

PERSONAL DATA PROTECTION AND PROCESSING POLICY

The protection of personal data is among the top priorities of DENTAPOINT DIŐ SAĐLIĐI MEDİKAL HİZMETLERİ İNŐAAT PETROL ÜRÜNLERİ PAZARLAMA İÇ VE DIŐ TİCARET LİMİTED ŐİRKETİ (DENTAPOINT). The most important aspect of this issue is the protection and processing of the personal data of our employees, company shareholders, company officials, our visitors, employees, shareholders, and officials of the institutions with which we cooperate, and third parties, as governed by this Policy.

According to the Constitution of the Republic of Turkey, everyone has the right to demand the protection of personal data concerning themselves. DENTAPOINT takes the necessary care to protect the personal data of job candidates, company shareholders, company officials, visitors, employees, shareholders, and officials of the institutions with which we cooperate, and third parties, which are managed by this Policy, and adopts this as a Company policy.

In this context, DENTAPOINT takes the necessary administrative and technical measures to protect personal data processed within the framework of legal regulations.

The basic principles adopted by the company in processing personal data are as follows:

- Processing personal data in accordance with the law and the rules of good faith,
- Ensuring that personal data is accurate and up-to-date when necessary,
- Processing personal data for specific, explicit, and legitimate purposes,
- Processing personal data in a manner relevant, limited, and proportionate to the purposes for which they are processed,
- Retaining personal data for as long as required by relevant legislation or for the purpose for which they are processed,
- Informing and enlightening data subjects,
- Establishing the necessary system for data subjects to exercise their rights,
- Taking necessary measures to safeguard personal data,
- Acting in accordance with relevant legislation and regulations of the Data Protection Authority when transferring personal data to third parties,
- Exercising due care in the processing, protection, and transfer of sensitive personal data.

PURPOSE OF THE POLICY

The primary purpose of this Policy is to ensure transparency and trust by informing individuals whose personal data is processed by the Company, and by conducting personal data processing activities in accordance with the law.

CONTENT

This Policy applies to all personal data of individuals processed by automated means or by non-automated means, provided that they are part of any data recording system.

The scope of application of this Policy to the groups of personal data owners mentioned above may cover the entire Policy or only a part of it.

IMPLEMENTATION OF THE POLICY AND RELATED LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data will take precedence. In the event of any inconsistency between the applicable legislation and this Policy, the provisions of the legislation in force will prevail.

ENFORCEMENT OF THE POLICY

This Policy, established by DENTAPOINT, is effective from the same date as the law it accompanies. If there are any updates or changes to the Policy, the effective date will be updated accordingly.

The Policy is published on DENTAPOINT's website and is made available to the relevant individuals upon request.

ISSUES RELATED TO THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the KVKK (Personal Data Protection Law), DENTAPOINT takes the necessary administrative, legal, and all possible technical measures to ensure appropriate security to prevent unlawful processing of personal data, unlawful access to data, and to safeguard the data. In this context, necessary audits are conducted.

ENSURING THE SECURITY OF PERSONAL DATA

Technical and Administrative Measures Taken to Ensure the Lawful Processing of Personal Data

DENTAPOINT takes technical and administrative measures based on the nature of the data to be protected, technological capabilities, and implementation costs to ensure the lawful processing of personal data, secure storage in safe environments, prevention of their destruction, loss, or alteration for unlawful purposes, and prevention of accidental or unauthorized disclosure, access, transmission, or any other form of unlawful access.

Measures Taken to Ensure the Lawful Processing of Personal Data

- ❖ Network security and application security are ensured.
- ❖ A closed network system is used for the transfer of personal data over the network.
- ❖ Key management is applied.
- ❖ Security measures are taken within the scope of IT system procurement, development, and maintenance.
- ❖ The security of personal data stored in the cloud is ensured.
- ❖ Disciplinary regulations containing data security provisions are in place for employees.
- ❖ Regular training and awareness activities on data security are conducted for employees.
- ❖ An authorization matrix has been created for employees.
- ❖ Access logs are kept regularly.
- ❖ Institutional policies regarding the use, retention, and disposal of access, information security, and other related matters have been established and implemented.
- ❖ Confidentiality agreements are made.

