1. INTRODUCTION

As the data controller, it is of great importance for Ekol Baz Özel Sağlık Hizmetleri Ticaret Anonim Şirketi (will be referred to as “Ekol” or “Company”) to protect the personal data of its patients, employees and other real persons with whom it is in contact. The purpose of this policy and other written policies for the processing and protection of personal data is the legal processing and protection of the personal data of our patients, potential patients, suppliers, employees, employee candidates, visitors, employees of the institutions we cooperate with and third parties who contact Ekol.

In this context, necessary administrative and technical measures are taken by Ekol for the processing and protection of personal data in accordance with the General Data Protection Regulation (GDPR), as well as the local legislation.

In this Policy, the following basic principles adopted by Ekol for the processing of personal data will be explained:

Processing personal data within the scope of consent,

Processing personal data in accordance with the law and honesty rules,

Keeping personal data accurate and up-to-date when necessary,

Processing personal data for specific, explicit and legitimate purposes,

Related, limited and measured processing of personal data for the purpose for which they are processed,

Keeping personal data for as long as required by the relevant legislation or for the purpose for which they are processed,

Clarifying and informing the persons whose personal data are processed,

Creating the necessary infrastructure for the persons whose personal data are processed to exercise their rights,

Taking the necessary measures for the protection of personal data,

To act in accordance with the relevant legislation and the regulations of the Personal Data Protection Board in the determination and implementation of the processing purposes of personal data, transferring them to third parties,

Special regulation of the processing and protection of sensitive personal data.

2. PURPOSE OF THE POLICY

The main purpose of this Policy is to make statements about the personal data processing activity carried out by Ekol in accordance with the law and the systems adopted for the protection of personal data, and in this context, to provide transparency towards the persons with whom our company is associated.

3. SCOPE OF THE POLICY

This Policy relates to all personal data of our patients, suppliers, employees, employee candidates, visitors, employees of the institutions we cooperate with and third parties that are processed automatically or non-automatically, provided that they are part of any data recording system.

4. ISSUES REGARDING THE PROTECTION OF PERSONAL DATA

Ekol takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of the personal data it processes, illegal access to the data, and to ensure the preservation of the data in accordance with Article 32 and Article 78 of the GDPR, and in this context, it carries out the necessary audits or has the audits conducted.

4.1. Measures Taken to Ensure Legal Processing of Personal Data and to Prevent Unlawful Access to Personal Data

Ekol takes technical and administrative measures according to technological possibilities and implementation costs in order to ensure that personal data are processed in accordance with the law and to prevent unlawful access.

4.1.1. Technical Measures

The main technical measures taken by Ekol to ensure the legal processing of personal data and to prevent unlawful access are listed below:

Network security and application security are provided.

A closed system network is used for personal data transfers via the network.

Encryption is done.

Security measures are taken within the scope of procurement, development and maintenance of information technology systems.

The security of personal data stored in the cloud is ensured.

An authorization matrix has been created for employees.

Access logs are kept regularly.

Cyber security measures have been taken and their implementation is constantly monitored.

The authorizations of employees who have a change in duty or quit their job in this field are removed.

Current anti-virus systems are used.

Firewalls are used.

Necessary security measures are taken regarding entry and exit to physical environments containing personal data.

Both the backup of personal data and the security of the backup of the personal data are ensured.

User account management and authorization control system is implemented, and these are also followed.

Log records are kept without user intervention.

If sensitive personal data is to be sent via e-mail, it must be sent in encrypted form and using a KEP or corporate mail account.

Personal data transferred in portable memory, CD and DVD media are encrypted and transferred.

Intrusion detection and prevention systems are used.

4.1.2. Administrative Measures

Administrative measures taken by Ekol to process personal data in accordance with the law and to prevent unlawful access:

There are disciplinary regulations that include data security provisions for employees.

Training and awareness activities are carried out periodically for employees on data security.

Institutional policies on access, information security, use, storage and destruction have been prepared and are being implemented.

Confidentiality commitments are made.

The signed contracts contain data security provisions.

Extra security measures are taken for personal data transferred via paper and the relevant document is sent in confidential document format.

