DOLPHİN GAYRİMENKUL YATIRIM VE GELİŞTİRME LİMİTED ŞİRKETİ

PERSONAL DATA RETENTION AND ERASURE POLICY

April 1, 2020

TABLE OF CONTENTS

1. THE PURPOSE OF THE PERSONAL DATA RETENTION AND ERASURE POLICY

This Personal Data Retention and Erasure Policy ("**Policy**") herein is prepared by the data controller Dolphin Gayrimenkul Yatırım ve Geliştirme Limited Şirketi ("**Company**"), with the purpose of fulfilling our obligations arising from the Personal Data Protection Law No.6698 ("**Law**") and the Regulation on Deletion, Destruction and Anonymization of Personal Data ("**Regulation**"), which is the secondary regulation of the Law, determining the maximum retention period required for the purpose of processing the personal data and to inform about the deletion, destruction and anonymization processes.

2. DEFINITIONS

Abbreviation	Definition
Explicit Consent	Freely given, specific and informed explicit consent
Receiver Group	The category of natural or legal persons of which the personal data is transferred by the data controller
Employee	Natural persons working in the Company
Inventory	The inventory of processing the personal data, which details the personal data processing activities performed by the data controller depending on the business processes by explaining; the purpose of processing the personal data and its legal reason, data category, data transfer receiver group and the minimum retention period required by the purposes of processing the personal data, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.
Data Subject	The natural person which its data is being processed.
Erasure	Deletion, destruction or anonymization of personal data
Law/PDPL	Personal Data Protection Law dated 24.03.2016 and numbered 6698
Filing Environment	Every environment which the personal data is processed by wholly or partly automatic means or otherwise than by automatic means which forms part of a filing system.
Personal Data	All information regarding an identified or identifiable natural person
Processing of Personal Data	Any action performed on the data; such as obtaining, collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making it obtainable, categorizing or preventing its use by wholly or partly automatic means or provided that the process is a part of any data registry system, through non-automatic means.
Personal Data Retention and Erasure Policy	The policy which the data controller make it as a foundation for determining the maximum retention period required for the purpose of processing the personal data and the deletion, destruction and anonymization processes.
Deletion of Personal Data	Making the personal data inaccessible, irrecoverable and non-re-usable for the related users.
Destruction of Personal Data	Making the personal data inaccessible, irrecoverable and non-re-usable for everyone.
Board	The Board of Protection of Personal Data
Sensitive Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life,

	convictions and security measures, and the biometric and genetic data are deemed as sensitive personal data
Periodical Erasure	The repetitive ex officio deletion, destruction or anonymization process which is mentioned in the Policy, in the case of removal of all the conditions for the processing of personal data provided in the Law
Policy	This Personal Data Retention and Erasure Policy dated April 1, 2020
Registry	The data controllers' registry which is kept by the Directorate of The Authority of Protection of Personal Data
Company	Dolphin Gayrimenkul Yatırım ve Geliştirme Limited Şirketi
Data Filing System	A filing system which personal data are processed by structuring according to specific criteria
Data Controller	Natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system.
Regulation	The Regulation on Deletion, Destruction and Anonymization of Personal Data published in the Official Gazette on 28.10.2017

(The definitions in the Law and Regulation are applied to those not included in the Policy.)

3. INFORMATION ON RETENTION AND ERASURE

3.1. Information on Retention:

Personal data are retained by the Company with the below mentioned purposes and in accordance with the purposes specified in the Law and other legal regulations, for the periods stipulated in the legislation and legal reasons specified in the Articles 5 and 6[1] of the Law:

- Implementation Of Emergency Management Processes,
- Implementation Of Information Security Processes,
- Implementation Of Employee Satisfaction And Commitment Processes

[1] **Conditions for Processing of Personal Data**

ARTICLE 5 – (1) Personal data shall not be processed without obtaining the explicit consent of the data subject.

(2) Personal data may be processed without obtaining the explicit consent of the data subject if one of the below conditions exists:

a) It is expressly permitted by any law; b) It is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent; c) It is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract; ç) It is necessary for compliance with a legal obligation which the controller is subject to; d) The relevant information is revealed to the public by the data subject herself/himself; e) It is necessary for the institution, usage, or protection of a right; f) It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Conditions for Processing of Special Categories of Personal Data

ARTICLE 6 – (1) Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are special categories of personal data.