- ❖ The authorities of employees who have changed roles or left the company are revoked in this area.
- ❖ Up-to-date anti-virus systems are used.
- ❖ Firewalls are utilized.
- ❖ Signed contracts contain data security provisions.
- ❖ Extra security measures are taken for personal data transferred via paper, and the relevant documents are sent in a confidential document format.
- ❖ Personal data security policies and procedures have been established.
- ❖ The monitoring of personal data security is conducted.
- ❖ Necessary security measures are taken concerning the entry and exit to physical environments containing personal data.
- ❖ The security of physical environments containing personal data is ensured against external risks (fire, flood, etc.).
- ❖ The security of environments containing personal data is maintained.
- ❖ A user account management and authorization control system is implemented, and its monitoring is conducted.
- ❖ Log records are kept in a manner that prevents user interference.
- ❖ Protocols and procedures for the security of sensitive personal data have been established and implemented.
- ❖ Intrusion detection and prevention systems are used.
- ❖ Cybersecurity measures are taken, and their implementation is continuously monitored.
- ❖ Encryption is performed.
- ❖ Personal data is minimized as much as possible.
- ❖ Personal data is backed up, and the security of the backed-up personal data is also ensured.
- ❖ Existing risks and threats have been identified.
- ❖ Service providers who process data are regularly audited for data security.
- ❖ Awareness of data security among service providers who process data is ensured.
- ❖ Data loss prevention software is used.

AUDIT OF MEASURES TAKEN TO PROTECT PERSONAL DATA

In accordance with Article 12 of the KVKK, DENTAPOINT conducts or commissions the necessary audits within its organization. The results of these audits are reported to the relevant department within the internal operations, and the necessary actions are taken to improve the measures implemented.

MEASURES TO BE TAKEN IN CASE OF UNAUTHORIZED DISCLOSURE OF PERSONAL DATA

In the event that personal data processed in accordance with Article 12 of the KVKK is obtained by others through unlawful means, DENTAPOINT will notify the relevant personal data owner and the Personal Data Protection Board (KVK Board) as soon as possible.

If deemed necessary by the KVK Board, this situation may be announced on the KVK Board's website or by other means.

PROTECTING THE RIGHTS OF DATA SUBJECTS; CREATING CHANNELS FOR DATA SUBJECTS TO COMMUNICATE THESE RIGHTS TO OUR COMPANY AND EVALUATING THEIR REQUESTS

DENTAPOINT ensures the implementation of the necessary channels, internal processes, administrative and technical arrangements in accordance with Article 13 of the KVKK for evaluating the rights of personal data owners and providing the necessary information to them.

If personal data owners submit their requests regarding their rights listed below in writing, DENTAPOINT will finalize the request free of charge as soon as possible and no later than thirty days, depending on the nature of the request. However, if the processing requires an additional cost, the fee determined by the KVK Board tariff may be charged by DENTAPOINT. Personal data owners have the right to:

- Learn whether personal data is being processed,
- Request information if personal data has been processed,
- Learn the purpose of processing personal data and whether it is being used in accordance with its purpose,
- Know the third parties to whom personal data is transferred domestically or abroad,
- Request the correction of personal data if it is incomplete or incorrectly processed and request that the third parties to whom personal data has been transferred be informed of the transaction carried out within this scope,
- Request the deletion or destruction of personal data, although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, in the event that the reasons requiring its processing disappear, and request that the third parties to whom personal data has been transferred be informed of the transaction carried out within this scope,
- Object to the emergence of a result against the person by analyzing the processed data exclusively through automated systems,
- Request the compensation of damages in case of damage due to the unlawful processing of personal data.
- More detailed information on the rights of data subjects is provided in this Policy.

PROTECTION OF SPECIAL CATEGORIES OF PERSONAL DATA

Under the Law on the Protection of Personal Data No. 6698, certain personal data are given special importance due to the risk of causing victimization or discrimination if processed unlawfully. These data include information on race, ethnic origin, political opinions, philosophical beliefs, religion, sect

or other beliefs, appearance and dress, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions, and security measures.

