# DATA BREACH INTERVENTION PLANNING REGULATION

KVKK_Y2 VERSION 1.00

## 1. PURPOSE AND SCOPE

1.1. Kardelen Paint and Chemical Industry Trade Limited Company (hereinafter referred to as "the Company") This Personal Data Breach Response Plan (hereinafter referred to as such) has been adopted by our Company as part of strategic planning actions to ensure that our Company is prepared to take immediate action against data security breaches, in accordance with the provision of the Announcement regarding the Decision No. 2019/10 of the Personal Data Protection Board dated 24.01.2019 on the Procedures and Principles for Notifying Personal Data Breaches, which states that "In the event of a data breach, the data controller shall prepare a data breach response plan that includes issues such as who to report to within their organization, who is responsible within their organization regarding the notifications to be made within the scope of the Law and the evaluation of the possible consequences of the data breach, and that this plan shall be reviewed at certain intervals." The focus of the response plan to be implemented in the event of any breach will be to take swift action to protect individuals and their personal data. Our Company primarily aims to carry out the following actions in the event of a data breach:

(a) To notify the Personal Data Protection Board (the Board) of a personal data breach without undue delay and within 72 hours at the latest after becoming aware of the data security breach (the Company has the discretion to decide whether or not to notify if the personal data breach is unlikely to pose a risk to natural rights and freedoms).

(b) To notify affected data subjects without unnecessary delay, unless the likelihood of a personal data breach resulting in a high risk to the rights and freedoms of natural persons is low.

1.2. This Regulation:

(a) This will be circulated to all relevant data processing parties. Those acting as data processors are obliged to immediately notify us as soon as they become aware of any breach of the security of personal data they process on behalf of our Company.

(b) The Intervention Plan provisions will be communicated to our employees upon their commencement of duty and will be discussed in periodic staff meetings and training sessions to ensure that personnel are informed about the plan.

1.3. Steps to be followed in the Flowchart, which forms part of this Regulation.

It has been summarized.

1.4. Definitions: The definitions applicable to the provisions of this Regulation are given below.

They are listed as follows:

1.4.1. Awareness of the Breach: A data controller shall be deemed "aware of the breach" when it has a reasonable degree of certainty that a security breach has occurred that compromises the security of personal data.

1.4.2. Damage: personal data that has been altered, corrupted, or is no longer complete.

1.4.3. Destruction: Data that is no longer available or that the data controller has lost in any way. not available in a form that he/she can use.

1.4.4. Loss: The data may still be available, but the controller has lost control over the data. They have lost control or access to the data, or no longer possess it.

1.4.5. Personal Data Breach is a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored, or processed;

1.4.6. "Temporary data loss": rendering personal data unusable for a period of time.
the event that caused it.

1.4.7. "Unauthorized or unlawful processing" means the disclosure (or access) of personal data to recipients who are not authorized to receive (or access) the data, or any other form of processing that violates the provisions of Law No. 6698.

