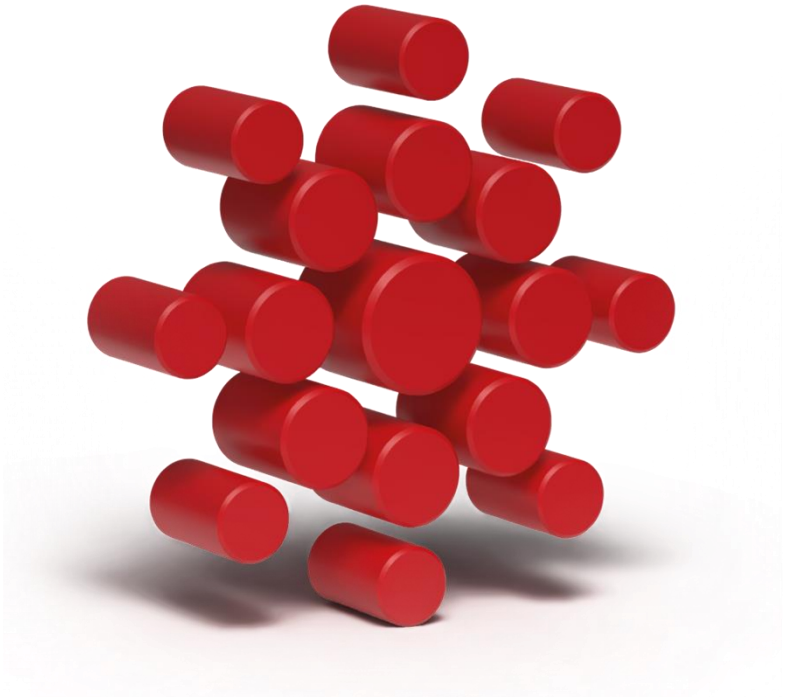

POLICY OF PRESERVATION AND DESTRUCTION OF PERSONAL DATA

Purpose

Personal Data Preservation and Destruction Policy (“Policy”) aims to determine and announce the procedures for preservation and destruction of personal data belonging to Employee, Employee Candidate, Service Providers, Customer, Customer Candidate, Visitor and third party which is processed by Remed Uluslararası Destek ve Danışmanlık Hizmetleri A.Ş. (Remed Assistance); in accordance with Republic of Turkey Constitution, international conventions, the European Union General Data Protection Regulation ("GDPR"), Law on Protection of Personal Data No. 6698 ("Law") and other relevant legislation.

Scope

Personal data belonging to Employee, Employee Candidate, Service Providers, Customer, Customer Candidate, Visitor and third parties are within the scope of this policy and this Policy shall apply in all recording environments and personal data processing activities where personal data of Remed Assistance are present or personal data processed or managed by Remed Assistance are present.

Authority and Responsibilities

In relation to fulfillment of requirements related with destruction of data stipulated in Law, Regulation and Policy, all employees, consultants, external service providers and all individuals who keep and process personal data at the company with other titles are obligated to fulfill these requirements. Each unit is obligated to preserve and protect the data produced in their work processes. Responsibility for notification or acceptance of communications or correspondence with the PDP Council on behalf of the data controller, such as notification or acceptance, and registration in the register shall belong to the “Data Controller Contact Person (DPO)”.

Definitions and Abbreviations

Clear Consent : Consent on a specific subject, declared with free will.

Data Subject/Related Individual : Real person whose personal data is processed.

Law : LPDP Law on Personal Data Protection No 6698.

Personal Data : all information related with real entity whose identity is defined or can be defined.

Related User : Excluding the individual or unit responsible for technical storage, protection or backup of data, they are the individuals who process the personal data within the data controller organization or with the authority and instruction received from the data controller.

Anonymization : Making personal data unrelated to an identifiable or identifiable with a natural person under any circumstances, even by matching with other data.

Electronic Media : Environments where personal data can be created, read, changed and written with electronic devices.

Non-Electronic Media : All written, printed, visual, etc., media other than electronic media.

Destruction : Deletion, destruction or anonymization of personal data.

