DATA PROTECTION IMPACT EVALUATION PROCEDURE AND ABOUT ITS PRINCIPLES REGULATIONS

KVKK_Y3 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

DATA PROTECTION IMPACT ASSESSMENT (DPIA) REGULATIONS ON PROCEDURES AND PRINCIPLES

1. INTRODUCTION AND SCOPE

1.1. This Regulation on the Procedures and Principles of Data Protection Impact Assessment (DPIA) (hereinafter referred to as the Regulation) should be evaluated together with our Company's Information Security Policy, Personal Data Protection Policy, and Framework Policy.

1.2. This Regulation governs the procedures and principles to be followed when our Company, as the data controller, is required to conduct an assessment of the impact of planned processing activities on the protection of personal data before the processing activity (GDPR Article 35), or when Information Asset Owners conduct Data Protection Impact Assessments during their annual review processes for the information assets they control, particularly when new technologies are used in terms of information and communication technology methodology or general commercial use, and when a type of processing is likely to pose a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context, and purposes of the data processing activity.

1.3. Definitions: For the purposes of this regulation, Information Assets are assets owned by Kardelen Boya that are necessary for the uninterrupted conduct of its operations and which it is therefore obligated to protect.

1.4. Owner of the Information Asset: The manager of the business area where the relevant asset is used.

2. DATA PROTECTION IMPACT ASSESSMENT

2.1. Employees assigned as Information Asset Owners are responsible for managing the information assets under their control in accordance with the responsibilities described in the Framework Policy.

2.2. Information Asset Owners must conduct an impact assessment at least once a year, and especially when there are significant changes to the information asset, its storage and processing methods, or changes to legal regulations or policies that foresee changes to the personal data stored within the information assets, they must conduct an impact assessment before any changes are implemented.

2.3. Information Asset Owners must ensure that the security of the assets they control meets the following conditions stated in the Company's Information Security Policy:

- All users must properly ensure they have access to the information before doing so. They must be authorized.
- Reasonable consideration that is compatible with the value and/or sensitivity of the information asset. A certain level of security must be ensured.

- Users must report any incident resulting in, or likely to result in, a data security breach to the Data Protection Liaison Officer and IT Manager. Affected users must also inform the IT Support Team, their Department Heads, or Senior Company Executives about the breach without delay.

- Users are obligated to conduct a Data Protection Impact Assessment (DIA) on their assets as part of the annual review of their information asset inventory.

2.3.1. Each Owner of an Information Asset is obligated to use reasonable efforts to ensure that all materials held in its possession meet the following requirements at all times:

- The data collected must be lawful.

- Compliance with the Terms of Use for IT Resources, as outlined in Section 11 of the Company's Information Security Policy, is required.

- Data collected must not contain links leading to illegal material and must not contain content that is inconsistent with the Company's Terms of Use for Information and Communication Tools.

- Unless approved by the relevant Department Head, no promotion or commentary on any goods, products, or services on behalf of the Company may be published.

- Unless approved by the relevant Department Head, the Information Asset Owner or any other person's company, partnership, consortium, or consultancy, or any information and/or data containing promotional or commentary on their "private" activities, should not be included.

2.3.2. Information belonging to any individual that is included in the company's information assets and data:

- It must not contain the company's trademark, logo, letterhead, etc.

- The materials retained must be directly related to or relevant to the Information Asset Owner's authorization to use the Company's IT assets.

- Regardless of how they are referenced, the relevant company policies and regulations and the manner in which individually held information is presented shall not be construed in any way as implying that the Company assumes any responsibility for or endorses the individually held information itself or any material or opinions contained therein.

For all individually held information, a certified disclaimer must be displayed on the screen indicating that this information has not been officially released by the Company.

2.4. All personnel are responsible for following best information security practices to ensure that information held by the Company is properly protected, regardless of the format in which it is held. All Department Heads are responsible for overseeing information security practices within their departments as part of their management responsibilities. As part of this process, Department Heads will review assets held within their departments and are obligated to implement necessary measures and controls to ensure that the Company's Information Asset Inventory accurately reflects all managed assets.

2.5. The Information Assets Inventory assists relevant departments in determining which specific IT support is needed for particular information assets in terms of information and communication technology security and IT asset management, and in conducting information security controls. Although the information assets inventory is managed by the IT Manager, necessary precautions should be taken, considering the security of the records and assets kept in paper format.

