

KfW IPEX-BANK GMBH
PERSONAL DATA STORAGE AND DISPOSAL POLICY

1. PURPOSE

The purpose of this Personal Data Storage and Disposal Policy (the “**Policy**”) is to ensure that KfW IPEX-Bank GmbH (“**KfW IPEX-Bank**”) fulfils its obligations set forth under the Personal Data Protection Law No. 6698 (“**Turkish Law No. 6698**”) and to provide the general principles on determining the minimum time period necessary for personal data storage and further information on erasure, destruction and/or anonymization of personal data.

Relevant units carry out necessary works within the scope of this policy.

2. SCOPE

Personal data of KfW IPEX-Bank’s employees, potential employees, persons receiving products or services, potential persons receiving products or services, customers and other third persons fall under the scope of this Policy and that this Policy is applicable to all personal data recording medium controlled or managed by KfW IPEX-Bank and operations concerning processing of personal data.

3. LIABILITY AND AUTHORITY

All KfW IPEX-Bank units and employees provide continuous assistance to relevant units to ensure that technical and administrative measures are followed properly, training and awareness of the unit employees are improved, observed and constantly inspected and unlawful means of processing of personal data are prevented and data security concerning all data processing mediums are provided to all relevant units within the scope of the Policy.

Titles, relevant units and job description of persons involved in the process of storage and disposal of personal data are shown in Table 1 below.

DEPARTMENT	TITLE	TASK
Management Board of KfW IPEX-Bank	Board of Management	Person(s) responsible for employees to follow and act according to the policy.
Management Board of KfW IPEX-Bank	Board of Management	Person(s) responsible from preparing, improving, updating and managing the Policy, as well as publishing it on relevant platforms.
Organisation and IT	Organisation and IT	Person(s) responsible from providing the necessary

		technical solutions concerning the implementation of the Policy.
All units except the ones listed above.	Other Units	Person(s) responsible from the management of the Policy in accordance with his/her duties.

4. DEFINITIONS

- 4.1. Explicit Consent:** means any freely given, specific, informed and unambiguous consent,
- 4.2. Data Subject:** means real person whose data is processed,
- 4.3. Personal Data:** means all information relating to an identified or identifiable natural person,
- 4.4. Disposal:** means erasure, destruction or anonymization of personal data,
- 4.5. Law:** Turkish Law No. 6698,
- 4.6. The Board:** means the Personal Data Protection Board,
- 4.7. Data Processor:** means the person who processes personal data only on behalf of the data controller,
- 4.8. Data Controller:** means the natural or legal person who determines the purpose and means of processing personal data and is responsible for the establishment and management of the data filing system,
- 4.9. Special Categories of Personal Data:** means personal data which, if obtained by others, can leave the data subject open to discrimination or unfair treatment. Hence, special categories of personal data require much more protection.
- 4.10. Periodical Disposal:** means erasure, destruction or anonymization of personal data determined in this Policy and to be performed periodically *ipso iure* upon the complete termination of conditions for the personal data processing available in the Law,
- 4.11. Anonymization:** means the process of rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.

5. APPLICATION

5.1. PERSONAL DATA RETENTION PERIOD

In relation to the personal data processed by KfW IPEX-Bank within the scope of its operations;

- Retention period based on all personal data processed within the scope of operations performed is specified in the Data Processing Inventory;
- Retention period based on data categories is entered upon VERBIS registration;
- Retention period based on the process is specified in this Policy.

DATA CATEGORY	DATA RETENTION PERIOD
ID Information	Is stored for 10 years after termination of the labor contract.
Contact Information	Is stored for 10 years after termination of the labor contract.
Location Information	Is stored for 10 years after termination of the labor contract.
Personnel Information	Is stored for 10 years after termination of the labor contract.
Financial Information	Is stored for 10 years after termination of the labor contract.
Professional Experience Information	Is stored for 10 years after termination of the labor contract.
Visual and Auditory Records	Is stored for 10 years after termination of the labor contract.
Society Membership	Is stored for 10 years after termination of the labor contract.
Foundation Membership	Is stored for 10 years after termination of the labor contract.

Time periods set forth under the legislation are regarded to be the maximum retention periods unless a longer time period is regulated within the Law or limitation period, period of prescription, retention period etc. are regulated with longer time periods.

Unless the Board decides otherwise, **KfW IPEX-Bank in its own capacity selects the method of erasure, destruction or anonymization of personal data.** However, upon the Data Subject's request, purposes behind selecting the proper method will be explained.

