PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

1.1 Purpose

The Personal Data Retention and Destruction Policy (the "Policy") has been prepared in order to determine the methods and principles regarding the retention and destruction activities performed by Ilab Holding A.S. (the "Company").

Operations and actions concerning the retention and destruction of personal data are realized in compliance with the Policy that has been prepared by the Company accordingly.

1.2 Scope

The personal data belonging to the Compan'y employees, employee candidates, service providers, visitors and other third parties are within the scope of this Policy and this Policy is implemented for all recording media, owned or managed by the Company, where the personal data are processed, and in the activities aimed for the processing personal data.

1.3 Definitions

The following terms used in this Policy have the meanings shown in the table below, unless they are defined differently within the Policy.

TERM	DEFINITION
Receiver group:	Means the real or legal entity category to which personal data are transferred by the data supervisor.
Open Consent	Means the consent, based on information on a specific subject and expressed with free will
Anonymization	Means making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching with other data
Secondary Legislation	In accordance with the law, it means any regulation, circular, communiqué, policy decision or similar administrative decision or general opinion issued or taken by the Personal Data Protection Authority.

Related Users	Means the persons who are inside the organization of the data officer or process personal data in line with the authorization and instruction received from the data officer, except the person or unit responsible for storing, protecting and backing up the data.
Destruction	Means deletion, destruction or anonymization of personal data.
Law	Means the Personal Data Protection Law no. 6698.
Recording Media	Means any environment where personal data is fully or partially automated or processed by non-automated means provided that it is not a part of any data recording system.
Personal Data Processing Inventory	Means the inventory attached to this Policy where personal data processing activities carried out by our company in the capacity of data controller, depending on business processes, the maximum period required for the purposes for which personal data is processed and created by associating personal data with the purposes of processing, the data category, the transferred recipient group and the data subject group, personal data envisaged to be transferred to foreign countries and measures taken regarding data security are detailed.
Personal Data	Means all data concerning a real entity whose identity is known or can be determined.
Processing Personal Data	Means all types of processes carried out on data such as the acquisition, recording, storage, maintenance, revision, rearrangement, disclosure, transfer, receipt, making available, classification, or prevention of the use of personal data through fully or partially automatic methods or non-automatic methods, provided that they are not part of any data recording system.
Board	Means the Personal Data Protection Board.
Agency	Means the Personal Data Protection Agency.
Sensitive Personal Data	Data related with race, ethnic origin, political opinion, philosophical belief, religion, sect or other faiths, appearance, association, foundation or union membership, health, sexual life, penal conviction and safety precautions and Biometric and

Periodical Destruction	Means the deletion, destruction or anonymization process that will be carried out automatically at repetitive intervals and specified in this Policy, in the event that all of the personal data processing conditions in the law are eliminated.
Registry	Means the Data Controllers Registry, which is a registration system where data controllers have to register and declare information about data processing activities.
Deletion	Means making personal data inaccessible and non-reusable for Relevant Users in any way.
Retention and Destruction Policy	Means the policy that the Company has prepared within the framework of the Regulation on the Deletion, Destruction or Anonymization of Personal Data, regulating the procedures and principles regarding deletion and destruction.
Company	Ilab Holding A.S.
Data Processor	Refers to the real or legal person who processes Personal Data on behalf of the Data Controller based on the authority given by it.
Data Protection Commission	Means Personal Data Protection Commission of the Company. Consists of Altug Inan, Simal Konanc, Ezgi Kizmaz and Samet Uzun.
Data Owner	Data Owner, defined as "Relevant Person" in the Law, refers to the real person whose Personal Data is processed. Data Owners also include customers, internet users, individuals in communication, e-mail and marketing database lists, employees, contractors and suppliers.
Data Controller	The real or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
Regulation on Data Controllers Registry	Means the Regulation on the Data Controllers Registry, which entered into force on 1 January 2018.
Destruction	Means making personal data inaccessible, irretrievable and reusable by anyone in any way.

2. RESPONSIBILITY AND DISTRIBUTION OF TASKS

All units and employees of the Company provide active support to the units that are responsible to take technical and administrative measures aimed to ensure data security in all media where personal data are processed, in order to make sure that the technical and administrative measures taken by the responsible units within the scope of the Policy are duly implemented, illegal processing of personal data is prevented, illegal access to personal data is prevented and the data are legally stored, by training and increasing the awareness, monitoring and continuously supervising the unit employees.

The distribution of the titles, departments and duty descriptions of those involved in the retention and destruction processes of personal data is shown below.