Personal data security policies and procedures have been determined.

Personal data security issues are reported quickly.

Personal data security is monitored.

Physical environments containing personal data are secured against external risks (fire, flood, etc.).

The security of environments containing personal data is ensured.

Personal data is reduced as much as possible.

In-house periodic and/or random audits are conducted and made.

Existing risks and threats have been identified.

Protocols and procedures for special quality personal data security have been determined and implemented.

Data processing service providers are periodically audited on data security.

Awareness of data processing service providers on data security is ensured.

4.2. Supervision of the Measures Taken for the Protection of Personal Data

Ekol has those concerned with the Protection of Personal Data. On behalf of Ekol, which is the data controller, this team personally carries out the necessary audits in order to ensure the implementation of the provisions of the Law in its own institution or organization, in accordance with its obligation arising from Article 32 of the Law and gets support from competent institutions when needed. According to the results of this audit, the detected violations, negativities and non-compliances are reported to the legal unit within the team and necessary measures are taken regarding these issues. In the event that an external service is outsourced by Ekol due to technical requirements regarding the storage of personal data, additional agreements are signed with the relevant companies to whom personal data is transferred in accordance with the law and the persons to whom personal data are transferred will take the necessary security measures for the protection of personal

data and that these measures will be complied within their own organizations. In addition, Ekol makes agreements with its personnel to comply with personal data protection measures in recruitment processes and in-house disciplinary policies.

5. RIGHTS AND REQUESTS OF THE PERSONAL DATA OWNER

Ekol, as the data controller, has established the Personal Data Application and Response Procedure, which is an annex to the personal data inventory, and a written template for applications that do not meet the application conditions specified in the law. Technical preparations have been made in order to carry out the necessary actions in accordance with these procedures.

Providing that the persons whose personal data are processed submit their requests regarding the rights listed below via a personal application showing the hard copy of their ID, or in writing or by using a previously registered electronic email address (KEP), by using a secure electronic signature, a mobile signature or by using the electronic mail address which has been previously registered in EKOL communication system and about which EKOL has been informed or on condition that they communicate their identities to Ekol in a verifiable form through a software or application developed for this purpose, the Company will respond to the request free of charge within thirty days at the latest, depending on the nature of the request. A detailed explanation on this matter is given below in Article 20 of this policy.

The persons whose personal data are processed will be able to claim all the rights in the relevant article of the law, including all data processing phases, its purposes and the information about the transfer of their personal data upon their application to be made in accordance with this procedure.

6. PROTECTION OF PRIVATE PERSONAL DATA

With the GDPR, special importance is attached to certain personal data due to the risk of causing victimization or discrimination when processed unlawfully. These data are; race, ethnicity, political thought, philosophical belief, religious affiliation, union membership, health, sexual life and sexual orientation, biometric and genetic data.

Ekol acts sensitively in the protection of sensitive personal data, which is determined as "sensitive" with the GDPR and is processed in accordance with the law. In this context, technical and administrative measures taken by Ekol for the protection of personal data are carefully implemented in terms of sensitive personal data and necessary audits are provided within Ekol.

7. TRAINING OF EKOL EMPLOYEES ON PROTECTION AND PROCESSING OF PERSONAL DATA

Ekol provides its employees with the necessary training in order to prevent the illegal processing of personal data as well as illegal access to the data, and to raise awareness about data protection.

8. ISSUES REGARDING THE PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution and Article 5 of the GDPR, Ekol engages in personal data processing activities in a fair and transparent manner in accordance with the law, accurately and, when necessary, for up-to-date, specific, clear and legitimate purposes and in a limited and prudent manner in connection with the purpose of processing personal data. Ekol preserves the integrity and confidentiality of personal data for as long as required by law or for the purpose of processing personal data. Ekol collects the personal information of its patients, employees, visitors, supplier company employees and third parties; identity information (name, surname, TR identity number, gender, age, date of birth), contact information (e-mail address, telephone number, address information), personal data, financial data, occupational data, audio-visual data, education data , family members data, health information, information on criminal convictions and security measures, military service information, transaction security information, physical space security, and while processing these data, the data subjects whose personal data are processed can benefit from Ekol's services, products and services effectively. As a result of these services, it operates by, taking into account data minimization within the framework of the performance of contracts, fulfilment of work and financial / legal / commercial obligations, as well as being able to be informed about marketing and innovations as a result of these services.

