**YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**PERSONAL DATA BREACH POLICY AND NOTIFICATION PROCEDURE**

**1. Introduction**

Dear Employees,

As YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ (“YARN DAY”), we place great importance on the protection of personal data. We take all necessary administrative and technical measures to ensure that personal data processed within YARN DAY continues to be handled in accordance with the law. The timely and effective implementation of these measures by you greatly supports YARN DAY’s efforts in the field of personal data protection.

As you know, YARN DAY has certain obligations under the Personal Data Protection Law (“KVKK”) and related secondary legislation. One of these obligations is to notify the relevant parties, namely the data subjects whose personal data have been unlawfully obtained by third parties (“Data Breach”), and the Personal Data Protection Board (“Board”) as soon as possible, in the event that personal data processed is obtained by others through illegal means. Below are the details and your obligations in this regard.

**2. Purpose**

This Policy has been prepared to fulfill our above-mentioned obligation and to determine the steps to be taken in the event of such an incident.

**3. Scope**

This Policy is applicable to every employee of YARN DAY who deals with personal data.

**4. Obligations**

Every employee of YARN DAY who deals with personal data is required to review and implement this Policy. In addition, YARN DAY employees must make the notifications specified in this Policy in the manner and within the time limits specified in this Policy.

**5. Personal Data Breach**

A Personal Data Breach is the situation where personal data is at risk of being obtained by unauthorized third parties in various ways. Therefore, any situation where such a risk is present should be considered a personal data breach and should be reported to YARN DAY as explained below. Examples of Personal Data Breaches include:

* Loss, leaving unattended for a certain period, or theft of equipment where data is stored (printed documents, SD cards, USB drives, laptops, tablets, smartphones, etc.),
* Unauthorized access to data or information systems (intentionally or accidentally sharing user session information to gain unauthorized access or make unauthorized changes to data or information systems),
* Unauthorized disclosure of sensitive or confidential information (e.g., sending emails or messages to unauthorized persons through movable devices or emails sent to the wrong recipient or address),
* User accounts with disclosed login information (e.g., accidentally disclosing login information through phishing),
* Successful or unsuccessful attempts to gain unauthorized access to YARN DAY information or information systems,
* Equipment failure,
* Malware or other harmful software.
* Any situation where there is a risk of personal data being obtained by unauthorized third parties, not limited to the above examples.

**6. Notification**

Every incident that carries the risk of unauthorized access to personal data, as given in the examples above, must be reported to **info@yarnday.com** via e-mail by filling out the attached form immediately and no later than 12 hours. The Data Controller will evaluate whether an incident actually poses a risk of access to personal data after the notification. Therefore, even if there is the slightest possibility, it is necessary to make the notification.

It is very important to make the notification as early as possible to prevent damages that may arise from the risk of a data breach.

If a data breach is detected, it will be reported to the Board and the relevant data subject within 72 hours from the date of occurrence by the Data Controller through the form available on the Board’s website.

If you have any questions about this Policy, please contact the Personal Data Protection Unit.

**EK – 1 Description of Incident Form**

Olayı bildiren YARN DAY çalışanının;

|  |  |
| --- | --- |
| Name: |  |
| Surname: |  |
| Department: |  |
| Date of Incident: |  |
| Time of Incident: |  |
| Description of Incident (Select one) |  |

  Denial of Service Attack (Dos/DDos)

  Information Leakage

  Malware

  Identity Spoofing

  Database Attack (SQL Injection)

  Phishing

  Data Exposure

  Sending Email/Message to the Wrong Recipient

  Document Loss

  Password Compromise

  Suspicion of Unauthorized Account Access

  Loss of Movable Device

  Other

Description of the Incident:

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Name  Surname |  |
| Date |  |
| Signature |  |

**YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**STEPS TO BE FOLLOWED IN CASE OF DATA BREACH**

Detection of a Data Breach (e.g., sending an email to the wrong recipient, detection of a data leak, loss of a movable device or file)

Completing the incident notification form, which is included as an appendix to the Company's Personal Data Breach Policy and Notification Procedure, in full and without any omissions.

The incident notification form must be sent to **info@yarnday.com** within 12 hours from the moment the breach is detected.

The Data Controller shall notify the Board of the data breach by filling out the form available on the Board’s website within 72 hours from the moment the breach occurs.

What constitutes a data breach, along with examples, can be found in the Personal Data Breach Policy and Notification Procedure.