Table : 1

TITLE	DEPARTMENT	DUTY
Chairman of Board of Directors	Management	Responsible for ensuring that employees act in accordance with the policy.
Data Protection Commission	Management	Responsible for monitoring compliance with the policy in the processes where personal data is processed and providing consultancy to the relevant units in the changes in the processes.
CFO	Management	Responsible for the preparation, development, execution, reviewing and updating of the Policy in relevant environments
Technology Services Manager	IT	Responsible for providing the technical solutions needed in the implementation of the Policy.
HR, Accounting, Audit, Product design, Advertising Sales, Digital Marketing, Data Analytics	Other Departments	Responsible for the execution of the Policy in accordance with their duties.

3. RECORDING MEDIA

Personal data are securely stored by the Agency in the media listed in Table 2, in compliance with the law.

Table: 2

Electronic Media	Physical Media
Servers (backup, e-mail, database, web, file share etc.) 1 Software (office software, other software used as per the business) Information security devices (firewall, intrusion detection and blocking, log file, antivirus, etc.) Personal computers (Desktop, laptop) Mobile devices (phone, tablet, etc.) Optic disks (CD, DVD, etc.) Removable memories (USB, Memory Card, etc..) Printer, scanner, photocopier	Paper (Files and folders) Written, printed, visual media

4. STATEMENTS CONCERNING RETENTION AND DESTRUCTION

Personal data of the employees, employee candidates, customers, visitors and employees of the third parties, establishments and institutes with which the Company is in relationship as the service provider is retained and destroyed by the Company in accordance with the Law. In this context, the explanations regarding retention and destruction are as follows:

4.1. Retention

The Company stores the personal data it obtains within the framework of its activities, as regulated in the Personal Data Protection Law and secondary legislation, for the period stipulated in the applicable legislation or suitable for our processing purposes.
Regarding processing and retention, rules regarding processing personal data in article 3 of the Law, being connected, limited and measured to the purpose of processing the processed personal data and keeping it during the period necessary for their purpose in article 4, processing personal data terms in articles 5 and 6.

4.1.1 Legal Reasons for Retention

Current Labor Law, Financial Legislation, OHS Law and other legislation and secondary regulations subject to the conduct of business and transactions

4.1.2 Purposes of Processing

- Execution of human resources processes,
- Establishing corporate communication,
- Ensuring physical security,
- Fulfillment of the obligations arising from the signed contracts (employment contract,
  service agreement etc)
- Ensuring the fulfillment of legal obligations as required or required by legal regulations (financial legislation, labor law, etc.)
- Getting in contact with real/legal persons who have a business relationship with the company
- Making legal reporting
- Providing information requested by public authorities
- Obligation of proof as evidence in legal disputes that may arise in the future.

4.1.3 Reasons Necessitating Destruction

Personal Data is deleted, destroyed or ex officio deleted, destroyed or anonymized by the company at the request of the person concerned in case of;

- Changing or abolishing the provisions of the relevant legislation, which is the basis for processing, disappearing of the purpose that requires processing or storage,

- The related person withdraws his open consent, under circumstances where personal data are only processed as pursuant to open consent requirement,

- The application filed by the related person regarding the deletion and destruction of his personal data as per article 11 of the Law is accepted by the Company,

- The related person files a complaint to the Board, under circumstances where the Company rejects the application filed by the related person, requesting the deletion, destruction or anonymization of his personal data, finds the given response inadequate or does not respond within the period set forth in the Law, and this request is approved by the Board,

- The maximum period necessitating the retention of personal data has expired and there are no conditions that would justify the retention of personal data for a longer period,

situations.

1. TECHNICAL AND ADMINISTRATIVE MEASURES

Technical and administrative measures are taken by the Company within the scope of the adequate measures determined and announced by the Board for sensitive personal data as per article 12 and the fourth paragraph of article 6 of the Law, for securely retaining personal data, preventing illegal processing and access, and destroying personal data in compliance with the law.

5.1. Technical Measures

The measures taken by the company regarding the protection of personal data are as follows.

- Risks and threats that may impact the continuity of the information system are monitored continuously as a result of information security incident management and real-time analyses.

- Access to the information system and authorization of users are made with the access and authorization matrix through security policies over the active corporate directory.

- Necessary precautions are taken for the physical security of the information systems hardware, software and data of the Agency.

- Hardware-oriented (access control system enabling only the authorized personnel to enter the system room, 7/24 employee monitoring system, ensuring the physical security of the side switches forming the local area network, fire extinguishing system, air-conditioning system, etc.) and software-oriented (firewalls, intrusion prevention systems, network access control, systems preventing malware, etc.) precautions are taken in order to ensure the security of the information systems against environmental threats.

- Risks are identified as aimed to prevent the illegal processing of personal data, it is ensured that measures compatible with such risks are taken and technical controls are made as aimed for the taken measures.