Ekol informs the persons whose personal data is processed in accordance with Article 13 of the GDPR and requests the consent of the persons concerned in cases where consent is required, and processes this personal data based on the criteria set out below.

8.1. Legality, Fairness and Transparency

Ekol processes personal data in accordance with the principles introduced by legal regulations and the legal processing conditions in the Law. In accordance with the principle of compliance with the law, Ekol carries out a transparent data processing process, taking into account the interests and reasonable expectations of the persons concerned, while trying to achieve its goals in data processing.

8.2. Truth

Keeping personal data accurate and up to date is essential for Ekol to protect the fundamental rights and freedoms of the person concerned. Ekol has an active duty of care to ensure that personal data is accurate and up to date when necessary. For this reason, all communication channels are open in order to keep the information of the persons whose personal data are processed by Ekol accurate and up to date.

8.3. Data Minimization

Ekol clearly and precisely determines the legitimate and lawful purpose of processing personal data and continues to process personal data limited only to the personal data necessary for the realization of this purpose.

8.4. Limitation of Purpose

Ekol processes personal data for purposes related to its field of activity and necessary for the conduct of its business. For this reason, Ekol processes personal data in a way that is suitable for the realization of the determined purposes and avoids the processing of personal data that is not related to the realization of the purpose or that is not needed.

8.5. Limitation of Storage

Ekol retains personal data only for as long as specified in the relevant legislation or required for the purpose for which they are processed. In this context, Ekol first determines whether a period is foreseen for the storage of personal data in the relevant legislation, and if a period is determined, it acts in accordance with this period. If a period has not been determined, personal data is stored for the processing purpose and as long as the period specified in the Retention and Disposal Policy published by Ekol. Ekol acts on the basis of the retention periods in the personal data inventory, and at the end of the periods specified here, personal data is deleted, destroyed or anonymized according to the nature of the data and the purpose of use, within the framework of the obligations under the Law.

8.6. Integrity and Confidentiality

In the personal data processing activities carried out by Ekol, security measures are taken to the extent required by the activity. The technical and administrative measures in the local legislation and GDPR are based on the determination of these data security measures taken to prevent data loss, unauthorized access and illegal data processing

8.7. Accountability

Ekol has a legal obligation to comply with the above-mentioned principles. In order to fulfill these obligations, the rights recognized by the Law are established for all persons whose personal data are processed and transparency is ensured in data processing activities.

9. ILLUMINATING AND INFORMING THE PERSONAL DATA OWNER

In accordance with Article 13 of the KVK Law, Ekol informs the persons whose personal data are processed during the acquisition of personal data. In this context, Ekol informs the persons considering the identity of the data controller, the identity of its representative, if any, the purpose for which the personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method of collecting personal data and the rights of the persons whose personal data are processed for legal reasons, and the nature of the data subject and the period of data processing. Along with this policy, the customer clarification text, cookie policy and application form have also been published on the Ekol website.

10. TRANSFERRING PERSONAL DATA

Ekol can transfer the personal data and sensitive personal data of the data subject to third parties by taking the necessary security measures in line with the purposes of processing personal data in accordance with the law. Personal data can be transferred by Ekol to foreign countries declared to have adequate protection by the KVK Board or, in the absence

of sufficient protection, to foreign countries where data controllers in Turkey and the relevant foreign country undertake in writing to provide adequate protection and where permission is granted by the KVK Board. The reasons for the transfer are explained below:

If there is a clear regulation in the law regarding the transfer of personal data,

If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,

If personal data transfer is mandatory for Ekol to fulfil its legal obligations,

If personal data transfer is necessary for the establishment, exercise or protection of a right,

If personal data transfer is necessary for the legitimate interests of Ekol, provided that it does not harm the fundamental rights and freedoms of the person concerned.

