Machine Translated by Google

DATA TRANSFER

SECURITY PROCEDURES AND

ABOUT ITS PRINCIPLES REGULATIONS

KVKK_Y8 VERSION 1.00

Machine Translated by Google

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

DATA TRANSFER SECURITY PROCEDURES AND PRINCIPLES REGULATIONS REGARDING

1. PURPOSE AND SCOPE

Our company stores a large amount of data, both electronically and in paper form, in the conduct of its economic activities. This Regulation on Data Transfer Security Procedures and Principles (hereinafter referred to as the "Regulation") aims to regulate the procedures applicable to the protection of stored data and to ensure the secure transfer of personal data within and outside the Company.

This Regulation shall apply to all of the following groups of individuals within our Company who process personal data and sensitive personal data and are required to transfer this data to Company stakeholders as part of their duties:

• Employees •
Suppliers and contractors with whom our company collaborates • Interns

Our employees should consider this Regulation together with the Regulation on the Procedures and Principles Regarding the Use of Information and Communication Technologies and the Information Security Policy. They should buy it.

2. RELEVANT LEGISLATION

Law No. 6698 on the Protection of Personal Data and related administrative regulations.

3. SPECIAL CATEGORY DATA

For the purposes of this Regulation, special categories of data include the following data categories:

• Data relating to a person's race, ethnic origin, political views, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

• Confidential data that our company considers trade secrets. • Confidential
data in contracts relating to goods, services, and products.
All defined data.

• Confidential data relating to our company's customers and suppliers.

Any employee who has any doubts about whether any data being processed constitutes special category data must report this to their relevant Department Head and act according to their instructions.

Machine Translated by Google

4. CONSIDERATIONS DURING DATA TRANSFERS ESSENTIAL POINTS

4.1. When transferring personal data and sensitive personal data, each employee must consult with the relevant Department Head for authorization of the data transfer and provide instructions.

4.2. Special categories of personal data and other personal data should only be transferred to the extent absolutely necessary for the proper conduct of our Company's legal activities. Accordingly, before each data transfer, it should be determined in advance whether the data transfer is necessary.

4.3. When communicating with third parties, it should be considered whether data sharing agreements and additional protocols regarding the protection of personal data have been signed with the relevant parties. Furthermore, it should be checked whether there is a provision regarding the proposed data transfer methods, and if so, care should be taken to use the proposed methods.

4.4. It should always be checked whether information beyond what is necessary for the stated purpose is being provided. For example, if only a section or specific part of a document is requested, the entire document or chart should not be sent.

4.5. In all cases where personal data and information containing special categories of personal data are transferred, the identity of the recipient and their access authorization to the data must be clearly defined.

5. DATA TRANSFER METHODS

Before determining data transfer methods, the following points should be considered:

• The nature of the information to be transmitted, its sensitivity, confidentiality level, or potential value

• The size of the data to be

transferred • The losses that may occur to the individuals concerned as a result of data transfer potential losses or difficulties that may remain

• The consequences of data loss for our Company. • Information

and documents beyond what is necessary for the stated purpose should not be transferred. All unnecessary data should be redacted or, if necessary, completely removed before transfer.

5.1. Data Transfers via Electronic Mail

• Email communication should not be used for the transfer of unencrypted, sensitive data that may contain personal information. Our employees need to be aware that email is not designed for attaching and transferring large amounts of data.

• Our employees should prefer to use alternative secure methods for the transmission of sensitive data whenever possible and feasible. Where a suitable alternative is not available, additional levels of security should be used.

Machine Translated by Google

For example, encryption should be used, or passwords and usernames should be required to access sensitive data that is to be sent. When transferring usernames and passwords, alternative methods such as mail, phone calls to designated numbers, or SMS messages should be used. • In email
messages, clear instructions should be provided regarding the legal responsibilities of the recipient who has received the data mistakenly, and what they should do with the incoming email, in cases where the recipient is not the correct person. • Where
applicable, the information sent should be enclosed in sealed attachments.
It should be sent.
• Care should be taken to ensure that the information included in the subject line or accompanying message of the email is accurate. The entire content of attachments or sensitive personal data should not be disclosed in the file name or subject line. • Emails should be
sent to the Company to display appropriate privacy and security information.
It must be transferred using the email address provided.