Personal Data Inventory : Inventory where data controllers create personal data processing activities by associating them with personal data processing purposes, data category, transferred buyer group and data subject individual group and which are detailed by explaining the maximum period required

for personal data processing purposes, transfer to foreign countries and foreseen personal data and data security precautions taken.

Recording Medium : Any environment in which personal data are processed, which are fully or partially automated or processed in non-automated ways, provided that they are part of any data recording system.

Council : Personal Data Protection Council.

Processing of Personal Data : Collection of personal data with non-automated methods provided that it is a part of a data registry system or which is completely or partially automatic, all action made on data such as recording, storage, maintenance, replacement, revision, explanation, transmission, assignment, rendering obtainable, classification or prohibition of usage.

Anonymization of Personal Data : Rendering personal data anonymous thus cannot be associated with a real entity whose identity is defined or can be defined even if they are matched up with other data.

Deletion of Personal Data : Deletion of personal data; making personal data inaccessible and unavailable to Users in any way.

Destruction of Personal Data : The process of making personal data inaccessible, non-retrievable and non-usable by anyone.

Special Personal Data : Biometric and genetic data of individuals related to race, ethnic origin, political thought, philosophical belief, religious, sect or other beliefs, costume and attire, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures.

Periodical Destruction : If the conditions for personal data processing stated in the Law are completely removed, the deletion, destruction or anonymization operations to be made on its own motion with repeating intervals stipulated in personal data storage and destruction policy.

Data Processor : A natural or legal person handling personal data on his behalf on the basis of the authority conferred by the data controller.

Data Controller : A natural or legal person who is responsible for setting up and managing the data recording system, determining the means and means of processing the personal data.

Data Record System : Recording system in which personal data is processed according to certain criteria.

Regulation : Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette on October 28, 2017.

Policy of Personal Data Preservation and Destruction

Data Controller Organization and Data Media

All employees of Remed Assistance take an active role in the proper implementation of the technical and administrative measures taken by the responsible units under the Policy. Measures are taken to ensure data security in all environments where personal data is processed in order to prevent the personal data from being processed and accessed illegally and to ensure that personal data are kept in accordance with the law, by increasing the training and awareness of the unit employees, monitoring and continuous supervision.

The distribution of titles, units and job descriptions of those who took part in the preservation and destruction processes of personal data are detailed below;

Data Controller Contact Person : It is defined as the primary duties of the contact person to design, plan, perform and organize related actions, to provide controls and to perform the works and procedures to be performed within the framework of the procedures and principles determined in GDPR and LPDP on behalf of the data controller.

Archive Officer : Carrying out the processes of processing, storing, deleting, destroying and anonymizing personal data stored in the archive.

Personal Data Protection Council Member : Assists in maintaining the processes related to personal data security by supporting the Data Controller Contact Person in order to design, plan, perform, and provide the relevant controls within the framework of the procedures and Principles determined in the GDPR and LPDP on behalf of the Data Controller

Personal data is securely stored by Remed Assistance in the following environments in accordance with the law;

Electronic Media

- Servers (Domain, backup, e-mail, Database, web, file sharing, etc.)
- CRM applications
- Office applications
- Information security devices (firewall, intrusion detection and blocking, log file, antivirus etc.)
- Personal computers (desktop, laptop)
- Mobile devices (phone, tablet etc.)
- Optical discs (CD, DVD etc.)
- Removable memory (Usb, memory card etc.)
- Security camera recorders
- Non-Electronic Media
- Paper
- Written, printed, visual environment

Personal data of Employees, Candidates, Service Providers, Customers, Candidates, Visitors and employees of third-party institutions or organizations are stored and destroyed by Remed Assistance; in accordance with the Law.