1.5. A data security breach can occur for a variety of reasons, including the following:

• Human error

• Loss or theft of documents or devices containing personal data

• Unauthorized entry, theft, robbery

• Implementing inadequate access controls that allow unauthorized use/access

• Equipment failure and inadequate system backups

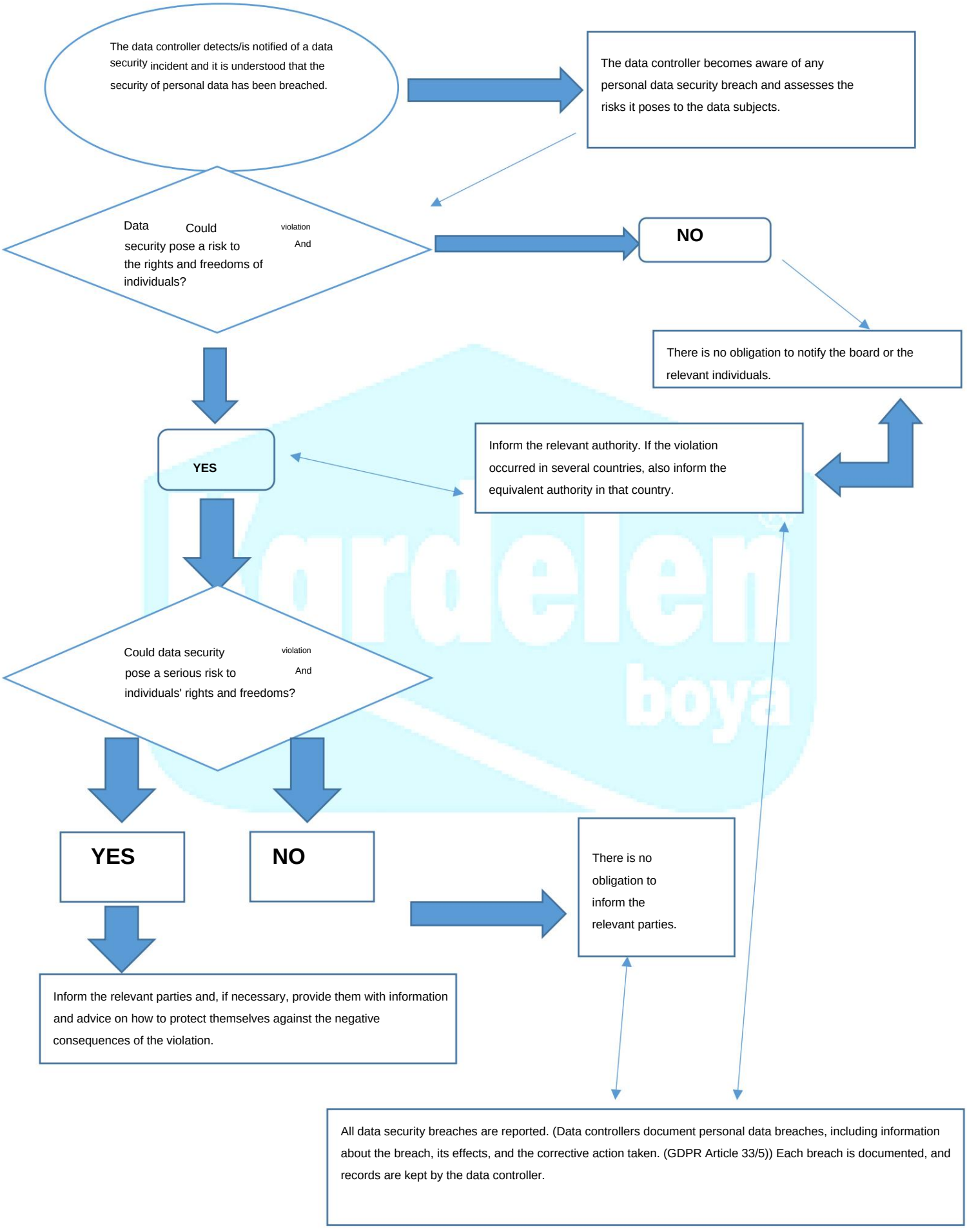
• Disaster situations such as floods or fires.

• Phishing (illegally obtaining someone's password or credit card details by sending messages), electronic fraud, or information theft, where personal information is obtained through deception or fraud.

• Malicious cyberattacks such as hacking, malware, denial-of-service (DoS-DDoS) attacks, or ransomware attacks.

1.6. Personal data breaches can have negative consequences for individuals, potentially causing physical, material, or moral harm. These situations may lead to embarrassment, distress, or humiliation for the data subject. Other negative consequences may include: loss of control over personal data, restriction of individual rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, and significant economic or social disadvantages for the affected individuals.

## A. Flowchart Regarding the Obligation to Report Violations



1.7. Personal data breaches can lead to the following situations, for example:
This could also harm our company:

• Damage to the trust relationship we have built with our staff and customers,

• Loss, deletion, or damage to personal data necessary for the management of our company seeing,

• Damage to our company's corporate reputation,

• Facing administrative sanctions under data protection legislation, or initiating lawsuits and investigations against us seeking material/moral damages.

## 2. INTERVENTION PLAN

In the event of a potential personal data security breach, the Company will act in accordance with the response plan described below:

2.1. Detecting a data security breach and informing the relevant officials of the situation.

2.1.1. The Data Protection Liaison Officer or Manager[1] shall be informed as soon as possible. will be done.

2.1.2. The Data Protection Liaison Officer or Manager shall immediately notify the General Manager. It will provide information.