DENTAPOINT takes great care in protecting special categories of personal data that are legally defined as "sensitive" and processed in accordance with the law. In this context, the technical and administrative measures taken by DENTAPOINT for the protection of personal data are carefully applied to sensitive personal data, and the necessary audits are conducted within the company. Detailed information regarding the processing of special categories of personal data is provided in this Policy.

RAISING AWARENESS AND AUDITING BUSINESS UNITS ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

DENTAPOINT ensures that the necessary training is provided to business units to increase awareness about preventing the unlawful processing of personal data, preventing unlawful access to data, and ensuring the preservation of data. DENTAPOINT establishes the necessary systems to raise awareness among both existing employees and new employees within business units about the protection of personal data and, if needed, works with professional individuals or organizations.

RAISING AWARENESS AND AUDITING BUSINESS PARTNERS AND BRANCHES ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

DENTAPOINT provides information to its branches to increase awareness about preventing the unlawful processing of personal data, preventing unlawful access to data, and ensuring the preservation of data.

DENTAPOINT's notifications to individuals in a business relationship are repeated when necessary, in accordance with changing provisions and regulations; reminders are made to ensure awareness among business partners, existing employees, and newly recruited employees within business units about the protection of personal data, and if needed, support is provided through professional individuals or organizations.

The results of awareness-raising activities and training conducted to increase awareness of personal data protection and processing among DENTAPOINT's business partners are reported to DENTAPOINT management. DENTAPOINT evaluates participation in relevant meetings and informational sessions in this regard and conducts or commissions the necessary audits.

ISSUES RELATED TO THE PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution and Article 4 of the KVKK, DENTAPOINT processes personal data lawfully, in good faith, accurately, and when necessary, keeping it up-to-date; pursuing specific, clear, and legitimate purposes; and processing personal data in a way that is related to, limited to, and proportionate to these purposes. Our company retains personal data for the period required by the relevant laws or for the period necessary for the purpose of processing the personal data.

DENTAPOINT processes personal data based on one or more of the conditions specified in Article 5 of the KVKK, in accordance with Articles 20 of the Constitution and 5 of the KVKK.

In accordance with Articles 20 of the Constitution and 10 of the KVKK, DENTAPOINT provides information to data subjects and ensures that necessary information is provided if data subjects request it.

DENTAPOINT complies with the regulations stipulated for the processing of special categories of personal data as per Article 6 of the KVKK.

In accordance with Articles 8 and 9 of the KVKK, DENTAPOINT adheres to the regulations for the transfer of personal data as prescribed by the law and the KVKK Board.

PROCESSING PERSONAL DATA IN ACCORDANCE WITH THE PRINCIPLES SET FORTH IN THE LEGISLATION

- Legal and Fair Processing

DENTAPOINT operates in compliance with the principles established by legal regulations and the general principle of trust and fairness in the processing of personal data. In this context, DENTAPOINT considers proportionality requirements and does not use personal data for purposes beyond what is required.

- Ensuring Accuracy and Currency

DENTAPOINT ensures that the personal data it processes are accurate and up-to-date, taking into account the fundamental rights of data subjects and its own legitimate interests. Necessary measures are taken to this end.

- Processing for Specific, Explicit, and Legitimate Purposes

DENTAPOINT clearly and precisely determines the legitimate and lawful purpose for processing personal data. The company processes personal data only to the extent necessary for providing its services and for the purposes required.

- Relevant, Limited, and Proportionate Processing

DENTAPOINT processes personal data in a manner suitable for achieving the defined purposes and avoids processing personal data that is not related to or required for achieving the purpose. For instance, personal data processing activities are not conducted for future potential needs.

- Retention for the Period Required by Relevant Legislation or for the Purpose of Processing

DENTAPOINT retains personal data only for the period specified by the relevant legislation or for as long as necessary for the purpose of processing. The company first determines if there is a specified retention period in the relevant legislation; if a period is specified, it adheres to that period; if no period is specified, it retains personal data only for the duration required for the purpose of processing. Upon expiration of the period or elimination of the reasons for processing, personal data are deleted, destroyed, or anonymized by DENTAPOINT. DENTAPOINT does not retain personal data for future use. Detailed information on this matter is provided in this Policy.