The concept of the processing of personal data is defined in the 4th article of the GDPR and the 3rd article of the Law. It is stated that the personal data processed in the 5th article of GDPR and 4th article of Law should be linked, limited and measured for the purpose for which they are processed and kept for the time required for the purpose or foreseen in the relevant legislation. In the relevant articles of GDPR and in 5th and 6th articles of Law, the processing conditions of personal data are stipulated. Accordingly, within the framework of its activities, Remed Assistance preserves personal data for a period specified in the relevant legislation or in accordance with our processing purposes

5.2.1. Legal Reasons that Require Storage

- Law on the Mode of Execution of Medicine and Medical Sciences No 1219
- Income Tax Law No. 193
- Enforcement and Bankruptcy Law No. 2004
- Tax Procedure Law No. 213
- Regulation on Job Authority, Responsibility and Training of Occupational Safety Specialists No. 28512
- Regulation on Emergency Situations in Workplaces No. 28681

- Regulation on International Health Tourism and Tourist Health No. 30123
- Road Transport Regulation No. 30295
- Law No. 4817 on Work Permits for Foreigners
- Labor Law No. 4857
- Banking Law No. 5411
- Social Insurance and General Health Insurance Law No. 5510
- Law No. 5651 on Regulating Broadcasts Made on the Internet and Combating Crimes Committed Through These Publications
- Insurance Law No. 5684
- Turkish Commercial Code No. 6102
- Occupational Health and Safety Law No. 6331
- Vocational Education Law No. 6899

Processing Purposes that require Storage

- **Execution of BT Activities** : Tracking internet logs, managing user requests, managing mail accounts, conducting information security activities, debt management
- **Technical Operation Processes :**Ensuring customer satisfaction, vehicle shooting organization, customer hotel, accommodation, transportation, aircraft etc. services, aircraft ticketing processes, flight ticket billing process, road assistance activities
- **Human Resources Operations :** Establishing an emergency/blood group cards, conducting emergency processes, providing AGI service, approving information security policies, conducting disciplinary processes, creating human resources processes, creating an account request to the user, creating consent and contracts, and making private health insurances, evaluation of staff performance, execution of wage / payroll processes, sharing of wage offer information, management of foreign employees, execution and approval of annual leave processes, creation and management of debt, approval of orientation training
- **Employment Processes :** Conducting employment activities, evaluation of job applications, placement of trainees
- **Management Process of Administrative Works :**Tracking the company vehicles, ensuring the physical security of the institution, conducting in-house purchasing activities, carrying out the services, creating the badges, giving the in-house work permits of the suppliers
- **Education Process :** Conducting training activities, conducting ISMS training activities, evaluating educators, conducting OHS training activities, providing orientation training
- **Legal Processes** : Execution of employee execution file processes, execution of legal processes
- **Execution of OHS Processes :** Conducting OHS training activities, approving the OHS commitment
- **Medical Unit Processes :** Research-investigation file can be created, translator arrangements can be made, funeral arrangements can be made, drug-medical equipment/medical devices can be adjusted, medical file can be tracked, medical escort arrangements, medical escort hotel and transportation, customer complaint and request notification form, hotel arrangements, patient transfer arrangements, determination and understanding of local representatives, on-site medical service arrangements
- **Accounting Processes :** Execution of billing / payment processes, execution of the customer's collection processes, ensuring communication with the supplier Sale Process Collecting potential customer information at conferences and meetings, creating brand customer contracts, managing events and organizations
- **Supplier Relations Management :** Collecting and archiving business cards, following customer operational processes, creating supplier contracts

- **Travel Services :** Car rental services, ensuring the continuity of service sales (ticket, hotel, visa, car rental, tour etc.), filling the mail order form and receiving the service fee, obtaining medical escort flight ticket and informing the airline company, making tour / travel insurance, customer purchase of plane tickets and flight confirmation of the passenger, obtaining visa application documents and obtaining visas, informing the passenger information to the competent authorities

Reasons that Require Destruction

Personal Data will be erased, destructed or erased, destructed or anonymized ex officio by Remed Assistance upon request of the related individual in following cases;

• when the relevant legislation provisions that constitute the basis for its processing are amended,

• when the purpose that requires processing or storage is eliminated,

• when the related individual's explicit consent is cancelled where the processing of personal data takes place only in accordance with the explicit consent condition,

• when the application of related individual regarding the deletion and destruction of personal data within the framework of the rights of the person concerned in accordance with the relevant articles of the GDPR and Article 11 of the Law, is accepted by Remed Assistance,

• In cases where Remed Assistance rejects the application made by the relevant person for the request of deletion, destruction or anonymization of his personal data, finds his answer insufficient or does not respond within the prescribed time in the Law; Personal Data Protection Complaints to the Board and this request is approved by the Board,

• if maximum period of time requiring the retention of personal data expires and there are no conditions to justify keeping the personal data for a longer period,

Ensuring Security of Personal Data

Remed Assistance takes all necessary technical and administrative measures to ensure the appropriate level of security required for the protection of personal data.