All operations relating to erasure, destruction and anonymization of personal data are recorded and those records are stored for **minimum three years** excluding other legal obligations.

Personal data is erased, destructed or anonymized by KfW IPEX-Bank , in its own capacity or upon the request of the Data Subject, in the event that all of the conditions for processing laid down in Article 5 and Article 6 of the Law no longer exist. In this context, upon the request of the Data Subject KfW IPEX-Bank shall:

- Conclude all request within 30 (thirty) days and inform the relevant data subject.
- In the event that the personal data which are subject to the request have been transferred to any third party; the third party is notified of such request and the performance of necessary operations by the third party is ensured.

As per article 11 of the Regulation on Erasure, Destruction or Anonymization of Personal Data, KfW IPEX-Bank 's time interval for periodic disposal is determined to be six months and KfW IPEX-Bank shall complete these periodic disposal proceedings during the months of June and December of every year.

Data listed with retention periods above is disposed of within the first period of disposal period following the end of retention period.

5.2. PERSONAL DATA RECORDING MEDIUM

All personal data stored within our company is stored in a recording medium that is in compliance with the nature of the data and our legal responsibilities. General characteristics of recording mediums used for personal data storage are as follows:

1. Non-electronic Mediums	Written, printed and visual mediums where data is stored is printed on paper or microfilm.
2. Electronic Mediums	Digital mediums such as servers, hard disk or portable hard drives and memory sticks (memory sticks, memory cards etc.), optic disks (CD, DVD etc.), servers (range, back up, e-mail, database, web, file sharing etc.), software (office software, portal), information security devices (firewall,

	intrusion detection systems and intrusion prevention, daily export registry file, antivirus etc.), personal computers (desktop, laptop), mobile devices (phones, tablets etc.), removable memory sticks, printer, copying machine within the company.
3. Cloud	Mediums where encrypted web-based systems are used by the Company. These mediums aren't contained within the Company.

5.3. REASONS REQUIRING STORAGE AND DISPOSAL

5.3.1. Reasons Requiring Data Storage and Purposes of Data Processing

KfW IPEX-Bank stores personal data of data subjects in accordance with the Law and other relevant legislation especially regarding:

- maintaining all commercial activities; performance of business, transactions and contracts, contacting real and/or legal entities that liaise with KfW IPEX-Bank,
- personal data to be used for establishing, exercising or protecting a right,
- performance of necessitated or required legal liabilities, completing legal reports,
- carrying out human resources proceedings and corporate communication,
- procuring KfW IPEX-Bank's - security,
- being able to satisfy the burden of proof concerning legal disputes which may arise in the future,
- Conducting activities in accordance with the legislation,
- planning and performance of employees' rights and side benefits,
- managing customer services in secured physical or electronic mediums and to provide secured data storage for data which requires data subject's consent for storage.

5.3.2. Reasons Requiring Disposal

As per the Regulation on Erasure, Destruction or Anonymization of Personal Data, personal data of data subjects is erased, destroyed or anonymized by KfW IPEX-Bank in its own capacity or upon the request of data subjects, when:

- relevant legislation provisions of which is the basis of personal data processing or storage are amended or annulled,
- conditions for the processing or storage of personal data no longer exist,
- conditions for processing set forth in article 5 and article 6 of the Law no longer exist,
- data subject's personal data is processed only upon explicit consent and that the data subject retrieves the given explicit consent,
- the data subject's request for personal data erasure, destruction or anonymization within the scope of article 11(e) and (f) is accepted by the data controller,
- in the event that a claim is made to KfW IPEX-Bank and that KfW IPEX-Bank approved such claim following data subject's request for erasure, destruction or anonymization of personal data is denied or found to be inadequate or not responded within the time period set forth under the law by the data controller,
- despite the maximum time period for storage has passed, there is not any condition that requires personal data to be stored for a longer period.

5.4. METHOD AND PROCEDURE OF PERSONAL DATA DISPOSAL

All disposal methods which KfW IPEX-Bank may exercise are identified in this Policy. Data owner unit is required to exercise the appropriate method in accordance with this Policy.

KfW IPEX-Bank shall in its own capacity erase, destruct or anonymize all personal data stored in accordance with the Law and Policy on Processing and Protection of Personal Data, upon the data subject's request as soon as conditions for processing personal data no longer exist or time periods stated in the Personal Data Storage and Disposal Policy are expired.