11. EKOL PERSONAL DATA INVENTORY AND CLASSIFICATION OF PERSONAL DATA

At Ekol, in line with Ekol's legitimate and lawful personal data processing purposes, based on and limited to one or more of the personal data processing conditions specified between Articles 5 and 11 of the KVK Law, in particular the provisions of the local legislation. In accordance with the principles set forth in Article 5 of the GDPR, in compliance with all obligations set forth in the GDPR and limited to the persons whose personal data are processed within the scope of this Policy, the personal data in the categories specified below are processed by informing the relevant persons.

Ekol has created a personal data inventory in accordance with the Data Controllers Registry Regulation issued by the Personal Data Protection Authority. This data inventory includes data categories, data source, data processing purposes, data processing process, recipient groups to which data is transferred, and retention periods. In this context, the following types of data categories are included in the Ekol personal data inventory, but it is not limited to these types.

PERSONAL DATA CATEGORY

PERSONAL DATA CATEGORY DISCLOSURE

It is the data group that can be used to reach the person (Phone, address, e-mail).

Identity Data

It is the data group that contains information about the person's identity (Name, surname, identity number, place of birth, date of birth, gender, passport number, nationality data).

Audio/Visual Data

It is a data group (Photo) that contains visual and auditory data of the person.

Physical Space Security Data

It is the data group containing the camera recording of the person (Camera recording).

Transaction Security Data

It is the data group containing the digital traces formed as a result of the processing of personal information (Log Records, IP address information, Cookie Information).

Finance Data

It is the data group containing the financial information of the person (Bank account number, IBAN number, card information)

Professional Experience Data

It is the data group that contains the information about the profession of the person (information of the institution where he/she works, registry of the professional chamber).

Health Data

It is a data group related to the health status of the person (Health report, medication information, hearing and vision information, consultation report, examination information, past health information).

As shown in the table above, Ekol has established Ekol Personal Data Inventory within the scope of data processing activities and both considering the types of the data used within the company and Ekol Personal Data Storage and Retention Policy.

12. PURPOSE OF PROCESSING PERSONAL DATA

Ekol carries out data processing activities by providing the purposes it has determined, provided that it is not contrary to the personal data processing conditions in the Bylaw. These purposes are:

Execution of Emergency Management Processes,

Execution of Information Security Processes,

Conducting Audit/Ethics Activities,

Conducting Educational Activities,

Execution of Access Authorizations,

Execution of Activities in Compliance with the Legislation,

Execution of Finance and Accounting Affairs,

Execution of Company/Product/Services Loyalty Processes,

Providing Physical Space Security,

Execution of Assignment Processes,

Follow-up and Execution of Legal Affairs,

Carrying out Internal Audit / Investigation / Intelligence Activities,

Execution of Communication Activities,

Execution/Audit of Business Activities,

Execution of Occupational Health/Safety Activities,

Receiving and Evaluating Suggestions for Improvement of Business Processes,

Ensuring Business Continuity and Execution of Activities,

Execution of Service Procurement Processes,

Execution of After-Sales Support Services,

Execution of Service Sales Processes,

Execution of Customer Relationship Management Processes,

Execution of Activities for Customer Satisfaction,

Organization and Event Management within the Company,

Conducting Marketing Analysis Studies,

Execution of Performance Evaluation Processes,

Execution of Advertising / Campaign / Promotion Processes,

Execution of Risk Management Processes,

Execution of Storage and Archive Activities,

Conducting Social Responsibility and Civil Society Activities,

Execution of Contract Processes,

Execution of Sponsorship Activities,

Execution of Strategic Planning Activities,

Follow-up of Requests/Complaints,

Ensuring the Security of Movable Property and Resources,

Execution of Supply Chain Management Processes,

Execution of Wage Policy,

Execution of Marketing Processes of Services,

Ensuring the Security of Data Controller Operations,

Providing Information to Authorized Persons, Institutions and Organizations,

Execution of Management Activities,

Creating and Tracking Visitor Records,

Carrying out studies to improve service quality and providing better service,

Issuing invoices for our services,

Answering questions and complaints,

Taking the necessary technical and administrative measures within the scope of data security,

Providing the necessary information in line with the requests and inspections of regulatory and supervisory institutions and official authorities,

Preservation of information on data that must be kept in accordance with the relevant legislation.

