



CRISIS MANAGEMENT and NOTIFICATION POLICY IN THE EVENT OF A DATA BREACH

Version dated: 10/12/2022

1. INTRODUCTION

1.1 Objective

Paragraph 5 of article 12 with the heading of “Data Security Obligations” of the Personal Data Protection Law no 6698 (the “Law”) provides that *“If the personal data being processed is obtained by others through unlawful means, the data controller must notify the data subject and board of the situation as soon as possible. The Board may, if necessary, announce the breach on its own website or through some other means it deems appropriate.”* **YEŞİL SİYAH DENİZCİLİK LOJİSTİK LİMİTED ŞİRKETİ** (the “Company”) is a Data Controller according to the Law and aims to establish the procedure the Company should follow when notifying breaches to the Personal Data Protection Board (the “Board”) in the event of any data breaches at its Zorlu Center T0-36, 34330 Beşiktaş/Istanbul address and to determine the acts and actions required after a data breach has occurred with this Crisis Management and Notification Policy in the Event of a Data Breach (the “Policy”).

1.2 Scope

The actions and measures to be taken as well as the notification procedure to be followed in notifying the Board and the Data Subject in case of a Data Breach at the Company has been set out in this Policy and the management procedures set out in this Policy shall be implemented in the event of any kind of breach.

1.3 Abbreviations and Definitions

Within the context of this Policy, the terms listed below shall have the meanings attributed to them below.

- **Employee:** shall mean Yeşil Siyah Denizcilik Lojistik Limited Şirketi personnel,
- **Form:** shall mean the personal data breach notice form published with the Personal Data Protection Board decision numbered 2019/10 and dated 24 January 2019,
- **Law:** shall mean the Personal Data Protection Law no. 6698,
- **Personal Data:** shall mean any and all personal data that relates to an identified or identifiable natural person,
- **Board:** shall mean the Personal Data Protection Board,
- **Authority:** shall mean the Personal Data Protection Authority,
- **Sensitive Data:** shall mean personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance,

membership in associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data of an individual,

- **Policy:** shall mean the Crisis Management and Notification Policy in the event of a Personal Data Breach,
- **Data Breach:** shall mean any event whereby Personal Data under Yeşil Siyah Denizcilik Lojistik Limited Şirketi's control is 'unlawfully processed', 'unlawfully accessed', 'unlawfully acquired' from within or outside of the Company or whereby 'the technical and administrative measures enacted by the Company to protect Personal Data and ensure a level of security have been breached by unauthorized persons,
- **Data Breach Response Plan:** shall mean the procedure to be followed in the event of a Data Breach at Yeşil Siyah Denizcilik Lojistik Limited Şirketi,
- **Data Subject:** shall mean the natural person whose personal data is being processed and who has become the victim of a Data Breach,
- **Data Controller:** shall mean Yeşil Siyah Denizcilik Lojistik Limited Şirketi.

2.CRISIS MANAGEMENT AND NOTIFICATION IN THE EVENT OF A PERSONAL DATA BREACH

2.1. Responsibilities and Duties

The procedure to be implemented in case of a Data Breach at Yeşil Siyah Denizcilik Lojistik Limited Şirketi has been prepared in compliance with the Board decision numbered 2019/10 and dated 24 January 2019. In the event of any breach the departments and employees specified below shall implement the procedures indicated below:

- All Employees who suspect a Breach should notify the shareholders of Yeşil Siyah Denizcilik Lojistik Limited Şirketi.
- An investigation should be launched within Yeşil Siyah Denizcilik Lojistik Limited Şirketi and the Data Breach Response Plan (Schedule 1 – Data Breach Response Plan) must be put into action.
- It is necessary to identify the source of the Data Breach, the date the Breach occurred and the date it was discovered.
- It is necessary to identify the personal data categories and number of people who have been affected.
- The existing risks and threats concerning the Data Breach must be identified.
- If the Data Subjects affected by the Data Breach can be identified, the notices to be served on such Data Subjects in line with the procedures set out in article 2.3 of this Policy must be prepared and sent by _____.
- _____ should prepare a notice to be sent to inform the Board of the Data Breach in line with the procedures set out in article 2.2 of this Policy. If the Data



Subjects affected by the Data Breach cannot be identified, such circumstances should also be included in the notice to be sent to the Board.