2.1.3. The Data Protection Liaison Officer/Manager will assemble a small team, referred to as the Cyber Incident Response Team (CIRT), to assess potential damage, loss, unauthorized access, temporary data loss, and to take appropriate measures to contain the breach/ remediate the situation and restore the pre-breach state. All personnel and all data processors and/or joint data controllers are obligated to provide all necessary assistance to the Data Protection Liaison Officer/Manager and the personnel in the team they have formed.

2.1.4. The Data Protection Liaison Officer/Manager shall prepare a written chronology of events, recording all aspects of the breach, including the following:

(a) Date and time the violation was reported (using DD/MM/YYYY and 24-hour time format).

(b) If the notification relates to a potential breach, details of the preliminary investigation (if necessary) to be conducted to determine whether a breach has actually occurred.

(c) Details regarding who reported the matter.
(d) What is known / what is suspected in this initial stage.
(e) details regarding which system/dataset the data breach is associated with.
(f) Assessment of the risk to the rights and freedoms of natural persons.

---

1. The Data Protection Liaison Officer is the person appointed by our Company as our liaison officer to the Board and may be a senior manager assigned within the Company's administrative structure, a Data Protection Specialist employed by the Company for this purpose, or a lawyer we have contracted for this purpose.

(g) Actions that need to be taken urgently (investigation, containment of damage, remediation of the situation, data recovery, etc.).
(h) Details of the team assembled to help.
(i) Details of the tasks assigned to each team member.
(j) In the same way as (g), within 72 hours of becoming aware of the infringement, to the Board notification to be made.
(k) (if necessary) notification to the affected persons without undue delay.

2.1.5. Regardless of whether a decision has been made to notify the Board, information regarding each potential, reported, or suspected personal data breach, including its effects and the corrective action taken, shall be documented.

2.2. **Limiting the Security Breach, Mitigating its Effects, and Measures to Eliminate**

2.2.1. The company will take immediate steps to contain the breach and implement necessary measures to prevent unauthorized access to retained personal data and to limit any resulting damage.

2.2.2. In the event of a data security breach involving Information Technology (IT) systems and/or electronic data, the IT support personnel within the Company will be contacted immediately to seek their advice and technical support regarding appropriate measures to be taken, such as limiting the damage, quarantining affected data storage areas, and preserving data and log records.

2.2.3. Depending on the nature of the breach/threat to personal data, the measures to be taken may include the following steps:

(a) Quarantining some or all of the personal computers, networks, etc.

(b) Staff should be warned not to access computers, networks, devices, etc.

(c) Suspension of user accounts,

(d) Checking the records kept on the backup servers,

(e) Identifying which types of personal data may have been potentially disclosed and how the unauthorized access incident occurred.

2.2.4. If deemed necessary, quarantine of data recording areas maintained manually or in other ways may also be considered.

2.2.5. Where necessary, the IT crime investigation team may be utilized and legal advice may be sought.

**2.3. Risk Analysis**

2.3.1. In the event of a personal data breach, the company is obligated to conduct a comprehensive risk analysis to determine whether the personal data breach poses a risk to the rights and freedoms of individuals.

2.3.2. The risk categories that will form the basis of the assessment are as follows:

- No Risk: The implementation of appropriate technical and administrative safeguards and the protection of personal data through measures such as encryption that renders the data unreadable to those without authorization to access it, along with additional precautions, ensure that a high risk to the rights and freedoms of data subjects is no longer possible.

- Low Risk: The individuals involved can overcome minor inconveniences.
  They may encounter (excessive time spent, inconvenience, etc.)
- Moderate Risk: Individuals may encounter difficulties that they are able to overcome.
  (extra effort, additional costs, stress, minor physical discomfort, etc.)
- High Risk: High: Individuals may face serious consequences that they will have to overcome (financial damage, loss of job, legal investigation, deterioration of health, etc.).
- Very High Risk: Individuals may face insurmountable difficulties and irreversible consequences (work stoppage, long-term psychological and physical distress, death, etc.)

If it is assessed that no risk will occur to the rights and freedoms of natural persons, the reasons leading to this assessment will be recorded.

2.3.3. When conducting a risk analysis, the Company will consider the sensitivity level of the data and the categories of individuals involved (e.g., children, vulnerable persons) to determine whether they would be at greater risk due to the breach.

2.3.4. The fact that personal data is securely encrypted using the latest encryption methods and that the keys have not been compromised in the event of a security breach may serve as grounds for concluding that the data breach does not pose a risk to the rights and freedoms of individuals and that it is not necessary to inform the Board and data owners.