13. PERSONAL DATA STORAGE PERIOD

Ekol keeps personal data for the period specified in these legislations, in case it is stipulated in the relevant laws and regulations, with priority being given to the periods regulated in the local legislation.

If a period of time is not regulated in the legislation regarding how long personal data should be kept, the personal data is stored for the period that requires it to be kept in accordance with Ekol's practices and industry practices, depending on the activity Ekol carries out while processing that data, and then it is created by Ekol in accordance with the nature of the data. It is deleted, destroyed or anonymized in accordance with the Personal Data Retention and Destruction Policy.

If the purpose of processing personal data has ended and the storage periods determined by the relevant legislation and Ekol have expired, personal data can be stored only to provide evidence in possible legal disputes or to assert the relevant right related to personal data or to establish a defence. Despite the expiry of the statute of limitations and the statute of limitations for asserting the aforementioned right in the establishment of the periods herein, retention periods are determined on the basis of the examples previously submitted to Ekol on the same issues. In this case, the stored personal data is not accessed for any other purpose, and only when necessary to use it in the relevant legal dispute, access to the relevant personal data is provided. Here, too, personal data is deleted, destroyed or anonymized after the aforementioned period expires.

14. THIRD PARTIES TO WHICH PERSONAL DATA IS TRANSFERRED BY EKOL AND THEIR PURPOSE

Ekol may transfer the personal data of the data subjects whose personal data is processed under this Policy to the following stakeholder categories in accordance with the provisions of Article 44-50 of the GDPR and the provisions of the local legislation:

Ekol business partners and group companies,

Bank and insurance companies,

Travel agencies,

Hotels,

Ekol suppliers,

Ekol company officials,

Lawyers and auditor companies,

Legally authorized public institutions and organizations.

The transfer scope and data transfer purposes are stated below:

Persons to whom Data Transfer can be made,

Definition,

Data Transfer Purpose,

Business partner.

It defines the parties with which Ekol establishes business partnerships for purposes such as carrying out various projects and receiving services while carrying out its commercial activities.

It is transferred on a limited basis to ensure the fulfilment of the purposes for which the business partnership was established.

Supplier

It defines the parties that provide services to Ekol on a contractual basis, in accordance with Ekol's orders and instructions, while carrying out Ekol's commercial activities.

It is transferred on a limited basis in order to ensure that the services that Ekol outsources from the supplier and that are necessary to carry out Ekol's commercial activities are provided to Ekol.

Authorized Public Institutions and Organizations

It defines the public institutions and organizations authorized to receive information and documents from Ekol in accordance with the provisions of the legislation.

It is transferred for a limited purpose in cases where public institutions and organizations demand and provide a legal basis.

15. PROCESSING PERSONAL DATA

15.1. Processing of Personal Data

The express consent of the person whose personal data is processed is only one of the legal bases that makes it possible to process personal data in accordance with the law. Apart from express consent, personal data may also be processed in the presence of one of the conditions specified in the law. The basis of the personal data processing activity can be only one of the conditions stated below, or more than one of these conditions can be the basis of the same personal data processing activity.

Processing Conditions

Scope

Sample

Provision of Law

Within the Scope of Legal Legislation

Keeping the health information of the patients in accordance with the legislation.

Performance of Contract

Sales Agreement, Service Agreement, Commitments etc.

Making a contract on Ekol's services.

Legal Responsibility of Data Controller

Financial and Administrative Audits, Social Security Legislation, Compliance with Sector-Oriented Regulations.

Sharing information in audits specific to areas such as the Social Security Institution.

Making Public

The person concerned submits his/her information to the public.

Announcement of the contact information of the person to be reached in case of emergency.

Establishment, Protection, Use of Right

Filing a lawsuit and request/complaint etc. mandatory data to be used in business.

Retaining necessary information about an employee leaving the job during the statute of limitations.