Necessary precautions are taken in order to meet the following conditions which are stipulated in 1st item of 12th article of LPDP;

• To prevent personal data from being processed unlawfully,

• To prevent personal data from being illegally accessed,

• To ensure the preservation of personal data.

The measures applied by Remed Assistance to ensure the security of personal data are detailed in the sub-articles:

Technical Precautions

In line with personal data security, Remed Assistance takes technical measures in accordance with the developments in technology. Infrastructure investments in accordance with developing technology are made. It enables the installation of software and hardware including virus protection systems and firewalls. It uses the necessary security measures against the current and known vulnerabilities of its systems and logs of the systems are taken. It ensures that the employees' access to personal data is kept under control in information technology units. Remed Assistance imposes restrictions on access to personal data according to the principle of minimum authority. Access rights are checked

periodically within the scope of ISO 27001 standard. It defines access and authorization in accordance with the management and process requirements. Checks whether the access is suitable for authorization. Reports the information obtained as a result of controlling the security of the systems to the concerned. Necessary technical measures are taken by determining the points that pose a risk. It promotes awareness to be a part of the corporate culture with a model that constantly processes technical measures to maintain the security of Personal Data. It ensures that the measures taken are maintained with the controls. Physical security measures are kept at the top level with camera systems within the organization. Environmental monitoring, automatic fire extinguishing systems and access authorization controls of digital media where personal data are kept are provided. Backups of personal data are stored in a different location under the control of Remed Assistance.

Administrative Precautions

Remed Assistance employs well-informed and experienced people to provide data security and provides Information Security and PDP Awareness training to its personnel. The necessary internal controls are performed for the installed systems. Operates the processes of risk analysis, data classification, information security risk assessment and business impact analysis within the scope of established systems. “Personal Data Protection Council” was established within Remed Assistance for personal data security. The committee meets at certain periods and evaluates the measures. Remed Assistance takes the necessary administrative measures to ensure the security of personal data and supervises the work of the employees according to these measures. It defines access authorizations in accordance with the management and process requirements at a level that does not cause disruption to business processes. Employees are informed that they cannot disclose the personal data they have learned to anyone else in violation of the provisions of the Law, cannot use them for purposes other than processing, and that this obligation will continue after they leave their jobs. Necessary commitments are taken from the employees in this direction. Concerning the sharing of personal data with third parties, it signs a confidentiality agreement with the people whose personal data is shared or provides personal data security with the provisions it will add to the contracts. Third parties whose personal data are shared agree to take necessary security measures to protect personal data and ensure that these measures are followed in their organization.

Audits for the Sustainability of Personal Data Protection

Remed Assistance conducts necessary inspections in accordance with the provisions of GDPR and article 12 of the Law or has them conducted by other parties. It provides internal and external audits to ensure the sustainability of Information Security. It regularly performs leak tests into the systems for technical gaps that may occur in the systems. The systems are regularly monitored by the data processing system. Necessary technical and administrative measures are taken to eliminate the findings obtained after management systems audits and risk analysis. When it is determined that the personal data is accessed or processed illegally, it is reported to the Information Security Board. The Information Security Board shares the detected nonconformities/risks with the Remed Assistance management.

Measures Applied to Ensure the Protection of Third Parties' Personal Data

Remed Assistance, in contracts with third parties; retains the necessary sanction provisions in order to prevent personal data from being processed unlawfully, to prevent unlawful access to data, and to ensure data retention. Confidentiality agreements are signed before information is shared with third parties. Necessary information is provided to third parties to raise awareness.