2.6. Information assets should be identified using logical links and collection methods. For example, information collected for an HSE study might be stored on various media, including a series of laptops, a group of drives, and USB drives. In this case, an entry describing each medium and how it is kept secure should be recorded.

2.7. Each relevant department must declare the information assets it holds and ensure they are recorded in the inventory. Each additional storage system acquired locally for digital/record storage purposes should be recorded as a "System used by the Department" asset. If there is any doubt as to whether additional information assets should be recorded, the IT Support Team should be contacted. Cloud storage systems and paper-based filing systems should also be defined as information assets and recorded in the inventory.

2.8. When reviewing the information assets of their departments, Department Heads should consider the following:

- Are there any information assets that need to be added to the inventory?

- Any information assets that are not in use and need to be removed from the inventory
  Is that possible?
- Is there a change in the use of information assets that would require updating the records in the information asset inventory?

- Are there any policy changes or legal regulations that foresee a change in how information assets used by the department are collected and processed?

2.9. It is acknowledged that Department Heads will not have comprehensive knowledge of all the information that personnel in their departments work with or all the elements in which that information is stored. It is recommended that departments, when completing their information asset record, give broad consideration to the fundamental risks associated with the information held by the department and where that information is stored. Departments may find it beneficial to focus on data transfer, particularly where data is sensitive or transferred outside the College. Please contact the IT Security Team for further guidance.

3. STRUCTURE OF THE INFORMATION ASSET INVENTORY

Domain Name	Explanations
Information Asset Owner	Who is responsible for the information stored in this data asset, and who is the point of contact/liaison officer for inquiries regarding this data asset?
Information Asset Manager	The role of the Information Asset Manager is defined in the ISMS Framework Policy Document and can be described as the most authorized person who uses the information asset on a daily basis.
Name of the Information Asset	The specific name assigned to the Information Asset
Definition of Information Asset	Provide a brief description of the information asset. If possible, include a short information note about the information that will be held within the asset.
The current status of the asset is shown only in the Information Assets inventory - Temporary, Approved, or Inactive, etc.	
Classification	• Does the information asset contain special categories of data? What are the risks associated with this data? What measures are being taken to eliminate or mitigate these risks? Data that will be considered as special category data are as follows: o Data relating to company administration or research that is considered commercially sensitive data.

	data. This refers to "data relating to individuals' 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" as specified in Article 6 of Law No. 6698. that is, individual financial data; that is, data related to research studies Development commissioned by the company. Personal data not included above, but which, if disclosed, could cause harm or damage the reputation of the individuals concerned, should also be considered in this category.
Where the asset will be stored Environment Type	Electronic, manual, or both.
Legal Basis	What is the legal basis for processing and/or storing the relevant data? In accordance with Law No. 6698, legitimate data processing grounds that can be used by data controllers must be considered in order to process personal data lawfully.
From a Workflow Perspective Its Importance	The vital importance of the information asset to the company's workflow and the level of negative consequences that would arise if the asset were lost or its confidentiality were breached.
Location of the Information Asset	Where is the information asset physically stored? For example, on local computers, in the central system, at the portal, or at a location other than the server?
Adding the Information Asset Side	The person who entered the relevant record into the Information Assets Inventory Who is it?
Anticipated Storage Duration	For how long will the information asset be kept in the inventory? What is the foreseen process for determining that the information is no longer necessary for the Company's operations and for its secure destruction? Please review the Company's Data Retention and Destruction Policy regarding the timeframe after which data should be destroyed.
Oldest Entry	The date of the oldest record that should not be within the current date-retention period range.
Last Record Entry	The date of the last entry for information assets that are no longer updated.

Officials appointed as Information Asset Owners must also consider the following:

• Responsible Unit: Which unit is responsible for the information asset in question? (Usually the unit responsible for the "asset owner")
• Units and/or personnel who will have access to the information asset? Please specify the groups of individuals expected to have access to the relevant information asset. For example, employees assigned to a specific team or all company employees. Additionally, third parties who are not company employees but are expected to have access to the relevant information asset should also be clearly identified.

• How will the security of the information asset be ensured? Summarize the measures taken to ensure the security of the information asset. For example, password protection. Are records containing sensitive personal data kept in paper format stored in a locked filing system? How are the locks maintained? Warning: Do not under any circumstances disclose the location where the passwords or locks are stored!
• Backup, Resilience and Disaster Recovery arrangements: What measures
are taken to recover data and/or maintain the functionality and accessibility of data in case of data loss or breach of data/system(s) security, or in case of disasters, earthquakes, etc.?