

ÇELEBİ HAVA SERVİSİ ANONİM ŞİRKETİ

PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. Purpose of the Destruction Policy

This Personal Data Storage and Destruction Policy (**'Policy'**) has been prepared by **Çelebi Hava Servisi Anonim Şirketi ('Company')**, as the data controller, in order to determine the procedures and principles to be applied by the Company regarding the deletion, destruction or anonymisation of the personal data we hold within the scope of the services we offer through Çelebi Platinum and our activities related to them, either ex officio by the Company or upon the request of the data subject in accordance with the Personal Data Protection Law No. 6698 (**'PDPL'**) and the relevant legislation.

Personal data belonging to our employees, employee candidates, customers, visitors, managers, dealers, employees of the companies we cooperate with, receive services/products from and/or provide services/products to, and other third parties and held by our Company are within the scope of this Policy. The provisions of this Policy shall apply to all recording media where personal data of the aforementioned persons are processed and to activities for personal data processing.

2. Media where Personal Data are Stored

Personal data stored by the Company are kept in a recording medium suitable for the nature of the relevant data and our legal obligations.

The recording media used for the storage of personal data are generally listed below. However, some data may be kept in a different medium than the media shown here due to their special characteristics or our legal obligations. The Company acts as a data controller in all cases and processes and protects personal data in accordance with the PDPL, the Personal Data Processing, Protection and Privacy Policy (you can access the relevant policy at _____) and this Personal Data Storage and Destruction Policy.

Electronic Media	Non-Electronic Media
Servers (Database, e-mail, web, backup, file sharing etc.)	Paper
Software (Microsoft Office programme)	Unit cabinets
Company-owned mobile devices (mobile phones, tablets)	Folders
Personal Computers (desktop, laptop)	Archive room
Optical discs (CD, DVD)	
Removable memories (USB, Memory Card)	
Camera recording area	
Printer, scanner, photocopy machine	

3. Ensuring the Safety of Media

The Company takes the necessary technical and administrative measures in accordance with the characteristics of the relevant personal data and the medium in which it is kept in order to store personal data securely and to prevent unlawful processing and access. In this context, the Company personnel are informed and regularly trained within the scope of current legislation.

These measures include the following administrative and technical measures to the extent appropriate to the nature of the relevant personal data and the medium in which it is kept.

3.1 Technical Measures

The Company takes the following technical measures regarding the personal data it processes:

- Only up-to-date and secure systems in accordance with technological developments are used in the media where personal data are kept.
- Security systems are used for the media where personal data are kept.
- Security tests are carried out to identify security vulnerabilities on information systems, and existing or potential risks identified as a result of the tests are eliminated.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- Access to the media where personal data are kept is restricted and only authorised persons are allowed to access these data limited to the purpose of storing personal data and all accesses are recorded.
- The authorisations of the personnel whose duties are changed or dismissed are removed.
- In order to ensure the security of the media where personal data are kept within the Company, sufficient technical personnel are employed and/or technical services are provided by contracted companies.

3.2 Administrative Measures

The Company takes the following administrative measures regarding the personal data it processes:

- Activities are carried out periodically to raise awareness of all Company employees who have access to personal data on data security and confidentiality of personal data.
- Legal and technical consultancy services are received in order to follow the developments in the field of data security and take necessary actions.

- Personal data security policies and procedures have been determined.
- The signed contracts contain data security provisions.
- Personal data security issues are reported.
- In case personal data is transferred to third parties due to technical or legal requirements, a protocol is signed with the relevant third parties for the protection of personal data and/or a commitment is obtained from the relevant third parties to comply with confidentiality obligations.

3.3 Internal Audit

Pursuant to Article 12 of the PDPL, the Company conducts internal audits regarding the implementation of the provisions of the PDPL and the provisions of this Policy and the Personal Data Processing, Protection and Privacy Policy.

In the event that deficiencies or defects regarding the implementation of these provisions are detected as a result of internal audits, these deficiencies or defects shall be corrected immediately.

In case it is understood that personal data under the responsibility of the Company is obtained by others illegally during the audit or in any other way, the Company shall notify the relevant person and the Personal Data Protection Board (**‘Board’**) as soon as possible.

4. Reasons for Storage and Destruction

Personal data kept within the Company are stored for the purposes and reasons specified herein in accordance with the PDPL and our Personal Data Processing, Protection and Privacy Policy.

Personal data held within the Company **shall be deleted, destroyed or anonymised** in accordance with this Policy upon the request of the relevant person or in the event that the reasons listed in Articles 5 and 6 of the PDPL disappear .

The reasons listed in Article 5 of the PDPL titled ‘Conditions for Processing Personal Data’ consist of the following:

- It is clearly stipulated in the laws.
- It is mandatory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid.