- Access procedures have been established within the company

- Accesses to the storage areas where the personal data are kept are recorded and illegitimate accesses or access attempts are kept under control.

- The Company takes the necessary precautions in order for the deleted personal data

not to be accessible and reusable by the related users.

- Security gaps are monitored and compatible security patches are installed and the information systems are kept up-to-date.

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

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

- Data backup systems ensuring the secure retention of personal data are used.

- Access to data kept on electronic or non-electronic media is restricted according to the access principles.

- If transfer is carried out between servers in different physical environments, data transfer is carried out by establishing a VPN between servers or using the sFTP method.

- If paper media transfer is required, necessary precautions are taken against risks such as theft, loss or viewing of documents by unauthorized persons.

5.2 Administrative Measures

The following administrative measures are taken by the Company regarding the processed personal data.

- Trainings on the prevention of illegal processing of personal data, the prevention of illegal access to personal data, the protection of personal data, the PDP law and other relevant legislation are planned and carried out to improve the quality of employees.

- Confidentiality agreements are signed by the employees regarding the operation of the company.

- The Company Code of Ethics contains provisions regarding compliance with Security policies and procedures.

- The obligation to enlighten the related persons is fulfilled by the Company before starting to process personal data.

- A personal data processing inventory has been prepared.

- Periodical and random audits are held in the Agency.

- Data security trainings are given as aimed for the employees.

- A Data Breach Response Plan has been prepared.

2. DESTRUCTION METHODS

The following operations are performed regarding the data that needs to be destroyed.

6.1. Deleting Personal Data

Media in which Data is Saved	Description
Personal Data on Servers	For personal data kept on servers, the necessary retention periods of which have expired, the access authorization of related users is annulled by the system administrator and such personal
Personal Data in Electronic Media	Personal data kept on electronic media, the necessary retention periods of which have expired, are made absolutely inaccessible and non-reusable by any employees (related users) except for the database administrator.
Personal Data in Physical Media	Personal Data in the physical media The personal data kept in the physical media, whose time period has expired, is rendered inaccessible and non-reusable for other employees, with the exception of the Audit Manager, with the approval of the CFO. Furthermore, these can be obscured by scratching/painting over/erasing so that they
Personal Data in Portable Media	Personal data kept on flash based storage media, the necessary retention periods of which have expired, are encrypted by the system administrator and are retained in secure media with encryption keys that solely the system administrator is authorized to access.

6.2 Destruction

Media in which Data is Saved	Description
Personal Data in Physical Media	Personal data on paper media, the necessary retention periods of which have expired, are destroyed in paper shredders in a non-recoverable
Personal Data on Optic / Magnetic Media	Personal data on optic media and magnetic media, the necessary retention periods of which have expired, are physically destroyed by melting, burning or pulverizing. Furthermore, magnetic media are exposed to a high magnetic field by passing through a special device so that the data on the device are unreadable.

6.3. Anonymization

Anonymization of personal data means putting personal data into such a form that it can no longer be associated with a real entity whose identity is known or can be determined under any circumstances, even when it is linked with other data.

Data that are thought to be needed for statistical purposes are rendered irreversible by any person or method, in this way, unable to identify a specific person.

3. RETENTION AND DESTRUCTION PERIODS

The retention periods for the personal data processed by the company within the scope of its activities are shown on the basis of data category in VERBIS. In addition, the data inventory includes retention periods on the basis of each data category.

4. PERIODIC DESTRUCTION TIMES

In accordance with Article 11 of the regulation, the period of periodic destruction in the company is determined as 6 months. The destruction of the data whose storage period has expired is done in March and September.

5. EFFECT AND VALIDITY

This Policy enters into force on 01.10.2020. It is reviewed once a year or in case of changes in the Personal Data Protection Law No. 6698 and related legislation and updated if necessary.

APPENDIX: 1

-Identity **Personal Data**	Year **15 Years**
2-Contact **Personal Data**	Year **15 Years**
3- Location **Personal Data**	Year **1 Year**
4-Personnel **Personal Data**	10 years after the end of the employment relationship
5-Legal Transaction **Personal Data**	Year **10 Years**
7-Physical Space Security **Personal Data**	Other 15 days
8- Transaction Security **Personal Data**	Other 42 days
10-Finance **Personal Data**	The data of other partnerships is kept indefinitely.
11- Occupational Experience **Personal Data**	10 years after the end of the employment relationship
13- Visual and Audio Records **Personal Data**	Other 15 days
21- Health Information **Sensitive Personal Data**	Other 10 years after the end of the employment relationship
23-Criminal Conviction and Security Measures **Sensitive Personal Data**	Other 10 years after the end of the employment relationship
24-Biometric Data**Sensitive Personal Data**	Other **Within 1 day after** the end of the business relationship