2.3.5. In its risk analysis assessment, the company will take into account the recommendations of the Board, the National Cyber Incident Response Center (USOM), and the European Union Agency for Network and Information Security (ENISA).

2.3.6. If it is determined that informing the Board and data owners is not necessary, the reasons for this decision will be documented, and this documentation will be kept on file for presentation during any audits that may be conducted by the Board.

---

2 www.enisa.europa.eu/publications/dbn-severity

**2.4. Notification of the Violation to Relevant Institutions and Individuals**

2.4.1. Reporting Data Security Breach Incidents to the Personal Data Protection Board: All incidents where personal data and sensitive personal data may be at risk (situations that do not pose a risk to the rights and freedoms of data subjects are not included in this scope).
The incident will be reported to the Board without unnecessary delay and within a maximum of 72 hours of being notified of the violation.

2.4.2. **COMPLETING THE KVKK PERSONAL DATA BREACH REPORTING FORM:** After accessing the Personal Data Protection Authority's website at www.kvkk.gov.tr, click on the Personal Data Breach Reporting icon located in the menus on the right side of the homepage to enter the personal data breach reporting area.

2.4.3. The login page contains the "ANNOUNCEMENT REGARDING THE DECISION OF THE PERSONAL DATA PROTECTION BOARD DATED 24.01.2019 AND NUMBERED 2019/10 CONCERNING THE PROCEDURES AND PRINCIPLES FOR NOTIFICATION OF PERSONAL DATA BREACHES". You can access the notification page by clicking on the Personal Data Breach Notification Form (Internet) located at the bottom of this announcement page. If you wish to fill out the form manually, click on the Personal Data Breach Notification Form (PDF).

2.4.2. The notification to the Board shall include at least the following points:

- Information about the source of the violation and how it occurred.
- Individual groups affected by the violation (e.g., children, other vulnerable groups, people with disabilities,
  - Number of people and

records affected by the data breach (at least estimated).
- Categories of personal data affected by the breach (e.g., identity information, educational records, social security data, financial information, bank account numbers, passport numbers, and health data, as well as special categories of data such as race and ethnicity)
- Name and contact information of the Data Protection Liaison Officer/Manager (contact information of the officer from whom detailed information can be obtained)
- A description of the potential impact of the breach on the affected individuals (e.g., loss of control over personal data, identity theft, discrimination, restriction of rights, fraud, financial loss, reputational damage, risk of disclosure of confidential professional information, etc.).
- A description of the administrative and technical measures taken by the company before the breach, as well as the measures taken or planned to address the breach. (For example, deleting mistakenly transmitted data, securing passwords, planning data security training, etc.) If possible, measures taken to mitigate the negative impacts of the breach will also be included under this heading.

- Important Note: The fact that definitive information regarding the matters listed above is not yet available should not cause a delay in notifying the Board in a timely manner. It should be stated that the current information will be conveyed and that the institution will be informed immediately when more detailed information becomes available.

2.4.3. In cases where the data breach falls within the purview of judiciaries, law enforcement agencies, or other public institutions located abroad, and regarding this breach...

Organizations or institutions located abroad may need to be informed. If notification is made, documents verifying that the notification has been made shall be recorded and submitted to the Board.
It must be submitted with the notification.

**2.4.4 Reasons for the Company's Notification:**

(a) Avoiding administrative fines: Article 18 of the Law No. 6698 on the Protection of Personal Data. Failure to notify the Board pursuant to the relevant article may result in an administrative fine.

(b) Seeking Advice: The company may seek advice from the Board regarding measures to be taken in response to the breach, and cooperation with the Board is important in order to justify its decisions regarding informing or not informing affected data owners.

**2.4.5. Informing the Relevant Persons Affected by the Breach**

2.4.5.1. After conducting the risk analysis mentioned in section 2.3.1 above, if a personal data breach is likely to pose a “high risk” to the rights and freedoms of natural persons, the Company shall:

(a) The relevant parties will be contacted by telephone, email, etc., without unnecessary delay.

(b) It will notify relevant individuals that a data breach has occurred.

(c) It will provide data subjects with detailed information on the matters described above under heading 2.4.2.

(d) Where appropriate, it will provide specific advice to data subjects on how to protect themselves from potential negative consequences of the breach (such as password reset).