PROCESSING PERSONAL DATA BASED ON ONE OR MORE OF THE CONDITIONS SPECIFIED IN ARTICLE 5 OF THE KVKK, AND LIMITED TO THESE CONDITIONS

The protection of personal data is a constitutional right. Fundamental rights and freedoms can only be limited by laws and for the reasons specified in the relevant articles of the Constitution, without affecting their essence. According to the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases specified by law or with the explicit consent of the individual. Accordingly, and in line with the Constitution, our company processes personal data only in cases specified by law or with the explicit consent of the individual. Detailed information on this matter is provided in this Policy.

INFORMING AND NOTIFYING THE DATA SUBJECT

In accordance with Article 10 of the KVKK, DENTAPOINT informs data subjects during the collection of personal data. In this context, DENTAPOINT provides information about its identity and that of its representative, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data may be transferred, the method and legal reason for collecting personal data, and the rights of the data subject. Detailed information on this matter is provided in this Policy.

Article 20 of the Constitution states that everyone has the right to be informed about their personal data. In line with this, Article 11 of the KVKK includes "requesting information" among the rights of data subjects. Accordingly, DENTAPOINT provides the necessary information if the data subject requests it, in accordance with Articles 20 of the Constitution and 11 of the KVKK. Detailed information on this matter is provided in this Policy and the Application Form.

PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

DENTAPOINT handles the processing of personal data classified as "special categories" by the KVKK with sensitivity to the regulations stipulated by the KVKK.

Article 6 of the KVKK designates certain personal data as "special categories" due to their potential to cause harm or discrimination if processed unlawfully. These data include race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, appearance and dress, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions, security measures, and biometric and genetic data.

In accordance with the KVKK, DENTAPOINT processes special categories of personal data only under the following conditions, with adequate measures determined by the KVKK Board:

- With the explicit consent of the data subject, or
- Without the explicit consent of the data subject:
 - Special categories of personal data other than health and sexual life, in cases provided for by law.
 - Special categories of personal data related to health and sexual life, only for purposes such as protecting public health, preventive medicine, medical diagnosis, treatment, and care services, planning and managing health services and financing, and by individuals or authorized institutions bound by confidentiality obligations.

TRANSFER OF PERSONAL DATA

DENTAPOINT may transfer personal data and special categories of personal data to third parties (third-party companies, business partners, third-party public or private natural or legal persons) in line with lawful personal data processing purposes, taking necessary security measures. DENTAPOINT acts in accordance with the regulations stipulated in Article 8 of the KVKK. Detailed information on this matter is provided in this Policy

TRANSFER OF PERSONAL DATA

DENTAPOINT may transfer personal data to foreign countries with Adequate Protection or to foreign countries where Data Controllers Have Committed Adequate Protection if one of the following conditions is met, in accordance with lawful and legal personal data processing purposes:

- If there is a clear legal regulation regarding the transfer of personal data in laws,
- If it is necessary to protect the life or physical integrity of the data subject or another person, and the data subject is unable to provide consent due to physical impossibility or if their consent is not legally valid,
- If it is necessary to transfer personal data of the parties to a contract directly related to the establishment or performance of that contract,
- If personal data transfer is required for our company to fulfill its legal obligations,
- If the personal data has been made public by the data subject,
- If the transfer of personal data is necessary for the establishment, use, or protection of a right,
- If the transfer of personal data is necessary for our company's legitimate interests, provided that it does not harm the fundamental rights and freedoms of the data subject.

TRANSFER OF SPECIAL CATEGORIES OF PERSONAL DATA ABROAD

DENTAPOINT, with due care and necessary security measures, and by taking adequate precautions as stipulated by the KVKK Board, may transfer special categories of personal data of the data subject to foreign countries with Adequate Protection or to foreign countries where Data Controllers Have Committed Adequate Protection if one of the following conditions is met:

- If the data subject's explicit consent is obtained, or
- If the data subject's explicit consent is not obtained:
 - Special categories of personal data other than health and sexual life (such as race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, appearance and dress, membership in associations, foundations, or trade unions, criminal convictions, security measures, and biometric and genetic data) in cases specified by law,
 - Special categories of personal data related to the health and sexual life of the data subject only for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and financing, by persons or authorized institutions with a confidentiality obligation.