Precautions Applied for the Protection of Special Personal Data

Sufficient precautions should be taken for the special personal data both in terms of their qualifications and because they can lead to victimization or discrimination. In the 9th article of the GDPR and in the 6th article of the Law, personal data that have the risk of causing victimization or discrimination of individuals when determined against the law are determined as “Special”.

These data are; data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data.

Remed Assistance takes the necessary precautions to protect the special personal data, which are determined as “special” and processed in accordance with the law. In the technical and administrative measures taken to protect personal data, necessary sensitivity is shown for special personal data.

Employees are informed about the use of special personal data with the Personal Data Security Policy. Special personal data are not processed in the event of the consent of the person or in the absence of the matters specified in Article 9 of the GDPR and Article 6 of the Law. In cases where special personal data can be processed, it will not be shared with anyone other than the third party that has been informed and explicitly informed.

Raising Awareness for the Protection of Personal Data

Employees are provided with necessary information, trainings are organized and their effectiveness is measured in order to raise awareness to prevent personal data from being processed unlawfully, to prevent illegal access to the data and to protect the data. Other documents related to the "Policy on Protection and Processing of Personal Data" have been published on the website of our institution. Policies are revised in case of changes in the relevant laws, regulations or legislations and are announced to the relevant parties again.

Personal Data Destruction Techniques

Remed Assistance destroys the personal data it obtains at the request of personal data subjects, due to legal obligations, due to the fact that it is not compulsory to use for the protection of the public order and on the condition that it does not affect the business processes. Personal data belonging to the data subjects are destroyed based on the decision of the organization when the requirements of continuing the service to our customers, fulfilling legal obligations, and planning the employee rights and fringe benefits are eliminated. Every year, personal data that are not required to be stored are destroyed in accordance with the legislation with the following techniques on the dates determined by the Data Controller Contact Person. Destruction processes; it is performed in three different methods: deletion, destruction and anonymization.

Deletion of Personal Data

The methods of deleting personal data are specified below;

- **Personal Data on Servers** : For those personal data whose necessary time period for storage on the servers expire, the system administrator can remove the access privileges of the users and delete them.
- **Personal Data on Electronic Media :** The personal data which are stored on electronic media and whose storage period expire are made inaccessible and unusable for other employees (related users) except for the database manager. In the operational processes, the personal data environments completed by completing the file are deleted only in such a way that the authorized administrator can access.
- **Personal Data on Physical Media :** The personal data which are stored on physical media and whose storage period expire, are made inaccessible and unusable for other employees except

for the unit manager responsible for the document archive. In addition, blackening is applied by drawing/painting/erasing in an unreadable manner.

- **Personal Data on Portable Media :** The personal data which are stored in flash-based storage media and whose storage period expire, are stored in secure environments with encryption keys by being encrypted by the system administrator and granting access authority only to the system administrator.

Destruction of Personal Data

The destruction of personal data is indicated below;

- **Personal Data on Physical Media :**The personal data which are stored in paper and whose storage period expire are irreversibly destroyed in paper shredder.
- **Personal Data on Optical /Magnetic Media :**The personal data stored in optical media and magnetic media and whose storage period expire are made irreversibly physically unreadable.

Anonymization of Personal Data

Anonymizing personal data is to make personal data unrelated to an identified or identifiable natural person by any means, even if it is compiled with other data.

In order for personal data to be anonymized; the personal data must be rendered unrelated to a identified or identifiable natural person, even by using appropriate techniques for the recording environment and related field of activity, such as the return of data by the data controller or third parties and/or the matching of the data with other data.

Preservation and Destruction Periods

The storage periods related to personal data processed by Remed Assistance within the scope of its activities are detailed in the following environments;

• The storage periods regarding the personal data related to all personal data within the scope of activities carried out depending on the processes, in the Personal Data Inventory document,

• Storage periods based on data categories are detailed in the Data Disclosure System (Verbis). The storage periods are determined by taking into consideration the laws that Remed Assistance is subject to, the terms of the contract with the relevant parties and the time required for the operational activities of Remed Assistance.

If necessary, updates are made by the Personal Data Contact Person on the retention periods in question.

Personal data, whose retention periods expire, are destroyed ex officio.