SİNCER LOJİSTİK EMLAK BUJİTERİ DIŞ TİCARET LTD. ŞTİ.
COOKIE POLICY PERSONAL DATA STORAGE AND DISPOSAL POLICY

Purpose

Personal Data Storage & Disposal Policy ("Policy") is prepared with the purpose of determining the procedures and principles regarding jobs and operations of the storage and destruction activities of Sincer Lojistik Emlak Bujiteri Dış Ticaret Ltd. Şti. ("Sincer")

In Sincer processing personal data of employees and potential employees, supplier officials, visitors and other third persons in accordance with Turkish Constitution, International Contracts, Personal Data Protection Law (KVKK) no.6698 and other related legislation, and enabling related persons to use their rights effectively is of utmost importance.

Where do we save the personal data?

Personal data are stored in the following mediums in accordance with the law.

Electronic Platforms	**Non Electronic Mediums**
Servers (domain, back-up, e-mail, database, web, file sharing etc.) • Softwares (office softwares, portals, EBYS, VERBİS.) • Information Security Devices (firewall), attack detection and prevention, daily log file, antivirus etc.) • Personal Computers (Desktop, laptop) • Mobile Devices (Phone, tablet etc.) • Optical disks (CD, DVD, etc.) • Removable Memories (USB, Memory Card etc.) • Printer, Scanner, Photocopy Machine	• Paper • Manual data logging systems (survey forms, visitor entrance log) • written, printed, visual mediums

Descriptions Regarding Storage

Your personal data is stored for the du

Processing Purposes That Requires Storing

Sincer stores the personal data it processes within its regular activities for the following purposes.

- Managing human resources processes
- Managing communication processes
- Providing protection
- Executing works and operations upon signed contracts and protocols.
- In scope of VERBIS; determining the preferences and needs of employees, data controllers, contact persons, data controller agents and data processors; arranging the services accordingly and updating them if necessary.
- Ensuring legal obligations are fulfilled as required by legal regulations.
- Fulfilling legal obligations
- Obligation to demonstrate as evidence in future legal disputes.

Reasons Requiring Disposal

- Purpose that requires the processing or storage of personal data, loses validity.
- When related person revoke their open consent if the processing of personal data only takes place with open consent condition
- Sincer accepting the persons application made within their rights, regarding the disposal and destruction of their personal data in accordance with Article 11 of the law.
- A person filing a complaint and Board approving this complaint.
- The time requiring the storage of personal data being passed and no other condition remains that justifies storing of the personal data.

Upon these situations, the data will be disposed, erased, or anonymized upon the request of related person.

TECHNICAL AND ADMINISTRATIVE MEASURES

Sincer takes technical and administrative measures; to store personal date safely, and to dispose of the date in accordance with the law to prevent illegal access & process of the data; according to regulations.

Technical Measures

The technical measures taken by Sincer regarding the personal data it processes are as follows:

•Leakage (Penetration) tests Sincer's information systems, surfacing risks, threats, weaknesses and vulnerabilities if any and necessary precautions are taken.

•As a result of real-time analysis with information security incident management, risks and threats that will affect the continuity of information systems are constantly monitored. •Access to Information Systems and authorization of users is done through security policies through the access and authorization Matrix and through the corporate Active Directory.

• Necessary precautions are taken for the physical security of information systems equipment, software and data.

•Hardware-wise (access control system that provides access of authorized personnel only, 24/7 monitoring system, providing physical security of edge keys that forms the local network, fire extinguishing system, air conditioning system), and software-wise (firewalls, attack prevention systems, network access control, systems that prevent malware etc.) precautions are taken

•Risks of preventing illegal processing of personal data, taking technical measures fit for these and risks and technical controls regarding these measures are done.

•Access procedures are formed with Sincer to report the access to personal data and analysis studies are conducted

•Access to storage units containing personal data are logged and inappropriate accesses or access trials are controlled. Sincer takes precautions to ensure that the the deleted personal data is inaccessibale and unusable.

•An appropriate system and infrastructure is formed by Sincer to notify the use and the Board if the personal data is accessed illegaly by others.

•Security breaches are followed and appropriate security patches are loaded and information systems are kept up-to-date. Strong passwords are used in electronic mediums in which personal data is processed.

•Safe logging systems are used in electronic mediums in which personal data is processed.

•Data backup programs are used that ensures personal data is stored safely.

•Access to stored personal data, whether stored electronical or non-electronical mediums, is limitied in accordance with access principles. Access to Sincer webpage is encrypted with SHA 256 Bit RSA algorithm by using safe protocol (HTTPS).

•A different policy is determined for the security of sensitive personal data.