(2) It is prohibited to process special categories of personal data without obtaining the explicit consent of the data subject.

(3) Personal data indicated in paragraph 1, other than personal data relating to health and sexual life, may be processed without obtaining the explicit consent of the data subject if processing is permitted by any law. Personal data relating to health and sexual life may only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations.

- Fulfilling The Obligations Arising From The Legislation And Labor Contract For The Employees
- Implementation Of Side Benefit And Interest Processes For The Employees
- Conducting The Audit / Ethic Activities
- Conducting The Educational Activities
- Execution Of Access Authorization
- Execution Of The Activities In Accordance With The Law
- Conducting The Finance And Accounting Businesses
- Providing Physical Place Security
- Implementation Of Assignment Processes
- Execution And Follow-Up Of Legal Affairs
- Carrying Out Homeland Control / Investigation / Intelligence Activities
- Carrying Out Communication Activities
- Planning The Human Resources Processes
- Auditing And Execution Of Work Activities
- Carrying Out Occupational Health And Safety Activities
- Carrying Out Activities To Provide Business Continuity
- Execution Of Product / Service Purchasing Processes
- Execution Of Product / Service After-Sales Support Service Processes
- Execution Of Product / Service Sales Process
- Execution Of Product / Service Manufacturing And Operation Processes
- Execution Of Management Of Customer Relations Processes
- Organization And Event Management
- Conducting Performance Evaluation Processes
- Conducting Advertisement / Campaign / Promotion Processes,
- Execution Of Agreement Processes
- Execution Of Wages Policy
- Execution Of Marketing Processes Of Products / Services
- Work And Residence Permit Processes Of Foreign Employees
- Informing Authorized Person, Institution And Establishments
- Carrying Out Management Activities
- Create And Follow-Up Visitor Records

3.2.Information on Erasure:

The personal data processed and retained by the Company with the purposes above mentioned will be erased, destructed or anonymized ex officio or upon the request of the Data Subject, in the case of the following:

- Amendment or abrogation of the relevant legislation provisions that constitute the basis for processing and storage,
- Removal of the purpose of processing or retaining the personal data,
- Revocation of the explicit consent given by the Data Subject, in the cases where the processing of personal data takes place only under explicit consent conditions.

- Company's acceptance of the application made by the Data Subject in accordance with its rights arising from Article 11[2] of the Law, regarding the deletion and destruction of the personal data.
- In the cases where the Company does not accept, Data Subject finds the reply insufficient or the Company does not reply within the period of time foreseen in the Law to the application made by the Data Subject regarding the deletion and destruction of the personal data; a complaint to the Board and the approval of this request,
- The maximum period of the personal data to be retained necessarily has passed and non-existence of any condition to justify retaining personal data for longer.

4. FILING ENVIRONMENTS

Personal data are preserved by the Company and by taking all necessary administrative and technical measures, in the environments below mentioned:

Electronic Environments	Non-Electronic Environments
• Servers (Impact area, backing up, e-mail, database, web, document sharing, cloud information systems etc.) • Software (office software, portal) • Information security devices (firewall, intrusion detection and prevention, daily filing document, antivirus etc.) • Personal computers (desktop, laptop) • Mobile devices (telephone, tablet etc.)	• Paper • Written, printed, visual media

5. PERSONAL DATA ERASURE TECHNIQUES

At the end of the retention period required by the purpose of processing or set forth in the relevant legislation, personal data will be erased in accordance with the relevant legislation by the Company itself or upon request of the Data Subject with the erasure techniques stated below.

5.1. Deletion of Personal Data

[2] **Rights of Data Subject**
ARTICLE 11 – (1) Everyone, in connection with herself/himself, has the right to;
a) Learn whether or not her/his personal data have been processed;
b) Request information as to processing if her/his data have been processed;
c) Learn the purpose of processing of the personal data and whether data are used in accordance with their purpose;
ç) Know the third parties in the country or abroad to whom personal data have been transferred;
d) Request rectification in case personal data are processed incompletely or inaccurately;
e) Request erasure or destruction of personal data within the framework of the conditions set forth under Article 7;
f) Request notification of the operations made as per indents (d) and (e) to third parties to whom personal data have been transferred;
g) Object to any negative result occurred with respect to data subject by means of analysis of personal data exclusively through automated systems;
ğ) Request compensation for the damages in case the person incurs damages due to unlawful processing of personal data by applying to the data controller.