Legitimate Interest

Provided that the fundamental rights of the data subject are not harmed, data may be processed if it is necessary for the legitimate interest of the data controller.

Data processing for the purpose of applying rewards and bonuses that increase employee loyalty.

16. DATA PROTECTION IMPACT ASSESSMENT

If Ekol makes any changes or innovations regarding personal data processing activities, it is obliged to perform the Data Protection Impact Assessment regulated in Article 35 of the Regulation. The procedures and principles on how to make this assessment are regulated in the Data Protection Impact Assessment Analysis Procedure.

17. PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT AT EKOL COMPANY BUILDING ENTRANCES AND INSIDE THE BUILDING

In order to ensure security by Ekol, personal data processing activities are carried out in Ekol buildings and facilities for monitoring with security cameras and tracking guest entries and exits.

Ekol processes personal data by using security cameras and recording guest entries and exits.

Ekol, within the scope of surveillance with security cameras; It aims to protect the interests of the company and other persons in order to ensure their safety. This monitoring activity is carried out in accordance with local legislation and article 32 of the GDPR. In this context, the information that monitoring is done with a camera is announced to all employees and visitors, and people are thus informed. Notifications are posted at the entrances of the monitoring areas. Ekol takes the necessary technical and administrative measures to ensure the security of personal data obtained as a result of camera monitoring in accordance with Article 32 of the GDPR.

17.1. Follow-up of Guest Entrance and Exit in Ekol Building, Inside the Facilities and at Facility Entrances

Personal data processing is carried out by Ekol for the purpose of ensuring security and for other purposes specified in this Policy, in order to monitor guest entries and exits at Ekol buildings and facilities. While obtaining the identity data of the people who come to Ekol buildings as guests, or through the texts posted by Ekol or made available to the guests in other ways, the relevant persons are informed in this context. The data obtained for the purpose of tracking guest entry-exit is only processed for this purpose and the personal data of the person concerned is recorded in the data recording system in the physical environment.

17.2. Keeping Log Records of Access to Software Provided to Employees at Ekol Facilities

For the purpose of ensuring security and other purposes specified in this Policy, Ekol provides internet access to visitors who request it during their stay in the buildings and facilities. In this case, log records of internet access are kept in accordance with the provisions of the local legislation, Law No. 5651 and data security in GDPR. These records are only processed when requested by authorized public institutions and organizations or in order to fulfil the relevant legal obligation during the audit processes to be carried out within Ekol.

18. TERMS OF DISPOSAL (DELETION, DESTRUCTION AND ANONYMIZATION) OF PERSONAL DATA

Without prejudice to the provisions of the local legislation, personal data will be deleted, destroyed or anonymized upon Ekol's own decision or upon the request of the personal data subject, in the event that the reasons requiring its processing cease to exist, although it has been processed in accordance with the provisions of the relevant law. Ekol has established a policy in this regard in accordance with the provisions of the regulation, and in accordance with this policy, it carries out the destruction process according to the nature of the data.

19. RIGHTS OF PERSONAL DATA OWNERS; USE OF THESE RIGHTS

Ekol informs him of the rights of the data subject regulated between Articles 12 and 23 of the GDPR and guides the data subject whose personal data are processed on how to use these rights, and Ekol follows the 13th article of the GDPR in order to evaluate the rights of the data subjects and to inform the relevant persons. It carries out the necessary channels, internal functioning, administrative and technical regulations in accordance with the article.

19.1. The Rights of the Relevant Person and the Use of These Rights

19.1.1. Rights of the person whose personal data is processed

The persons whose personal data are processed have the following rights:

Necessary at contract establishment or pre-contractual stages

Legal obligation to which the controller is subject

Processing is necessary in order to protect the vital interests of the data subject or another natural person.

The performance of a task performed in the public interest, or the exercise of a formal authority vested in the controller

Unless the data subject is a child, processing is necessary in line with the interests in question.

19.1.3. The exercise of the rights of the person whose personal data is processed

Persons whose personal data are processed will be able to submit their requests regarding their rights set forth in this Policy to Ekol free of charge, with the information and documents that will identify them, by filling out and signing the Application Form, using the methods specified below or other methods determined by the Personal Data Protection Board. Comprehensive regulation on this subject has been made in the Ekol Personal Data Application and Response Procedure and the Ekol Patient Disclosure Text.

