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

**KİŞİSEL VERİ AÇIĞI POLİTİKASI VE BİLDİRİM PROSEDÜRÜ**

1. **Giriş**

Değerli çalışanlarımız,

Şirketimiz YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ **(“YARN DAY”)** olarak kişisel verilerin korunmasına büyük bir önem vermekteyiz. YARN DAY bünyesinde işlenen kişisel verilerin hukuka uygun bir şekilde işlenmeye devam etmesi için gerekli tüm idari ve teknik tedbirleri almaktayız. Alınan bu tedbirlerin sizler tarafından zamanında ve efektif bir şekilde uygulanması YARN DAY’in kişisel verilerin korunması kapsamında ortaya koyduğu çabalara büyük bir destek sağlamaktadır.

Bilindiği üzere YARN DAY olarak Kişisel Verilerin Korunması Kanunu (“**KVKK**”) ve ilgili ikincil mevzuat kapsamında birtakım yükümlülüklerimiz mevcuttur. Bu yükümlülüklerden birisi de işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde (“**Veri İhlali**”), bu durumu en kısa sürede ilgilisine yani kişisel verileri hukuka aykırı olarak üçüncü kişilerin eline geçen veri sahibi gerçek kişilere ve Kişisel Verilerin Korunması Kurulu’na (“**Kurul**”) bildirme yükümlülüğü olup aşağıda bu konuya ilişki detaylar ve yükümlülükleriniz bilginize sunulmuştur.

1. **Amaç**

İşbu Politika, yukarıdaki yükümlülüğümüzü yerine getirebilmek ve böyle bir durum ile karşılaşılması halinde atılması gereken adımları belirlemek üzere hazırlanmıştır.

1. **Kapsam**

İşbu Politika, YARN DAY’in kişisel verilerle ilgili işlem yapan her çalışanı için geçerlidir.

1. **Yükümlülükler**

YARN DAY’in kişisel veriler ile ilgili işlem yapan her çalışanı işbu Politika’yı incelemek ve uygulamakla yükümlüdür. Buna ek olarak, YARN DAY çalışanları, bu Politika’da belirtilen bildirimleri bu Politika’da belirtildiği usulde ve belirtilen sürede yapmalıdır.

1. **Kişisel Veri Açığı (Veri İhlali)**

Kişisel Veri Açığı, birden fazla şekilde oluşabilen ve kişisel verilerin yetkisiz 3. kişilerin eline geçme ihtimalinin oluşmasıdır. Bu sebeple, böyle bir ihtimalin olduğu her durum bir kişisel veri açığı olarak kabul edilmeli ve aşağıda açıklanacağı şekilde YARN DAY’e bildirilmelidir. Kişisel Veri Açığı’na örnek olarak aşağıdakiler verilebilir;

* Verilerin depolandığı ekipmanın kaybı, belirli bir süre denetimsiz ve erişilebilir bırakılması veya çalınması (basılı evrak, SD kart, USB, laptop, tablet, akıllı telefon vb. ekipmanlar)
* Veri veya bilgi sistemlerine yetkisiz erişim (Yetkisiz erişim elde etmek veya veri veya bilgi sistemlerinde yetkisiz değişiklik yapmak için kasıtlı veya yanlışlıkla kullanıcı oturum bilgilerini paylaşma)
* Hassas veya gizli bilgilerin yetkisiz olarak ifşa edilmesi (örneğin yanlış bir alıcıya veya yanlış bir adrese veya alıcıya gönderilen e-postaya gönderilen e-postalar veya taşınır cihazlar aracılığıyla yetkisiz kişilere gönderilen mesajlar)
* Giriş bilgileri ifşa olmuş kullanıcı hesapları (örn. Yanlışlıkla kimlik avı yoluyla kullanıcı girişi bilgilerini ifşa etme)
* YARN DAY bilgi veya bilgi sistemlerine yetkisiz erişim elde etmek için başarısız veya başarılı girişimler
* Ekipman arızası,
* Malware vb. zararlı yazılımlar.
* Bunlarla sınırlı olmamak üzere kişisel verilerin yetkisiz üçüncü kişilerin eline geçmesi ihtimali bulunan tüm durumlar
1. **Bildirim**

Yukarıda örnekleri verilen ve kişisel verilere yetkisiz kişilerin erişme ihtimalini barındıran her olay ek’li form doldurularak derhal ve en geç 12 saat içerisinde info@yarnday.com adresine e-posta yoluyla bildirilmelidir. Bir olayın gerçekten kişisel verilere erişim riski oluşturup oluşturmadığı konusunda değerlendirme, bildirim sonrasında Veri Denetçisi tarafından yapılacaktır. Bu sebeple en ufak bir ihtimal dahi olsa söz konusu bildirimi yapmanız gerekmektedir.

Bildirimin mümkün olduğunca erken yapılması, veri açığı ihtimalinden kaynaklanan zararların önüne geçebilmek için çok önemlidir.

Veri ihlalinin tespit edilmesi halinde söz konusu ihlal ortaya çıktığı tarihten itibaren 72 saat içerisinde Kurul’a ve ilgili veri sahibine Kurul’un internet sitesinde yer alan form aracılığıyla Veri Denetçisi tarafından bildirilecektir.

İşbu Politika hakkında herhangi bir sorunuz olması durumunda Kişisel Verileri Koruma Birimi ile bağlantıya geçebilirsiniz.

**EK – 1 Olay Bildirim Formu**

Olayı bildiren YARN DAY çalışanının;

|  |  |
| --- | --- |
| Adı: |  |
| Soyadı: |  |
| Departmanı: |  |
| Olay Tarihi: |  |
| Olay Saati: |  |
| Olay Tanımı (lütfen birini seçiniz): |  |

* Servis Dışı Bırakma Saldırısı (Dos/DDos)
* Bilgi Sızdırma
* Zararlı Yazılım
* Kimlik Taklidi
* Veritabanı Saldırısı (Sql Injection)
* Oltalama (Phishing)
* Veri İfşası
* Yanlış Kişiye e-posta/mesaj gönderimi
* Dokuman Kaybı
* Parola Ele Geçirme
* Hesaba İzinsiz Erişim Şüphesi
* Taşınır Cihaz Kaybı
* Diğer

Olay Açıklaması

|  |
| --- |
|  |

|  |  |
| --- | --- |
| AdSoyad |  |
| Tarih |  |
| İmza |  |

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

**VERİ İHLALİ[[1]](#footnote-1) HALİNDE İZLENECEK ADIMLAR**

Veri İhlalinin (örneğin; yanlış kişiye e-posta gönderilmesi, veri sızıntısı tespit edilmesi, taşınır cihaz veya dosya kaybı) tespit edilmesi

Şirket Kişisel Veri Açığı Politikası ve Bildirim Prosedürü’nün ekinde yer alan olay bildirim formunun eksiksiz olarak doldurulması

İhlalin tespit edildiği andan itibaren 12 saat içerisinde olay bildirim formunun info@yarnday.com mail adresine iletilmesi

Veri Denetçisi, ihlalin ortaya çıktığı andan itibaren 72 saat içerisinde Kurul’un internet sitesinde yer alan formu doldurarak Kurul’a veri ihlal bildiriminde bulunur.

**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.

**Attachment 1 – Description of Incident Form**

|  |  |
| --- | --- |
| 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:

|  |
| --- |
|  |

|  |  |
| --- | --- |
| NameSurname |  |
| 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.

1. Veri ihlalinin ne olduğu, örneklerin de yer aldığı Kişisel Veri Açığı Politikası ve Bildirim Prosedürü’ nden öğrenilebilir. [↑](#footnote-ref-1)