2.4.5.2. The notification to the data subject will clearly and simply explain the nature of the personal data breach and will include, at a minimum, the name and contact information of the data protection officer or another point of contact from whom further information can be obtained, the possible consequences of the personal data breach, and, where appropriate, explanations of the measures taken or recommended by our Company to address the personal data breach, including measures to mitigate the possible negative effects of the personal data breach.

2.4.6. Notification to the data subject is not mandatory if any of the following conditions are met:

(a) The company must have implemented appropriate technical and administrative safeguards, including measures such as encryption that renders personal data unreadable to anyone not authorized to access it, and these measures must have been applied to the personal data affected by the breach;

(b) The company must take additional measures to ensure that the high risk to the rights and freedoms of data subjects is no longer possible;

(c) If the notification would require an excessive effort. In this case, a public notification or similar measure, in which data subjects are informed with equal effectiveness, shall be applied instead.

**2.4.7. Notification to Law Enforcement Authorities**

(a) In case of unauthorized access to personal data, the matter shall be reported immediately to the relevant law enforcement agency.

(b) Depending on the nature of the personal data at risk, and especially where sensitive personal data may be at risk, further assistance should be requested from law enforcement.

(c) In the event of data "damage," the matter must be reported to law enforcement. Failure to do so may expose the Company to penalties and security measures.

2.4.8. Other Institutions and Organizations: If necessary, the Ministry of Health, the Ministry of Family and Social Policies, financial institutions, and other relevant ministries and organizations may be informed.

2.4.9. The company will notify the insurance company with which the insured contract has been concluded and inform them of a personal data security breach.

2.5. Utilization of Legal Consultancy and Attorney Services: The company may inform stakeholders from whom it receives legal consultancy and attorney services and may notify them of a personal data security breach in order to seek legal advice, defense in potential lawsuits, settlement, or other amicable solutions.

2.6. Actions to be Taken After a Breach: After the necessary emergency response measures are taken in the initial stage, a complete assessment and review process regarding the breach should be conducted within a reasonable time. The following points will be considered during this process:

2.6.1. It will be confirmed that personal data breaches are documented, including information about the personal data breach, its effects, and the corrective action taken.

2.6.2 The conclusions drawn from the incident, the aspects that need improvement, and the details of the measures to be taken should be determined.

2.6.3 The Company shall request an appropriate briefing and investigation report from its Data Protection Liaison Officer/Prosecutor (and/or other external experts whose experience may be utilized to assist it), and a copy of the correspondence exchanged with the Board and/or relevant parties affected by the breach shall be retained.

2.6.4 The company will carefully consider whether or not to initiate disciplinary procedures, if necessary.

2.6.5 Where corrective actions are deemed necessary, responsibility will be assigned to the relevant officials, and they will be tasked with ensuring that the necessary actions are completed within specific timeframes according to their areas of responsibility.

2.6.6 Personnel should be informed of any changes to this Response Plan and any updated security measures. Personnel should receive refresher training as needed.

## APPENDIX - SAMPLE VIOLATION REPORT
## DATA SECURITY BREACH REPORT

FOR THE USE OF KARDELEN PAINT ONLY.

Personal Data Breach: This refers to a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data that is transmitted, stored, or processed.

| | |
|---|---|
| Violation Tracking Number: | |
| When did the data security breach occur? | |
| Where did the data security breach occur? | *Location where the violation occurred* |
| When was the violation reported? | *Please specify the date and time.* |
| Who reported the security breach? | |
| Contact information for the person who reported the data breach? | |
| Has a notification been made to the Personal Data Protection Board? | **Yes ÿ No ÿ** |
| If the answer is "Yes," please specify the notification method (phone, email, etc.) and the date and time of the notification. | |
| If the answer is "No," has any other senior official, Director, etc., been contacted, and if so, by what means (e.g., phone, email, etc.) and the time and date of the contact? | |
| Are there any witnesses to the incident? If the answer is "Yes," please provide their names and telephone contact information. | |

| |
|---|
| Please provide information about the source of the violation. |
| Provide detailed information about how the violation occurred. |
| Please provide information on the categories of relevant parties affected or likely to be affected by the breach. (Interns, employees, job applicants, customers, suppliers, contractors, etc.) |
| What is the number of individuals and records affected or likely to be affected by the data breach? (If the number of individuals and/or records is an estimate, please explain why the exact numbers cannot be determined.) |
| What categories of personal data were affected by the breach? (Identity, contact, location, personal information, legal proceedings, customer transactions, physical security, transaction security, risk management, finance, professional experience, marketing, audio and visual recordings, race and ethnicity, political opinions, philosophical beliefs, clothing, association membership, health information, criminal convictions and security measures, biometric data, etc.) |

