DACHSER TURKEY LOJİSTİK HİZMETLERİ A.Ş.

SENSITIVE PERSONAL DATA PROTECTION POLICY

1. THE SCOPE

In Article 6 of the Personal Data Protection Law No. 6698 ("Law"), a number of personal data that carry a risk of victimization or discrimination of the persons when being processed illegally is designated as "Sensitive Personal Data". These data are deemed to be sensitive data;

- Race, ethnic origin,
- Political opinion, philosophical belief,
- Religion, sect or other belief,
- Clothing,
- Membership of associations, foundations or unions,
- Health and sexual life,
- Convictions and security measures,
- Biometric and genetic data.

The scope of this Policy constitutes the activities for the protection and processing of the sensitive personal data regarding the privacy and confidentiality of sensitive personal data belonging to the Dachser Turkey Lojistik Hizmetleri A.Ş.'s employees, employee candidates, service providers, customers, visitors and other third parties. In this context, only several provisions of this Policy mentioned above might be applied to the groups of personal data owners as well as all the provisions of this Policy.

2.THE DEFINITIONS

Definitions of terms used in the Policy are given below:

Explicit Consent	A consent for his personal data upon information on any particular matter and his own free will.
Recipient Group	The category of natural or legal persons to whom personal data is transferred by the Data Controller.
Anonymisation	Rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data.
Presidency	Presidency of Protection of Personal Data
Employee	Dachser Turkey Lojistik Hizmetleri A.Ş.'s personnel.
Electronic Environment	An environment where personal data can be created, read, changed and written with electronic devices.
Non-Electronic Environment	All written, printed, visual, etc. media that are excluded from electronic media.
Service Provider	A natural or legal person providing services under a fixed-term contract with the Dachser Turkey Lojistik Hizmetleri A.Ş..

Data Subject	A natural person whose sensitive personal data is processed.
Destruction	The process of rendering personal data inaccessible and unusable for any person.
Board	Personal Data Protection Board
Law	Personal Data Protection Law
Committee on the Protection of Personal Data	A committee established to carry out administrative monitoring of processes within the scope of the Personal Data Protection Law and sub-regulation by Dachser Turkey Lojistik Hizmetleri A.Ş.
Sensitive Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive data.
Periodic Destruction	If all of the terms of the processing of personal data contained in the Law are eliminated, the deletion, destruction and anonymity will be performed at repeated intervals as set out in the Policy of retention and destruction of personal data.
Policy	Dachser Turkey Lojistik Hizmetleri A.Ş. Sensitive Personal Data Protection Policy.

Definitions in the Law are valid for definitions that are not included in this Policy.

3.THE PROCESS OF SENSITIVE PERSONAL DATA

Dachser demonstrates sensitivity about the processing of sensitive personal data which is considered to be more critical importance for the Data Subject from various aspects. Sensitive Personal Data is processed by Dachser in accordance with the Law, provided that adequate measures are taken to be determined by the Board and the conditions below:

- If the data subject has given his explicit consent,
- If the data subject has not given his explicit consent; Sensitive Personal Data excluding those relating to health and sexual life can be processed as stipulated in the Law; sensitive personal data related to the health and sexual life can be processed with the aim of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing by persons under the confidentiality obligation or authorized institutions and organizations.

4. THE MEASURES FOR PROCESSING SENSITIVE PERSONAL DATA

Dachser, In Article 6 of the Law, the processing of Sensitive Personal Data, pursuant to the Decision numbered 2018/10 and dated 31.01.2019 issued by the Board, takes the following measures below as the Data Controller:

a- For the protection of the Sensitive Personal Data, systematic, clearly-defined, manageable and sustainable Policy has been determined.

b- For employees involved in the processing of Sensitive Personal Data;

- Trainings are provided regularly for the subjects of Sensitive Personal Data Protection in accordance with the regulations and the Law.
- Confidentiality agreements are formed.
- The scope and the duration of the authorization of the users who have access to the data are clearly defined.
- Authority checks are carried out periodically.
- Employees who have been reassigned or who have resigned are immediately withdrawn of the authorisations in this area.

c- Media, where Sensitive Personal Data is processed, maintained and/or accessed, is an electronic media,

- Personal data are maintained by using special methods.
- Transaction records of all activities performed on personal data are logged securely.
- Security updates for personal data environments are constantly monitored, necessary security tests are regularly performed and test results are recorded.
- If personal data is accessed through software, authorized users relating to this software, security tests of this software are performed regularly and test results are recorded.
- If the remote access to personal data is required, this access is provided with at least two-stage identity validation system.

d- The environment where Sensitive Personal Data is processed, maintained and/or accessed is a physical environment;

- Adequate security measures (against electricity leakage, fire, flood, theft, etc.) are taken depending on the nature of the environment in where Sensitive Personal Data is.
- Unauthorized entry and exits are prevented by ensuring the physical security of these environments.

e- If Sensitive Personal Data will be transferred;

- If personal data needs to be transferred via e-mail, it is transmitted by encoded institutive e-mail address or using an Electronic Mail (KEP) account.
- Data is encrypted if it needs to be transferred via media such as portable memory, CD and DVD.
- If it is necessary to transfer personal data through paper media, necessary measures are taken against risks such as theft, loss or access of the document by unauthorized persons and the document is sent in a “confidential” format.

f- In addition to the measures mentioned above, technical and administrative measures to ensure the appropriate level of security stated in the Personal Data Security Guide published on the website of the Personal Data Protection Authority should also be taken into account.

5.THE TRANSFER OF SENSITIVE PERSONAL DATA

Dachser can transfer the Sensitive Personal Data of the Data Subject which were obtained lawfully to third parties in the direction of the purposes of data processing by taking the necessary security measures. Accordingly, Dachser will be able to transfer Sensitive Personal Data to third parties one of the processing conditions stated in the section above and the following conditions below must be met:

- If the Data Subject has given his explicit consent,
- If it is explicitly provided for by the laws,
- It is mandatory for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical disability,
- Processing of personal data belonging to the parties of a contract is necessary provided that it is directly related to the conclusion or fulfilment of that contract,
- If it is mandatory for Dachser to fulfil its legal obligations,
- If the Sensitive Personal Data is made manifestly public by the Data Subject,
- If the transfer of Sensitive Personal Data is mandatory for the establishment, exercise or protection of any right,
- If it is mandatory for the legitimate interests of the controller, provided that such processing shall not violate the fundamental rights and freedoms of the data subjects.

6. THE INTERNATIONAL TRANSFER OF SENSITIVE PERSONAL DATA

Dachser can transfer Sensitive Personal Data of the Data Subject to foreign countries that Data Controller has adequate protection or is committed to providing adequate protection in the following cases by taking the necessary and adequate security measures envisaged by the Board for legitimate and lawful personal data processing purposes.

- If the Data Subject has given his explicit consent,
- If the Data Subject has not given his explicit consent;

a- Sensitive data excluding those relating to health and sexual life (race, ethnicity, political opinion, philosophical belief, religion, sect, or other belief, clothing, associations, foundations, or trade unions membership, criminal convictions and security measures, biometric and genetic data) is explicitly provided for by the Laws,

b- Personal data relating to health and sexual life, by persons under an obligation of confidentiality or by authorised institutions and establishments for protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Dachser Turkey Lojistik Hizmetleri A.Ş.