Personal data is deleted by the Company, with the below mentioned techniques according to the filing environment they are being retained.

Data Filing Environment	Description
Personal Data Contained on Servers	Deletion is performed by the system manager for the personal data contained on servers whose retention period has expired.
Personal Data Contained in Electronic Environment	Personal data contained in electronic environment whose retention time has expired cannot be accessed or reused by the employees other than the employees with access authorization.
Personal Data Contained in Physical Environment	Personal data contained in physical environment whose retention time has expired cannot be accessed or reused by the employees other than the employees with access authorization.
Databases	Relevant lines containing personal data will be deleted by the database controller with database commands (DELETE etc.).

5.2. Destruction of Personal Data

Personal data is destroyed by the Company, with the below mentioned techniques provided that the required technical and administrative measures are taken:

Data Filing Environment	Description
Environmental Systems	Personal data contained in environmental systems are depending on the type: • **Network devices (switch, router etc.):** Products often have a delete command but do not have the destruction command. Therefore, they are destroyed with one or more of the erasure techniques stated in 5.1. • **Flash Based Environments:** ATA SATA, PATA etc.), SCSI (SCSI Express etc.) flash based hard disks are destroyed with <block erase> command if supported, if not supported they are destroyed with the destruction method suggested by the producer or with one or more of the erasure techniques stated in 5.1.
Personal Data Contained in Physical Environment	Personal data on paper whose retention time has expired will be destroyed with destruction or shredding machines irreversibly.
Personal Data Contained in Optical/Magnetic Media	Personal data contained in optical/magnetic media whose retention time has expired will be

	destroyed physically by melting, burning or trituration.
Local Systems	Personal data contained in local systems are destroyed by demagnetizing, physical destruction, overwriting techniques.

5.3.Anonymization of Personal Data

In order for personal data to be anonymized, personal data should not be relatable to any identified or identifiable natural person even if the suitable techniques for the field of activity and filing environment are used such as personal data is reversed by the data controller or third parties and/or matching data with any other data.

Within this scope, personal data is anonymized by the Company, with one or more of the personal data anonymization techniques determined in the following table, having regard to the criteria such as the category, size, variety, distribution/centricity ratio of the personal data provided that the anonymized data set cannot be disclosed by combining with another data set, one or more values cannot constitute a meaningful whole in a way that can make a singular record, values on the data set cannot be able to combine to create hypothesis or results:

Personal Data Anonymization Techniques	
Anonymization Techniques that Does Not Cause Value Irregularity	• Excluding Variables • Extracting Records • Upper and Lower Limit Coding • Regional Hiding • Exemplification
Anonymization Techniques that Cause Value Irregularity	• Micro-Combining • Data Exchange • Adding Display • Resampling
Statistic Techniques that Empower Anonymizing	• K-Anonymity • L-Variety • T-Proximity

At the same time the Company, after anonymizing the personal data, controls the utilization of the transferred personal data contained within other institutions and organizations or public data and whether such data has become identifying for a person with contracts and risk analysis.

6. DURATION OF RETENTION AND ERASURE

Retention and erasure periods based on personal data related to all the personal data in scope of the activities performed depending on the process are found on the Envantory prepared by the Company, retention and erasure periods based on the activities are found on this Policy.

You may find the details of retention periods on the table below:

ACTIVITY	RETENTION PERIOD	ERASURE PERIOD
Creating Employee Personnel File	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Maintenance and Repair Activities	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Transactions Related to Information Technologies	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Work Permit Transactions	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Checking Account Transactions	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Security Activities (License Plate – Employee/Representative of Lessee and Natural Person/Private Company Lessee)	3 Months Following the Termination of the Employment or Lease Relationship	During the first periodic erasure following the end of the retention period
Execution of Security Activities (Providing Physical Place Security - Guest)	10 Years Following The Collection of the Relevant Information	During the first periodic erasure following the end of the retention period
Execution of Security Activities (Building Entry – Exit Records Information – Employee and Employee/Representative of Supplier)	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Security Activities (Building Entry – Exit Records Information – Employee/Representative of Legal Entity Lessee)	10 Years Following the Termination of the Lease Relationship	During the first periodic erasure following the end of the retention period
Execution of Security Activities (Camera Recordings)	30 Days Following the Capture of the Image	During the first periodic erasure following the end of the retention period
Execution of Security Activities (License Plate)	30 Days Following the Capture of the Image	During the first periodic erasure following the end of the retention period
Carrying Out Occupational Health And Safety Activities	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Carrying Out Lease and Linked Agreement Processes	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period