| |
|---|
| Describe the potential impacts of the breach on the affected individuals. (Loss of control over personal data, identity theft, discrimination, restriction of rights, fraud, financial loss, reputational damage, loss of personal data security, etc.) |
| Please describe the measures taken or proposed by the Company to address the personal data breach, including measures to mitigate the potential negative impacts of the personal data breach.<br><br>Important Note: Lack of awareness of the details regarding the measures mentioned above does not justify refraining from notifying the Personal Data Protection Board.<br>Information may be provided in stages without any unnecessary further delay. If so, please indicate clearly. |
| Do you think a data security breach is a temporary situation? Is it possible to recover compromised personal data and regain access to it? |

| |
|---|
| Was any IT system affected by the incident? (e.g., email, website, cloud programs, electronic document management systems, etc.) If so, please list them below. |
| Are there any additional informational materials available, such as error messages, screenshots, log files, or CCTV footage? |
| Have you taken any action to eliminate/mitigate the risks to data subjects you believe may have been affected, or to other data subjects you believe may have been affected? If your answer is “YES,” please explain below. |
| Did you inform any management personnel, such as a member of the company's Board of Directors, CEO, or Head of the IT Department, about this matter? If the answer is "YES," please briefly describe who you spoke with and what advice or instructions you received during the conversation. |
| Have you contacted any external entities, e.g., insurance companies, IT providers, law enforcement agencies, etc.? If the answer is “YES,” please describe below who you contacted and provide their names and contact information. |

.

| If there is anything else you would like to clarify, please mention it below. |
|---|
| |

| | |
|---|---|
| Edited by: | |
| Your task: | |
| Officer Being Unit: | |
| Your Contact Information: (Ideally your phone number) | |
| History: | |
| Report Completion Time: | |

Thank you for your effort in completing this form. Completing this form will help Kardelen Boya to better investigate/ analyze the matter.
Please ensure this report is forwarded directly to the Company's Data Protection Liaison Officer/Professor:

Data Protection Liaison Officer/Manager: Name and Surname:
Position:
Address:
Phone:
E-mail:

***THIS FORM HAS BEEN PREPARED TAKING INTO ACCOUNT CIVIL AND CRIMINAL CASES.**

**FOR YOUR INFORMATION:**

Data security breaches are classified according to the following generally accepted information security principles:

A) Data Privacy: This refers to preventing data from being accessed by unauthorized persons. "Confidentiality breach" refers to the unauthorized or accidental disclosure or access to personal data.

B) Data Integrity: This refers to ensuring that data is maintained and protected in the way it should be. "Breach of integrity" refers to unauthorized or accidental alterations to personal data.

C) Data Accessibility/Availability: This refers to the data being accessible and usable at all times. "Access breach" refers to the accidental or unauthorized loss of access to personal data, or the accidental or unauthorized destruction of personal data.

Depending on the circumstances, a data security breach can occur through a violation of the confidentiality, integrity, and availability of personal data, or a combination of these. Information that helps determine whether a confidentiality or integrity breach has occurred is relatively readily apparent. However, determining whether the availability of data has been breached can be more difficult. When personal data is permanently lost or destroyed, it will always be considered a breach of the data availability principle.

**PROCEDURES TO BE FOLLOWED WHEN RESPONDING TO SECURITY BREACHES.**
**THINGS YOU SHOULDN'T DO:**

**THINGS TO DO:**

- More unauthorized access, data disclosure, damage to record systems, etc.
  To prevent further incidents, immediately isolate the affected system.
- Use your phone for communication. Attackers can monitor email traffic.
- Contact the company's Data Protection Liaison Officer/Manager immediately.

  Data Protection Liaison Officer/Manager:

  Name and Surname:
  Job Title:
  Address:
  Telephone:
  E-mail:

- Retain all relevant log records, e.g., firewall, router, and intrusion detection system.