• The necessary trainings are given about sensitive personal data security to personnel working in sensitive personal data storing processes, nondisclosure agreements are signed, users with access are authorized.

•The electronic mediums in which sensitive personal data is processed, stored and/or accessed are kept safe with cryptographic methods, cryptographic keys are kept in safe mediums, all processes are logged, security updates of mediums are followed, necessary security tests are done regularly and test results are logged.

•The physical mediums in which sensitive personal data is processed, stored and/or accessed are secured as required, and physical security is ensured by preventing unauthorized access.

•If sensitive personal data are to be transferred via e-mail, it should be sent via corporate mail address or KEP account, encrypted. If it is to be transferred via mediums like memory stick, CD, DVD it should be cryptographically encrypted and cryptographical keys should be kept

apart. If the transfer is in between servers that are in different physical locations, a VPN should be set up between servers or sFTP method should be used for data transfer. If the transfer must be through paper, necessary precautions should be taken against risks like stealing, losing and the document being seen by unauthorized people and the documents should be sent "confidentially".

Administrative Measures

The administrative measures taken by Sincer regarding the personal data it processes are as follows:

- To improve the qualifications of the workers trainings on prevention of unlawful processing of personal data, prevention of unlawful access of personal data, provision of protection of personal data, communication techniques, technical skills and related legislation.
- Nondisclosure Agreements are signed by employees regarding the activities of Sincer.
- Disciplinary Procedure is prepared for the employees not conforming with security policies and procedures.
- Clarification obligation must be fulfilled by Sincer before processing personal data.
- Personal data processing inventory was prepared.
- Periodical and random internal audits are made.
- Information security trainings are given to employees.

METHODS OF DISPOSAL OF PERSONAL DATA

After the storing period of the personal data that is provided in related regulations or required by the purpose of processing; the personal data are deleted by Sincer after related persons application by themselves or ex officio, in accordance with the regulations, with the following methods.

Disposal of Personal Data

Your personal data are deleted with the following methods:

Logged Medium of Data	**Description**
Personal Data in Servers	The personal data in servers of which that doesn't need to be stored anymore, the access authorization of related are removed and deletion is done.
Personal Data in Electronic Medium	The personal data in electronic mediums of which that doesn't need to be stored anymore are made inaccessible and unusable to other employees (related users) except for the database manager.

Personal Data in Physical Medium	The personal data in physical mediums of which that doesn't need to be stored anymore are made inaccessible and unusable to other employees except for the manager responsible for document archives. Moreover, black-out is applied by drawing/painting/erasing making it unreadable
Personal Data in Portable Medium	The personal data in portable mediums of which that doesn't need to be stored anymore are encrypted by system manager and kept safe with the encryption key only giving access to system manager.

Destruction of Personal Data

Your personal data are destroyed with the following methods.

Logged Medium of Data	**Description**
Personal Data in Physical Medium	The personal data in paper mediums of which that doesn't need to be stored anymore are destroyed irreversibly with paper shredders.
Personal Data in Optical/Magnetic Medium	The personal data in optical and magnetic mediums of which that doesn't need to be stored anymore are destroyed physically with methods like melting, burning or pulverizing. Moreover, data in magnetic medium are made unreadable with a special device that applies high magnetic field on the medium.

Anonymization of Personal Data

Anonymization personal data is to make personal data unrelated to an identified or identifiable person by any means, even if it is matched with other data. To anonymize personal data, it must be rendered unrelated to an identified or identifiable person, and keeping it unrelated even by using appropriate techniques for the recording environment and related field of activity.

STORAGE & DISPOSAL PERIODS

Storage & disposal periods are as follows.

Personal Data	**Storage Period**	**Distruction Period**
Identity Data	10 years	In the first periodical disposal after its storage period ends
Communication Data	10 years	In the first periodical disposal after its storage period ends
Location Data	5 years	In the first periodical disposal after its storage period ends
Personal Data	10 years	In the first periodical disposal after its storage period ends
Legal Transaction Data	10 years	In the first periodical disposal after its storage period ends
Customer Transaction Data	10 years	In the first periodical disposal after its storage period ends
Physical Place Secuirty Data	6 months	In the first periodical disposal after its storage period ends
Transaction Security Data	5 years	In the first periodical disposal after its storage period ends
Professional Experience Data	10 years	In the first periodical disposal after its storage period ends
Audio-visual records.	6 months	In the first periodical disposal after its storage period ends
Health Data	10 years	In the first periodical disposal after its storage period ends
Data on Criminal Convictions and Security Measures	10 years	In the first periodical disposal after its storage period ends

Periodic Disposal Period

Sincer determined the periodic disposal period as 6 months according to Article 11 of the regulation.

Updating The Policy

The policy will be reviewed and parts necessary will be updated.