Transfer of Personal Data Abroad

DENTAPOINT can transfer personal data and special categories of personal data to third parties in compliance with legal and legitimate purposes for processing personal data, taking necessary security measures. Our company transfers personal data to foreign countries that the KVK Board has declared to provide adequate protection ("Country with Adequate Protection") or, in the absence of adequate protection, to foreign countries where data controllers in Turkey and the relevant foreign country have committed to providing adequate protection in writing and with the permission of the KVK Board ("Country with Data Controller Providing Adequate Protection"). DENTAPOINT acts in accordance with the regulations stipulated in Article 9 of the KVK Law. Detailed information on this subject is provided in this Policy.

Transfer of Personal Data Abroad

DENTAPOINT can transfer personal data to countries with Adequate Protection or to countries where the Data Controller provides Adequate Protection if one of the following conditions is met, whether or not the data subject's explicit consent is available:

If there is a clear regulation in the laws regarding the transfer of personal data:

- If it is necessary for the protection of the life or bodily integrity of the data subject or another person, and the data subject is unable to provide consent due to physical impossibility or if consent is not legally valid;
- If the transfer of personal data is necessary for the establishment or performance of a contract directly related to the parties to the contract;
- If the transfer of personal data is required for our company to fulfill its legal obligations;
- If the personal data has been made public by the data subject;
- If the transfer of personal data is necessary for the establishment, exercise, or protection of a right;
- If the transfer of personal data is necessary for our company's legitimate interests, provided it does not harm the fundamental rights and freedoms of the data subject.

Transfer of Special Categories of Personal Data Abroad

DENTAPOINT, by taking necessary precautions, implementing required security measures, and following the adequate measures prescribed by the KVK Board, can transfer special categories of personal data to countries with Adequate Protection or to countries where the Data Controller provides Adequate Protection under the following conditions:

- **If the data subject's explicit consent is available, or**
- **If the data subject's explicit consent is not available:**
 - Special categories of personal data other than health and sexual life (such as race, ethnicity, political opinions, philosophical beliefs, religion, sect, or other beliefs, clothing, membership in associations, foundations, or unions, criminal convictions, and security measures, as well as biometric and genetic data) may be transferred in the situations specified by the laws
 - Special categories of personal data related to the health and sexual life of the data subject may only be transferred within the scope of public health protection, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, and processed by persons or authorized institutions and organizations under a confidentiality obligation

Categorization, Processing Purposes, and Retention Periods of Processed Personal Data

DENTAPOINT, in compliance with the clarification obligation under Article 10 of the KVK Law, informs the data subjects about which groups of personal data it processes, the purposes of processing, and the retention periods.

Categorization of Personal Data

In accordance with Article 10 of the KVK Law, DENTAPOINT processes personal data in specific categories mentioned below, restricted and based on one or more of the personal data processing

conditions stipulated in Article 5 of the KVK Law, and in compliance with the general principles and obligations outlined in the KVK Law, particularly those specified in Article 4 regarding the processing of personal data. The categories of personal data processed under this Policy are as follows, and the data subjects to whom these categories relate are also specified in this Policy:

- **Identity**
- **Contact**
- **Location**
- **Employment**
- **Legal Transaction**
- **Customer Transaction**
- **Physical Space Security**
- **Operational Security**

◆ ****Communication:****

- Execution of Emergency Management Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes for Employee Candidates
- Fulfillment of Contractual and Legal Obligations for Employees
- Execution of Training Activities
- Execution of Activities in Compliance with Legislation
- Execution of Finance and Accounting Operations
- Execution of Assignment Processes
- Monitoring and Execution of Legal Affairs
- Execution of Internal Audit/Investigation/Intelligence Activities
- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution/Control of Business Activities
- Execution of Occupational Health/Safety Activities
- Collection and Evaluation of Suggestions for Improving Business Processes
- Execution of Business Continuity Activities
- Execution of Goods/Services Procurement Processes
- Execution of Post-Sales Support Services for Goods/Services

- Execution of Goods/Services Sales Processes
- Execution of Goods/Services Production and Operations Processes
- Execution of Customer Relationship Management Processes
- Execution of Activities Related to Customer Satisfaction
- Execution of Advertising/Campaign/Promotion Processes
- Execution of Retention and Archiving Activities
- Execution of Contract Processes
- Tracking Requests/Complaints
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Location:****