5.2. Internal Company Portal

• Users who need to copy or transfer data to a removable medium, or who have a very large amount of data to send, should seek assistance from the Company's IT Support Team.

• The portal should not be accessed using a file explorer without prior permission from the IT Support Team. • When
uploading data to the portal, ensure that file names are appropriately named and stored in the correct locations. Specialized data that needs to be uploaded to the portal should not be stored in publicly accessible locations.
• When uploading data to the company's network, care should be taken to use a secure portal by following appropriate procedures.
• Each piece of data to be transferred to online educational resources must be encrypted using a password-protected document or an encrypted zip file.

5.3. Removable Data Storage Devices (memory card, USB drive, etc.)

• All data transferred via removable media such as USB portable memory devices must be encrypted. Encrypted portable storage devices must be protected using strong passwords. If the password itself needs to be disclosed to a third party, this information should be transmitted using alternative methods such as mail, telephone, or SMS message.

• Users who need to copy or transfer data to removable media, or who have a very large amount of data to send, should seek assistance from the Company's IT Support Team.

• The ownership of removable media used must be clearly defined. Removable media must be returned to its owner after data transfer, and the transferred data must be deleted from the data storage device after use.
• In cases where the recipient is not the correct person and data has been mistakenly transferred, clear instructions should be provided regarding the recipient's legal responsibilities and what to do with the incoming email.

Machine Translated by Google

- Disclosure of information about the contents of the encrypted file in the file name and attached messages. It should not be done.
- The sender must confirm in a timely manner whether the data transfer was successful and issue a receipt for this purpose.
  Email messages confirming receipt of the file may be suitable for this purpose. • Any issues should be reported to immediate supervisors, and the Data Protection Officer/Liaison Officer should be informed immediately about any lost or corrupted data.

5.4. Telephone Calls

Because telephone conversations can be monitored, overheard, or interrupted (intentionally or accidentally), the following precautions should be taken:

- Personal data should not be transmitted or discussed over the phone unless you have verified the recipient's identity and authorization.
- When using an answering machine, do not leave sensitive or confidential messages or include any personal data. Simply provide a means of communication and expect the recipient to speak with you personally.
- While listening to voicemail messages left for you, others might be eavesdropping.
  Be careful not to turn on the audio recording in open areas where there is a risk of accidents.

5.5. Data Transfers via Post and Courier

- For data transfers on physical media such as memory cards or CDs, secure postal services should be used. Special delivery and registered mail services should be preferred over first or second class postal services. If using postal services other than PTT (Turkish Post), companies offering secure courier services that require a signature upon delivery should be chosen.

- The recipient must be clearly stated on the postal shipment form, and the physical packaging must be securely designed to prevent breakage or damage. • Recipients should be informed in advance of when they are expected to receive the data. The recipient must confirm receipt of the data securely as soon as it arrives. The sender responsible for data transmission is obligated to confirm that the data has been received securely.

5.6. Hand Delivery

Hand delivery and receipt of documents are among the approved transfer methods. If a person is scheduled to receive the data to be transferred, their identity must be determined in advance, and appropriate identity verification methods must be used at the time of delivery to confirm that the recipient is the intended person.

Machine Translated by Google

6. Missing Data

Whenever an employee discovers that any data has been lost, they must immediately inform their immediate supervisor and the Data Protection Officer/Liaison Officer, and the procedures specified in the Personal Data Breach Response Plan Regulation must be carried out without delay.

If there is suspicion that unauthorized users have gained access to sensitive personal data, law enforcement should be notified immediately.

7. Negligence in Data Transfer Procedures

Employees who fail to comply with the provisions of this Regulation may be deemed to have committed gross negligence in their duties and their employment contracts may be terminated. Personal data breaches may result in our Company losing contact and incurring heavy fines.

Therefore, our employees must exercise utmost care when transferring sensitive personal data.
It is essential. Actions that may be considered negligence and faulty behavior include: transferring data without authorization, not properly encrypting the data, not using compression and encryption protection, not using registered or insured postal services, etc.