- It is necessary to process personal data belonging to the parties to a contract, provided that it is directly related to the conclusion or performance of a contract.
- It is mandatory for the data controller to fulfil its legal obligation.
- It has been made public by the data subject himself/herself.
- Data processing is mandatory for the establishment, exercise or protection of a right.
- Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

The reasons listed in Article 6 of the PDPL titled ‘Conditions for Processing Special Categories of Personal Data’ are as follows:

- Explicit consent of the data subject.
- It is clearly stipulated in the laws.
- It is mandatory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid, himself/herself or someone else.
- It is related to the personal data made public by the data subject and is in accordance with the will of the data subject to make it public.
- It is mandatory for the establishment, exercise or protection of a right.
- It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of health services by persons under the obligation to keep secrets or authorised institutions and organisations.
- It is mandatory for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance.
- It is intended for current or former members and members of foundations, associations and other non-profit organisations or formations established for political, philosophical, religious or trade union purposes, or for persons who are in regular contact with these organisations and formations, provided that it complies with the legislation to which they are subject and their purposes, is limited to their fields of activity and is not disclosed to third parties.

5. Destruction Methods

The Company deletes, destroys or anonymises personal data that it stores in accordance with the PDPL and other legislation and the Policy on Processing, Protection and Privacy of Personal Data, upon the request of the data subject or ex officio within the periods specified in this Policy, if the reasons requiring the

processing of the data disappear.

The most commonly used deletion, destruction and anonymisation techniques used by the Company are listed below:

5.1. Deletion Methods

Deletion Methods for Personal Data Stored in Printed Media

Obfuscation Personal data in printed media are erased using the obfuscation method. The obfuscation process is performed by cutting out the personal data on the relevant document, where possible, and making it invisible by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.

Deletion Methods for Personal Data Stored in Cloud and Local Digital Media

Secure deletion from software: Personal data stored in the cloud or on local digital media is deleted by digital command in such a way that it cannot be recovered. Data deleted in this way cannot be accessed again.

5.2. Destruction Methods

Destruction Methods for Personal Data Stored in Printed Media

Physical destruction: Documents kept in printed media are destroyed by document shredders in such a way that they cannot be reassembled.

Destruction Methods for Personal Data Stored in Local Digital Media

Physical destruction: The process of physically destroying optical and magnetic media containing personal data, such as melting, physically damaging (drilling, breaking), burning or pulverising. Data is rendered inaccessible by processes such as melting, burning, unusable physical damage (drilling, breaking), pulverising or passing the optical or magnetic media through a metal grinder.

De-magnetisation (degaussing): It is the process of distorting the data on the magnetic media in an unreadable way by exposing it to a high magnetic field.

Overwriting: Random data consisting of 0s and 1s are written at least seven times on magnetic media and rewritable optical media, preventing the reading and recovery of old data.

Destruction Methods for Personal Data Stored in Cloud Environment

Secure deletion from software: Personal data stored in the cloud is deleted by digital command in such a way that it cannot be recovered and all copies of the encryption keys necessary to make the personal data usable are destroyed when the cloud computing service relationship ends. Data deleted in this way cannot be accessed again.

5.3. Anonymisation Methods

Anonymisation is the process of making personal data impossible to associate with an identified or identifiable real person under any circumstances, even by matching them with other data.

Removing variables: It is the removal of one or more of the direct identifiers contained in the personal data of the data subject that can be used to identify the data subject in any way. This method can be used to anonymise personal data, or it can be used to delete personal data if it contains information that is inappropriate for the purpose of data processing.

Regional hiding: It is the process of deleting the information that may be distinctive for the data that is exceptional in the data table where personal data are collectively anonymised.

Generalisation: It is the process of bringing together personal data belonging to many people and turning them into statistical data by removing their distinctive information.

Lower and upper limit coding/Global coding: For a certain variable, ranges for that variable are defined and categorised. If the variable does not contain a numerical value, then data close to each other within the variable are categorised. Values within the same category are combined.

Micro-merging: With this method, all records in the dataset are first arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Then, the value of each subset for the specified variable is averaged and the value of that variable of the subset is replaced with the average value. In this way, the indirect identifiers in the data will be distorted, making it difficult to associate the data with the relevant person.

Data hashing and corruption: Direct or indirect identifiers in personal data are mixed or distorted with other values, so that their relationship with the person concerned is severed and they lose their identifying characteristics.

In order to anonymise personal data, the Company uses one or more of these anonymisation methods depending on the nature of the relevant data. The Company may use K-Anonymity, L-Diversity and T-Closeness statistical methods when using these anonymisation methods.

6. Storage Periods

Data Subject	Data Category	Storage Period
Employee	Employee identity information, personal	10 years from the end of the employment contract.

	information, contact information, legal contact information, salary information, occupational experience information and trainings received, employee performance and compliance information, criminal conviction and security, business suit measurements, fringe benefits information, financial information, location data, vehicle / licence plate information, location information.	
Employee	Data obtained through hardware and software access processes.	2 years from the end of the employment contract.
Business Partner/Solution Partner/Consultant Website Visitor	Identity information, contact information, financial information, data belonging to their employees regarding the execution of the business relationship / commercial relationship between the Business Partner / Solution Partner (Dealer / Franchise / Supplier) / Consultant and the Company.	10 years as per Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code during and after the termination of the business relationship/commercial relationship between the Business Partner/Solution Partner/ (Dealer/Franchise/Supplier) /Consultant and the Company.
Website Visitor	Name, surname, e-mail address, cookies and log records of the website visitor.	6 months, maximum 2 years. Information on online visitors is kept for 2 years.
Visitor	Traffic information processed during the use of the company's internet network, access to the internet and remote connection; IP address, start and end time of the service provided, type of service utilised, amount of data transferred and subscriber identification information, if any, etc. data.	2 years.
Visitor	Voice recordings taken during call centre calls.	2 years.