Most exercised methods of erasure, disposal and anonymization in which KfW IPEX-Bank uses are listed below; KfW IPEX-Bank is required determine whichever method is applicable case by case:

5.4.1. Methods of Erasure

Methods of Erasure for Personal Data Stored in Non-Electronic Mediums		
Blanking	:	Personal data stored in non-electronic medium is erased by blanking. Process of blanking is performed by deleting personal data on relevant paper where possible, and in cases

		where this is not possible, it can be rendered invisible to the relevant user by using fixed ink so that it cannot be reversed and read by technological solutions.
Methods of Erasure for Personal Data Stored in the Cloud and Electronic Mediums		
Secured erasure from the software	:	Personal data stored in the cloud or electronic medium is permanently erased on a digital medium. In addition, electronic back up is periodically erased when a backup system is used for data security.

5.4.2. Methods of Destruction

Methods of Destruction for Personal Data Stored in Non-Electronic Mediums		
Physical destruction	:	Documents stored in a printed medium are irreversibly destroyed with a paper shredder.
Methods of Destruction for Personal Data Stored in Electronic Mediums		
Physical destruction	:	Hard disks and devices alike which contain personal data are physically destructed with punch method.
Demagnetization (degauss)	:	The data over magnetic fields are rendered unreadable by exposing them to another higher magnetic field.
Overwrite	:	0 and 1's are written at least seven times randomly over magnetic media and rewritable optical media and the old data is rendered impossible to be readable and save.
Methods of Destruction for Personal Data Stored in the Cloud		
Secured erasure from the software	:	Personal data stored in the cloud is permanently erased on a digital medium and when the service agreement for cloud usage is expired, all copies of encryption keys which may be used to retrieve personal data are

		destroyed. Data erased with such method cannot be retrieved.
--	--	--

5.4.3. Methods of Anonymization

Extraction of variables	:	Extraction of one or some of the direct identifiers of the data subject's the personal data of which may help to identify the data subject. This method can be exercised for erasure of information that is not in compliance with the purpose of processing personal data as well as anonymization of personal data.
Regional concealment	:	Method of erasing distinctive information of explicit data contained in the data table where all personal data is stored anonymously.
Generalisation	:	Method of composing people's personal data and rendering that data actuarial by removing distinctive information.
Lower and Upper Limit Coding/ Global Coding	:	Concerning certain variable, intervals of that variable are categorised. If the variable does not contain a numerical value, then all data that is in close approximation within the variable will be categorised together. Variables in the same category then will be combined.
Micro integration	:	All records contained in the data set are aligned in a significant order and then the data set is subsetting in specific numbers. Later the average of the specified variable's value in each subset is switched with the average of the variable of that subset. Thus, associating the data subject with the relevant data will be obstructed since the indirect identifiers within the data are falsified.
Data combining and corrupting	:	This is done by mixing direct or indirect identifiers within personal data with other

		variables or by disassociating its connection with the data subject by obstruction and making sure that it loses its qualifications.
--	--	--

6. TECHNICAL AND ADMINISTRATIVE MEASURES

KfW IPEX-Bank shall take all technical and administrative measures for secured storage of personal data and preventing unlawful data processing and data access, as well as destruction of personal data in accordance with article 12 and article 6 (4) of the Law concerning sensitive personal data.

ADMINISTRATIVE MEASURES	TECHNICAL MEASURES
<ul style="list-style-type: none"> - Preparing Personal data Processing Inventory, - Corporate Policies (Access, Information Security, Usage, Storage and Destruction etc.) - Contracts (between the Data Controller and Data Controller and Data Controller and Data Processor) - Confidentiality Declarations, - Periodic and/or Random Inspections within the Company - Risk Analysis - Employment Contract, Disciplinary Code and Procedure (Scheduling Lawful Amendments) - Corporate Communication (crisis management, Information Procedure for the Board and Data Subject, Reputation Management etc.) - Training and awareness operations (Information Security and the Law) - Notifying the data Controllers Registry (VERBIS) 	<ul style="list-style-type: none"> –Authorisation Matrix –Authorisation Control –Access Logs –User Account Management –Network Security –Application Security –Encryption –Penetration Test –Intrusion Detection and Prevention Systems –Log history –Data Masking –Data Loss Prevention Softwares –Backup –Firewall –Up to date Antivirus systems –Erasure, Destruction or Anonymization –Key Management

7. UPDATING AND COMPLIANCE

KfW IPEX-Bank reserves the right to amend its Policy on Protection and Processing of Personal Data or Personal Data Storage and Disposal Policy as per amendments in laws and regulations, Board decisions or developments within the market or IT field.

All amendments made to this Policy shall be incorporated into this policy's text and explanations with regards to amendments shall be stated at the end of the Policy.