- Monitoring and Execution of Legal Affairs
- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution of Contract Processes
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Personnel:****

- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes for Employee Candidates
- Execution of Employee Satisfaction and Loyalty Processes
- Fulfillment of Contractual and Legal Obligations for Employees
- Execution of Training Activities
- Execution of Activities in Compliance with Legislation
- Execution of Finance and Accounting Operations
- Execution of Assignment Processes
- Monitoring and Execution of Legal Affairs
- Planning of Human Resources Processes
- Execution of Occupational Health/Safety Activities

- Collection and Evaluation of Suggestions for Improving Business Processes
- Execution of Business Continuity Activities
- Execution of Retention and Archiving Activities
- Execution of Contract Processes
- Execution of Wage Policy
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Legal Action:****

- Execution of Processes for Employee Benefits and Interests
- Execution of Audit/Ethics Activities
- Execution of Activities in Compliance with Legislation
- Execution of Finance and Accounting Operations
- Monitoring and Execution of Legal Affairs
- Execution of Internal Audit/Investigation/Intelligence Activities
- Execution of Contract Processes
- Tracking Requests/Complaints
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Customer Transactions:****

- Execution of Audit/Ethics Activities
- Execution of Finance and Accounting Operations
- Execution of Processes Related to Company/Product/Service Loyalty
- Monitoring and Execution of Legal Affairs
- Execution of Internal Audit/Investigation/Intelligence Activities
- Execution/Control of Business Activities
- Collection and Evaluation of Suggestions for Improving Business Processes
- Execution of Business Continuity Activities
- Execution of Goods/Services Procurement Processes
- Execution of Post-Sales Support Services for Goods/Services

- Execution of Goods/Services Sales Processes
- Execution of Goods/Services Production and Operations Processes
- Execution of Customer Relationship Management Processes
- Execution of Activities Related to Customer Satisfaction
- Execution of Contract Processes
- Tracking Requests/Complaints
- Execution of Marketing Processes for Products/Services
- Ensuring the Security of Data Controller Operations
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Physical Space Security:****

- Execution of Audit/Ethics Activities
- Execution of Access Permissions
- Ensuring Physical Space Security
- Execution of Internal Audit/Investigation/Intelligence Activities
- Ensuring the Security of Data Controller Operations
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Transaction Security:****

- Execution of Information Security Processes
- Execution of Audit/Ethics Activities
- Execution of Access Permissions
- Execution of Activities in Compliance with Legislation
- Execution of Internal Audit/Investigation/Intelligence Activities
- Execution of Retention and Archiving Activities
- Ensuring the Security of Data Controller Operations
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Marketing:****

- Execution of Processes Related to Company/Product/Service Loyalty
- Execution of Communication Activities

- Execution of Customer Relationship Management Processes
- Execution of Performance Evaluation Processes
- Execution of Advertising/Campaign/Promotion Processes
- Execution of Marketing Processes for Products/Services
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Risk Management:****

- Execution of Emergency Management Processes
- Execution of Audit/Ethics Activities
- Execution of Internal Audit/Investigation/Intelligence Activities
- Execution of Risk Management Processes

◆ ****Professional Experience:****

- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes for Employee Candidates
- Execution of Employee Satisfaction and Loyalty Processes
- Fulfillment of Contractual and Legal Obligations for Employees
- Execution of Processes for Employee Benefits and Interests
- Execution of Training Activities
- Execution of Activities in Compliance with Legislation
- Planning of Human Resources Processes
- Execution/Control of Business Activities
- Execution of Occupational Health/Safety Activities
- Collection and Evaluation of Suggestions for Improving Business Processes
- Execution of Performance Evaluation Processes
- Execution of Wage Policy
- Execution of Talent/Career Development Activities
- Providing Information to Authorized Persons, Institutions, and Organizations
- Execution of Management Activities