- After the Board has been informed of the Data Breach, the data back-ups should be used.

2.2. Procedure for Informing the Personal Data Protection Board of a Data Breach

Those responsible according to the allocation of duties set forth in article 2.1 ("Responsibilities and Duties") of this Policy shall inform the Board of the Data Breach at the latest within 72 hours of discovering such breach in line with the Board decision numbered 2019/10 and dated 24 January 2019.

If the grace period granted for notifying the Breach to the Board proves insufficient due to just grounds, the late notification should include an explanation of the grounds for the delay.

The "Personal Data Breach Notification Form" should be used when notifying the Board of a Data Breach. **(Please check the website for the most current version of the form.)**

If the information requested in the form is not immediately available at once, the Board shall be notified in stages as the information is acquired so as not to give rise to any delay.

Details of the Data Breach, effects of such breach and the measures taken against such breach shall be filed on the record and be made available for the Board's inspection.

The Data Breach will be notified to the Board by one of the following means:

a) Notification via e-mail: if this is the first notification, the Form is filled out and then sent to the ihlalbildirimi@kvkk.gov.tr email address with a subject line of "personal data breach notification". If the notification is a follow-up notification, the Form should be added as an attachment to the e-mail that was sent with the initial notification.

b) Notification via post: if a decision is made to send the Form by post, it should be mailed to "Kişisel Verileri Koruma Kurumu (Personal Data Protection Authority) Nasuh Akar Mahallesi Ziyabey Cad. 1407. Sok. No:4, 06520 Çankaya/Ankara" by APS (first class post).

c) Notification via the website: If there is a desire to share the notification over the Authority's website, notification should be made in accordance with the "Personal Data Breach Notification Form Guidelines" published on the Authority's website on www.kvkk.gov.tr by clicking on the "Create Notification" link on <https://ihlalbildirim.kvkk.gov.tr/> and following the steps as they come up on the referred website.

2.3. Procedure for Informing the Data Subject of the Data Breach



The department and Employees described in article 2.1 (“Responsibilities and Duties”) of this Policy shall notify the affected Data Subjects in line with the rules specified below whenever any breaches occur at Yeşil Siyah Denizcilik Lojistik Limited Şirketi:

They will inform the Data Subject of the Data Breach as soon as reasonably possible after identifying the Data Subject.

The notification sent to the Data Subject must, at the very least, include the following:

- When the breach occurred,
- Which personal data was affected on a personal data category basis (by distinguishing between personal data and sensitive data),
- Possible consequences of the personal data breach,
- Measures enacted and precautions suggested to mitigate the negative impact of the data breach,
- The names and contact information of the contact persons from whom the Data Subject can obtain information regarding the Data Breach or the details of the entire website address, call center information, and similar means of communication for Yeşil Siyah Denizcilik Lojistik Limited Şirketi.

Details of the Data Breach, the effects of such breach, and the measures taken against such violation shall be filed on the record and be made available for the Board’s inspection.

The Data Breach shall be notified to the Data Subject in the manner explained below:

- If they have access to the Data Subject’s contact address, by sending it through the post to such address;
- If they do not have access to the Data Subject’s contact address, by publishing it on the Yeşil Siyah Denizcilik Lojistik Limited Şirketi website;
- Any other means determined by Yeşil Siyah Denizcilik Lojistik Limited Şirketi in compliance with legislation.

3. POLICY PUBLICATION AND SAFEKEEPING

The policy shall be published digitally. The digital copy will be saved in a shared digital space accessible within Yeşil Siyah Denizcilik Lojistik Limited Şirketi.

4. POLICY’S UPDATE INTERVAL

The Policy will be reviewed as necessary and the relevant section will be updated as required. The most current version of the Policy may be accessed from Yeşil Siyah Denizcilik Lojistik Limited Şirketi’s _____ department or the shared digital space.

5. EFFECTIVENESS AND ABOLISHMENT OF THE POLICY



The Policy will be deemed to enter into effect upon its publication on Yeşil Siyah Denizcilik Lojistik Limited Şirketi's shared digital space.

