся в течение 2 лет, как того требует закон.
Данные сохраненные в системных журналах отслеживания записей.	10 лет после окончания сервисных отношений	Идентификационные данные и контактная информация, полученная от гостей при регистрации / бронировании в отелях, хранятся в течение 10 лет со дня истечения срока действия договора.
Информация полученная от гостей при регистрации / бронировании в отелях Gül Palas ve Ali Bey Hotels & Resorts	10 лет после окончания сервисных отношений	Данные, полученные от гостей отеля с целью удовлетворения требований предлагаемых услуг, хранятся в течение 10 лет.
Информация полученная от гостей при оказании и организации гостиничных услуг в отелях Gül Palas ve Ali Bey Hotels & Resorts		

Приложение-2: Процедура уведомления о нарушении персональных данных

В соответствии с 5-ым пунктом 12-ой статьи Закона, в котором говорится: “если обработанные персональные данные получены незаконным путем другими лицами, ответственный за сохранение персональных данных, обязан информировать об этом заинтересованное лицо и Совет Компании как можно скорее.... Выражение ” как можно скорее " , по Закону, подразумевает - в течение 72-х часов.

В связи с этим «Гюрок» обязан информировать об этом Совет Компании без задержки и не позднее, чем через 72 часа с момента обнаружения нарушения, установить пострадавшего (-их) и сообщить об этом в течение максимально разумного периода времени на контактные адреса пострадавших лиц, если же это невозможно, опубликовать, соответствующим образом, уведомление через веб-сайт ответственного за сохранение персональных данных.

Если «Гюрок» не сможет уведомить, по обоснованным причинам, Совет Компании в течение 72 часов, то вместе с уведомлением, Совету Компании должны будут объяснены и причины задержки.

Для уведомления Совета Компани используется “Форма уведомления о нарушении персональных данных”, содержащаяся на веб-странице Совета Компани. На случай,

если информация, содержащаяся в форме, не сможет быть предоставлена одновременно, эта информация будет предоставляться Совету Компании поэтапно и без задержки.
Информация о нарушениях данных, последствиях и принятых мерах «Гюрок» будет записана и храниться в готовом для рассмотрения Советом Компани виде.
В случае, если персональные данные, обрабатываемые от имени «Гюрок», полученны незаконным путем другими лицами, обработчик данных обязан принять меры и без каких-либо задержек информировать об этом «Гюрок».
В случае если от нарушения пострадавшие Компании, отдел Информационных Технологий информирует подразделения Компании и готовит отчет о возможных последствиях. Только потом составляется план и принимаются необходимые меры.