◆ ****Visual and Audio Records:****

- Execution of Emergency Management Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes for Employee Candidates
- Execution of Employee Satisfaction and Loyalty Processes
- Execution of Training Activities
- Execution of Activities in Compliance with Legislation
- Ensuring Physical Space Security
- Monitoring and Execution of Legal Affairs
- Execution/Control of Business Activities
- Execution of Occupational Health/Safety Activities
- Execution of Post-Sales Support Services for Goods/Services
- Execution of Organization and Event Management
- Execution of Retention and Archiving Activities
- Tracking Requests/Complaints
- Execution of Marketing Processes for Products/Services
- Ensuring the Security of Data Controller Operations
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Race and Ethnicity:****

- Execution/Control of Business Activities
- Execution of Goods/Services Procurement Processes
- Execution of Goods/Services Production and Operations Processes
- Execution of Customer Relationship Management Processes
- Execution of Activities Related to Customer Satisfaction
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Health Information:****

- Execution of Emergency Management Processes
- Execution of Application Processes for Employee Candidates
- Execution of Employee Satisfaction and Loyalty Processes

- Fulfillment of Contractual and Legal Obligations for Employees
- Execution of Activities in Compliance with Legislation
- Execution/Control of Business Activities
- Execution of Occupational Health/Safety Activities
- Collection and Evaluation of Suggestions for Improving Business Processes
- Execution of Goods/Services Procurement Processes
- Execution of Post-Sales Support Services for Goods/Services
- Tracking Requests/Complaints
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Criminal Convictions and Security Measures:****

- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes for Employee Candidates
- Execution of Employee Satisfaction and Loyalty Processes
- Fulfillment of Contractual and Legal Obligations for Employees
- Planning of Human Resources Processes
- Execution of Occupational Health/Safety Activities
- Providing Information to Authorized Persons, Institutions, and Organizations

◆ ****Biometric Data:****

- Execution/Control of Business Activities
- Execution of Customer Relationship Management Processes
- Execution of Activities Related to Customer Satisfaction
- Providing Information to Authorized Persons, Institutions, and Organizations

► ****PERSONAL DATA RETENTION PERIODS****

DENTAPOINT retains personal data for the duration specified in the relevant laws and regulations. If no such duration is specified, personal data is processed for as long as it is required by the services provided by DENTAPOINT, then deleted, destroyed, or anonymized.

If the purpose for processing personal data has expired and the retention period has ended, personal data may be retained only for the purpose of providing evidence in possible legal disputes, asserting a related right, or establishing a defense. These retention periods are determined based on the statute of limitations and previous examples of similar requests made to DENTAPOINT. After these periods expire, the personal data is deleted, destroyed, or anonymized.

► ****THIRD PARTIES TO WHOM PERSONAL DATA IS TRANSFERRED****

DENTAPOINT informs the data subject about the categories of persons to whom personal data is transferred, in accordance with Article 10 of the KVKK. Personal data may be transferred to the following categories of persons in accordance with Articles 8 and 9 of the KVKK:

- Natural persons or private law legal entities
- Authorized Public Institutions and Organizations
- Others-Laboratories
- Others-Insurance Companies
- Shareholders
- Business Partners

► **OTHER APPLICATIONS CONDUCTED BY OUR COMPANY**

In order to process personal data based on the explicit consent of the data owner, visitors and third parties are informed about different data collection practices, and their explicit consent is obtained. Upon the request of our visitors, they are informed about the requested data, their rights, and our obligations through the necessary disclosure process.

If it is necessary to process personal data of the parties directly related to the establishment or performance of a contract, it is possible to process such personal data.

To ensure security, DENTAPOINT may engage in personal data processing activities through security camera monitoring in DENTAPOINT buildings and facilities, and for tracking guest entries and exits.

In this context, DENTAPOINT will act in accordance with the Constitution, the Law on the Protection of Personal Data (KVK Law), and other relevant legislation. The purposes of DENTAPOINT's camera monitoring activity include improving the quality of service, ensuring reliability, protecting the safety of the company, employees, and other individuals, and protecting the interests of third parties regarding the services they receive. The camera monitoring activity conducted by DENTAPOINT is carried out in accordance with the Private Security Services Law and relevant legislation. Our company commits to comply with the regulations stipulated in the KVK Law when conducting camera monitoring for security purposes. A limited number of individuals who have access to the records declare that they will protect the confidentiality of the data they access through a confidentiality agreement.