Employee Candidate	Information contained in the CV and job application form of the employee candidate.	When the recruitment for the position in question is over, the relevant CVs and resumes are destroyed. If permission is obtained from the candidates to keep their CVs and resumes for the evaluation of future positions, the relevant data is kept for 1 year.
Intern	Information contained in the internship file of the intern.	10 years from the beginning of the calendar year following the end of the internship relationship.
Customer	Customer's name, surname, contact information, product/service preferences, transaction history, special days information.	10 years from the delivery of each product/service purchased by the Customer in accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.
Customer	Camera footage of the customer, vehicle licence plate information.	1 month.
Potential Customer	Identity information, contact information, financial information obtained during contract negotiations regarding the establishment of a commercial relationship between the potential customer and the Company.	2 years.
Consumer	Data obtained by the Company through distance sales contracts concluded with consumers.	3 years.
Company/Personal Company	Legal Transaction.	10 years following the termination of the legal transaction.
Customer/Supplier/ Franchise	Preparation of contracts.	10 years following the expiry of the contract.

* In the event that a longer period is regulated in accordance with the legislation or a longer period is stipulated for statute of limitations, forfeiture period, storage periods, etc. in accordance with the legislation, the periods in the provisions of the legislation are accepted as the maximum storage period.

7. Destruction Periods

The Company deletes, destroys or anonymises personal data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymise the personal data for which it is responsible in accordance with the PDPL, relevant legislation, Personal Data Processing, Protection and Privacy Policy and this Policy arises.

When the relevant person requests the deletion or destruction of his/her personal data by applying to the Company pursuant to Article 13 of the PDPL;

- If all of the conditions for processing personal data have disappeared; The Company deletes, destroys or anonymises the personal data subject to the request within 30 (thirty) days from the day it receives the request, by explaining its reason, with the appropriate destruction method. In order for the Company to be deemed to have received the request, the person concerned must have made the request in accordance with **the Personal Data Processing, Protection and Privacy Policy**. In any case, the Company informs the relevant person about the transaction.
- If all the conditions for processing personal data have not disappeared, this request may be rejected by the Company by explaining the reason in accordance with the third paragraph of Article 13 of the PDPL, and the rejection response shall be notified to the data subject in writing or electronically within thirty days at the latest.

8. Periodic Destruction

In the event that all of the conditions for the processing of personal data in the PDPL disappear; the Company deletes, destroys or anonymises the personal data whose processing conditions have disappeared through a process specified in this Personal Data Storage and Destruction Policy and to be carried out ex officio at recurring intervals.

9. Supervision of the Lawfulness of Destruction

The Company carries out ex officio destruction operations both upon request and in periodic destruction processes in accordance with the PDPL, other legislation, the Personal Data Processing and Privacy Policy and this Policy. The Company takes a number of administrative and technical measures to ensure that the destruction processes are carried out in accordance with these regulations.

10. Technical Measures

- The Company shall have technical tools and equipment suitable for each destruction method specified in this Policy.

- The Company ensures the security of the place where destruction operations are carried out.
- The Company keeps access records of the persons performing the destruction process.
- The Company employs competent and experienced staff to carry out the destruction process or receives services from competent third parties when necessary.

11. Administrative Measures

- The Company carries out activities to increase the awareness of its employees who will carry out the destruction process on information security and confidentiality of personal data.
- The Company receives legal and technical consultancy services in order to follow the developments in the field of information security, personal data protection and secure destruction techniques and to take necessary actions.
- In cases where the Company has third parties carry out the destruction process due to technical or legal requirements, the Company signs protocols with the relevant third parties for the protection of personal data and takes all necessary care to ensure that the relevant third parties comply with their obligations in these protocols.
- The Company regularly audits whether the destruction operations are carried out in accordance with the law and the conditions and obligations specified in this Policy, and takes the necessary actions.
- The Company records all transactions regarding the deletion, destruction and anonymisation of personal data and keeps such records for at least three years, excluding other legal obligations.

12. Personal Data and Compliance

Each unit and department that processes personal data, especially the Human Resources Department / Unit, is personally responsible for the implementation of this Policy. Legal advisors are in the position of guides and counsellors in the follow-up and interpretation of the relevant laws and legal follow-up of the PDPL processes.

13. Update and Compliance

The Company reserves the right to make changes in the Personal Data Processing, Protection and Privacy Policy or this Policy due to the amendments made in the PDPL, in accordance with the Board decisions or in line with the developments in the sector or in the field of informatics.

Amendments to this Policy are immediately incorporated into the text and explanations regarding the amendments are stated at the end of the Policy.

Last Update Date:.../...../2024