- Create backup copies of damaged or modified files and store these backups.
  Keep it in a safe place.
- Determine where the affected system is located within the network topology.
- Identify all systems and units connected to the affected system.
- Programs and processes running on the affected system(s), the impact of the outage, and permissions
  Specify the maximum allowed outage duration.
- If evidence of the affected system is collected, make arrangements to ensure service continuity, i.e., prepare a redundant system and create data backups.

**THINGS YOU SHOULDN'T DO:**

• Do not delete, move, or modify files on affected systems. • Do not contact suspected attackers. • Do not perform digital crime analysis unless authorized to do so.

**THIS FORM MUST BE FILLED OUT ONLY BY THE SOME-DATA BREACH RESPONSE TEAM.**

| | |
|---|---|
| Data Protection Liaison Officer/Manager: | |
| Date and Time of Submission of This Form to the Company: | |
| Please specify the impact of the data security breach.<br>*Data Privacy, Data Integrity, Data Access/ Availability (See explanations above)* | |
| Number of Individuals and Records Affected by the Data Breach | *Estimated number of individuals and records affected by the breach?*<br>*Which data categories are affected?* |
| Due to the data breach, what special categories of personal data (Race and ethnic origin, Political Opinion, Religious, philosophical and genetic data, Health Information, Sexual *special categories of many data* subjects' *special categories of personal data were affected* Has life been affected? | **Yes ÿ No ÿ**<br>beliefs, Relevant denomination and other beliefs, Association, union membership, Biometric *personal data) were affected? Please write the relevant information below. For example, how by the breach?* |

| | | |
|---|---|---|
| The possibility of the relevant individuals being exposed to adverse effects."<br>*Accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to transmitted, stored, or processed personal data constitutes a security breach.*<br><br>*The extent of the breach should be determined by assessing its potential impact on the affected individuals. This assessment should consider the nature and cause of the breach, the type of data involved, the measures taken to mitigate its effects, and the categories of individuals affected.*<br><br>**** If no risk is assessed, please explain the reasons:*** |  | **Very High:** Individuals may face insurmountable difficulties and irreversible consequences (work stoppage, long-term psychological and physical distress, death, etc.) |
| |  | **High:** The individuals involved may face serious consequences that they will have to overcome (material damage, loss of employment, legal investigation, deterioration of health, etc.). |
| |  | **Moderate:** Individuals may encounter manageable setbacks (excessive effort, additional costs, stress, minor physical discomfort, etc.). |
| |  | **Low:** Individuals may encounter minor setbacks that they can overcome (e.g., spending too much time, boredom). |
| |  | **No Risk:** The implementation of appropriate technical and administrative safeguards, and the protection of personal data through measures such as encryption that renders it unreadable to anyone without authorization, ensure that there is no longer a high risk to the rights and freedoms of data subjects. |

| | |
|---|---|
| Have the senior executives on the board been informed? | **Yes ÿ No ÿ** |
| Has the IT Service Provider/IT Technical Support Team been informed? | **Yes ÿ No ÿ** |
| Has the insurance company been informed? | **Yes ÿ No ÿ** |
| Has a report/complaint been filed with law enforcement? | **Yes ÿ No ÿ** |
| Have the legal advisors been informed? | **Yes ÿ No ÿ** |
| Have the relevant individuals been informed?<br><br>*Number of people involved?*<br><br>*Are there any contact lists that would allow us to reach the relevant individuals? Or is it possible to recover the contact information?* | **Yes ÿ No ÿ** |
| Has a notification been made to the Personal Data Protection Board?<br><br>*Personal Data Protection Authority*<br><br>*Phone: 0312 216 50 00*<br>*Call Center: ALO 198 Data Protection Hotline Information and Consulting Center*<br>*E-mail: veriguvenligi@kvkk.gov.tr*<br>*Web page containing the Violation Notification Form: https:// www.kvkk.gov.tr/ Icerik/ 5362/ Veri-Breach-Notification*<br>*Address: Nasuh Akar Neighborhood, 1407th Street. No:4, 06520 Çankaya/ Ankara* | **Yes ÿ No ÿ**<br><br>*If the answer is "YES," please include the date and time of the notification (if applicable).*<br>*Write down the advice and instructions received from the institution below:* |
| Other Points to Note | |
| Signature of the Data Protection Liaison Officer/Manager: | |
| CEO or Appointed Representative's Signature: | |
| History: | |

***THIS FORM IS FOR USE IN CIVIL AND CRIMINAL CASES.**

**PREPARED BY HAVING IT AVAILABLE.**