► TECHNIQUES FOR THE DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

Techniques for Deletion and Destruction of Personal Data

DENTAPOINT may delete or destroy personal data on its own decision or upon the request of the data owner if the reasons for processing personal data, although processed in accordance with the relevant legal provisions, cease to exist. The most commonly used deletion or destruction techniques by DENTAPOINT are listed below:

(i) Physical Destruction

Personal data may also be processed through non-automated means as part of a data recording system. When deleting/destroying such data, a physical destruction system is applied to ensure that the personal data cannot be used later.

(ii) Secure Deletion from Software

When deleting/destroying data processed wholly or partially by automated means and stored in digital environments, methods are used to ensure that the data is securely deleted from the software and cannot be recovered.

(iii) Secure Deletion by an Expert

In some cases, DENTAPOINT may engage an expert to delete personal data on its behalf. In this case, personal data is securely deleted/destroyed by the expert in a way that it cannot be recovered.

Techniques for Anonymizing Personal Data

Anonymization of personal data means rendering personal data impossible to link with an identified or identifiable person, even when combined with other data. DENTAPOINT may anonymize personal data when the reasons for processing personal data cease to exist in compliance with the law.

In accordance with Article 28 of the KVK Law, anonymized personal data may be processed for purposes such as research, planning, and statistics. Such processing is outside the scope of the KVK Law, and the explicit consent of the data owner will not be required. Since personal data anonymized in this way will fall outside the scope of the KVK Law, the rights stipulated in the Policy will not apply to these data.

The anonymization techniques that may be used by DENTAPOINT are as follows:

- **Masking**
Data masking is the method of removing the primary identifying information from the data set, thereby rendering the personal data anonymous.
- **Aggregation**
The aggregation method involves combining multiple data points, rendering the personal data non-associable with any individual.
- **Data Derivation**
Data derivation involves creating more general content from the data, making the personal data non-associable with any individual.
- **Data Shuffling**
The data shuffling method ensures that the values within the personal data set are scrambled, breaking the link between the values and individuals.

► RIGHTS OF THE DATA OWNER AND EXERCISING THESE RIGHTS

Rights of the Personal Data Owner

Personal data owners have the following rights:

1. To learn whether their personal data is processed,
2. To request information regarding the processing of their personal data,
3. To learn the purpose of processing their personal data and whether it is used in accordance with this purpose,
4. To know the third parties to whom personal data is transferred within the country or abroad,
5. To request the correction of their personal data if it is incomplete or incorrectly processed, and to request notification of the correction to third parties to whom the data has been transferred,
6. To request the deletion or destruction of their personal data, even if it has been processed in accordance with the KVK Law and other relevant laws, if the reasons for processing cease to exist, and to request that the third parties to whom the data has been transferred be notified of this deletion or destruction,
7. To object to a result against themselves arising from the exclusive analysis of processed data by automated systems,
8. To claim compensation for damages if they suffer harm due to unlawful processing of their personal data.

Cases Where the Data Owner Cannot Assert Their Rights

According to Article 28 of the KVK Law, the following cases are excluded from the scope of the KVK Law, and therefore the data owner cannot assert their rights in these cases:

1. Processing of personal data for purposes such as official statistics and anonymization for research, planning, and statistics,
2. Processing of personal data for artistic, historical, literary, or scientific purposes, or within the scope of freedom of expression, provided that national defense, national security, public security, public order, economic security, privacy of private life, or personal rights are not violated or constitute a crime,
3. Processing of personal data within the scope of preventive, protective, and intelligence activities carried out by public institutions and organizations authorized by law for national defense, national security, public security, public order, or economic security,
4. Processing of personal data by judicial authorities or execution authorities concerning investigation, prosecution, trial, or execution processes.

According to Article 28/2 of the KVK Law, in the following cases, except for the right to claim compensation for damages, the data owners cannot assert their rights:

1. When personal data processing is necessary for the prevention of crime or criminal investigation,

2. When personal data made public by the data owner is processed,
3. When personal data processing is necessary for the performance of supervisory or regulatory duties by authorized public institutions and organizations and professional organizations in the nature of public institutions based on the authority granted by law, or for disciplinary investigations and prosecutions,
4. When personal data is processed by judicial authorities or execution authorities regarding investigation, prosecution, trial, or execution processes.