Sending copy of the form signed in ink at …. address by hand or in writing via registered mail with return receipt to the address "……" or applying in person,

Filling the form at address …… and after signing it with the "secure electronic signature" within the scope of the Electronic Signature Law No. 5070, sending the secure electronic signature form to the …….. Kep address via a registered email or by sending an e-mail to info@ekolhospital address via a registered email in our systems.

In order for the above-mentioned application to be accepted as a valid application, in accordance with the Communiqué on Application Procedures to the Data Controller, the relevant person must provide the following information:

a) Name, surname and signature if the application is written,

b) For citizens of the Republic of Turkey, T.C. identity number, nationality for foreigners, passport number or identification number, if any,

c) Domicile or workplace address based on notification,

ç) E-mail address, telephone and fax number for notification, if any,

d) Demand Topic,

Otherwise, the application will not be considered as a valid application. For applications to be made without filling out the application form, the issues listed here must be conveyed to Ekol in full.

In order for third parties to request an application on behalf of the persons whose personal data are processed, a special power of attorney issued by the relevant person through a notary public on behalf of the applicant.

20. RELATIONSHIP OF EKOL PERSONAL DATA PROTECTION AND PROCESSING POLICY WITH OTHER POLICIES

Ekol has established the principles set forth in this document on the basis of policies regarding other data assets within Ekol and sub-procedures for internal use regarding the protection and processing of personal data.

ANNEX-1 DEFINITIONS

Open Consent: Consent on a particular subject, based on information and expressed with free will.

Anonymization: It is the change of personal data in such a way that it loses its quality as personal data and this situation cannot be undone. Ex: Masking, aggregation, data corruption etc. making personal data incapable of being associated with a natural person through techniques.

Application form: “Application Form Regarding the Applications to be Made by the Related Person to the Data Controller in accordance with the Law on Protection of Personal Data No. 6698, which includes the application to be made by the persons whose personal data are processed to exercise their rights”.

Employee Candidate: Real persons who have applied for a job at Ekol by any means or have opened their CV and related information.

Employees, Shareholders and Officials of Collaborating Institutions: Real and legal persons, including shareholders and officials of these institutions, who work in institutions (such as but not limited to business partners, suppliers) with which Ekol has any business relationship.

Business Partner: Parties with whom Ekol establishes business partnerships for purposes such as carrying out various projects, receiving services, in person or together with them while carrying out its commercial activities.

Processing of Personal Data: Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available personal data by fully or partially automatic or non-automatic means provided that it is a part of any data recording system, all kinds of operations performed on data such as classification or prevention of use.

Related person: The real person whose personal data is processed, e.g., customer, staff.

Personal Data: Any information relating to an identified or identifiable natural person. Therefore, the processing of information regarding legal persons is not within the scope of the Law, e.g., name-surname, TCKN, e-mail, address, date of birth, credit card number, etc.

Sensitive Personal Data: Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Supplier: Parties that provide services to Ekol on a contractual basis, in accordance with Ekol's orders and instructions, while carrying out Ekol's commercial activities.

Third Party: Natural persons whose personal data are processed within the scope of the policy, who are not defined differently within the scope of the policy, e.g., family members, former employees.

Data Processor: A natural or legal person who processes personal data on behalf of the data controller, based on the authority given by the data controller, e.g., departments working within Ekol.

Data Controller: The person who determines the purposes and means of processing personal data and manages the place where the data is kept systematically (data recording

system). Within the scope of this policy, Ekol Baz Özel Sağlık Hizmetleri Ticaret Anonim Şirketi is the data controller.

Deletion of Data: It means that all relevant users' data within the company are encrypted to prevent access to personal data and only the data protection officer has this password.

Data Destruction: It refers to the complete elimination of personal data, physically or technologically, in a way that cannot be recovered.

Visitor: Real persons who have entered the physical premises owned by Ekol for various purposes or visited our websites.