6. APPROVA

Version	Date Approved	Approved By	Signature
1			

7. CIRCULATED TO AND SHARED WITH

All Yeşil Siyah Denizcilik Lojistik Limited Şirketi Employees

Joint Information Sharing Areas (Document Management System, Company File Sharing System)

SCHEDULE 1 – DATA BREACH RESPONSE PLAN

All Employees of Yeşil Siyah Denizcilik Lojistik Limited Şirketi must comply with this Policy and any instructions issued by the shareholders of Yeşil Siyah Denizcilik Lojistik Limited Şirketi concerning the methods to be implemented in the event of a Data Breach at Yeşil Siyah Denizcilik Lojistik Limited Şirketi. Furthermore, employees shall promptly inform the responsible departments in writing of any occurrence or suspicion of a Data Breach that may have occurred at the Company.

As soon as a Data Breach is identified, the Data Breach Response Plan described in the Policy shall be implemented regardless of who has placed such Data Breach. The persons listed in Table 1 shall begin investigating the breach as soon as they have been notified. The investigation shall focus on “identifying the source of the Data breach when the breach occurred, and when the breach was finally identified, the personal data categories that have been affected, and the risks and threats corresponding to the Data Breach.” The following issues must be taken into consideration when identifying potential risks and threats:

- Whether the personal data is also categorized as sensitive data;
- The level of confidentiality such data requires by its very nature;
- The nature and amount of damage the data subject may suffer due to the security breach.

A report describing and prioritizing these risks shall be prepared. The measures described in the Data Breach Response Plan and set out below are aimed at mitigating or even eliminating such risks and must be implemented:

1) Ensuring Cyber Security: shall serve as the first line of defense against the threat of unauthorized access to the information technology systems containing personal data. If a Data Breach does occur, it shall be necessary to:

- Determine whether the unauthorized access/attack was made from inside or outside of the Company,
- Attempt to ascertain whether the unauthorized access/attack on the Company systems is still ongoing,
- Investigate the cause of the breach,
- Conduct a study to identify the potential problems the breach may cause to the Company’s course of business,
- Make the necessary changes to the passwords, access authorization, and control matrix about the sections thought to be connected to the Breach and restrict access authorizations if necessary,
- Put away and store any devices believed to be subject to the breach or a crime or any devices believed to have served as an intermediary vehicle and, except where urgent intervention is required, not use such devices until the requisite legal determinations can be made;

- Implement actions such as rebooting systems that need to be operational after the Breach, evaluate the general security measures about the breached section, report on and correct any points that appear deficient, and enact new measures.

2) Ensuring the Physical Security of Data: If the Data Breach or Potential Data Breach at Yeşil Siyah Denizcilik Lojistik Limited Şirketi occurs in an actual physical environment and:

- If it is discovered that documents, hard disks, USB sticks, or some other similar storage device containing personal data and other electronic devices are being kept in a public area of the Company or if any of these are stolen, such items shall be stored in an enclosed space such as an envelope or box so that the information contained therein cannot be read by anyone until the person who is the author/owner/data subject of the document can be found. If the item is stored in such a way as a document, and its author/owner/data subject cannot be found, the record shall be destroyed at the end of the retention period.
- Suppose it is discovered that cabinets, boxes, and other similar storage items that should be kept closed within the Company are being left open to access by all. In that case, such cabinets or boxes shall be secured until the owner/person concerned/data subject can be identified.
- Yeşil Siyah Denizcilik Lojistik Limited Şirketi shareholders should be promptly notified if a fire or any other circumstance that could destroy or harm documents or devices containing personal data are observed within the Company at a location where personal data is kept or near the such site.
- If available, camera recordings from the location of the Breach shall be examined, and interviews will be held with other Employees of Yeşil Siyah Denizcilik Lojistik Limited Şirketi who might have information and opinions on the matter. Furthermore, if deemed necessary, data and any documents as may be required concerning the event shall be shared with Company consultants such as lawyers, and legal action may be taken.
- Actions such as evaluating the general security measures concerning the section that suffered a breach, reporting on and correcting any points that appear deficient, and enacting new measures shall be implemented.

3) Keeping Files on the Elements of the Data Breach for the Record: Files shall be marked as a record of the identification of the source of the Data Breach, when the breach occurred and when it was identified, as well as the determinations made about the personal data categories that were affected and be made available for the Board's inspection.

4) Making Use of the Personal Data Backups: If the personal data is damaged, destroyed, stolen, or lost for any reason whatsoever, data controllers must continue operations as quickly as possible by making use of the backups of such data.