Managing the Wage Payment Process	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Advertising and Marketing Processes	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Purchasing Processes	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution and Follow Up of Company General Assembly/Board of Managers' Resolutions and Other Legal Transactions	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period
Execution of Cleaning Activities	10 Years Following the Termination of the Employment Relationship	During the first periodic erasure following the end of the retention period

7. DURATION OF PERIODICAL ERASURE

Company has determined the periodic destruction time as 6 (six) months. Accordingly, periodic destruction will be performed every year in June and December.

8. TECHNICAL AND ADMINISTRATIVE MEASURES

In the light of sufficient precautions determined and announced by the Board in accordance with Article 12 and 6/IV of the Law for sensitive personal data, the Company takes technical and administrative measures in order to retain the personal data safely, to prevent the personal data to be processed and accessed against the law and to erase the personal data in accordance with the law.

8.1.Technical Measures

The Company takes the following technical measures to ensure the safety of personal data:

a. Network security and application security is provided.
b. Necessary measures are taken within the scope of information technologies supply, development and treatment.
c. Procedures are applied for access authorization and role distributions.
d. Authorization matrix is determined.
e. In case of change of position or cease of employment, authorizations of employees in this field are removed.
f. Safety of the physical areas containing personal data is provided against the outside risks (fire, flood, etc.).
g. Personal data is minimized to extend possible.
h. Personal data is backed up and safety of the backed up personal data is also provided
i. Appropriate security patches are installed by following security flaws.
j. Up-to-date anti-virus systems are used.
k. Firewalls are used.

l. Problems with respect to personal data security are reported quickly.
m. Information systems are kept up to date.
n. In electronic environments where personal data are processed, strong passwords and secure logging systems are being used.
o. Backup programs are used to ensure that personal data are stored securely, and access to personal data stored in electronic or non-electronic environments is restricted according to access principles.
p. Data loss prevention software is used.
q. Intrusion detection and prevention systems are used.

8.2. Administrative Measures

The Company takes the following administrative measures to ensure the safety of personal data:

a. The quality and technical knowledge/skills of the employees are being improved.
b. Illegal processing of personal data is prevented.
c. Illegal access to personal data is prevented.
d. Personal data is preserved.
e. Signed contracts include data safety terms.
f. In case of a detection of an illegal transaction, it is notified to the data subject and the board.
g. Personal data security policies and procedures have been determined.
h. Corporate policies on access, information security, usage, retention and destruction have been prepared and implemented.

9. RESPONSIBILITY AND DISTRIBUTION OF ROLES

All units and employees of the Company actively support the responsible units for applying the technical and administrative measures taken in scope of this Policy as required, expanding, tracking and continuously controlling the unit workers' awareness and education and for taking the required administrative and technical measures to provide data safety in environments where data is being processed in order to prevent personal data from being accessed unlawfully and to store the personal data in accordance with the law.

The distribution of titles, units and job descriptions of those who participate in personal data retention and erasure processes in the Company are as follows:

TITLE	UNIT	JOB DESCRIPTION
CEO		Responsible for taking administrative measures regarding the personal data safety and application of the Policy in accordance with the duties.
Administrative Director	**Management**	Responsible for education of employees regarding personal data and making them comply with the Policy.
Finance Director	**Finance and Accounting**	Responsible for taking administrative measures regarding

		the personal data safety and application of the Policy in accordance with the duties.
Information Security Management System Representative	**Information Technology**	Responsible for taking technical measures regarding the personal data safety, delivery of the technical solutions needed in the implementation of the Policy and application of the Policy in accordance with the duties.

10. OTHER MATTERS

In case of inconsistency between the Policy and the Law and other relevant legislations, the provisions of the Law and other relevant legislations shall prevail.

This Policy prepared by the Company came into force on the date of April 1, 2020. In case of amendments to the Policy, the effective date and the relevant articles of the Policy will be updated accordingly.