SİDERKEMCO METALURJİ SAN. VE TİC. A.Ş.
KİŞİSEL VERİ AÇIĞI POLİTİKASI VE BİLDİRİM PROSEDÜRÜ

Değerli çalışanlarımız,

Siderkemco Metalurji San. ve Tic. A.Ş. ("**Şirket**") olarak kişisel verilerin korunmasına büyük bir önem vermekteyiz. Şirketimiz bünyesinde işlenen kişisel verilerin hukuka uygun bir şekilde işlenmeye devam etmesi için gerekli idari ve teknik tedbirleri almaktayız. Alınan bu tedbirlerin sizler tarafından zamanında ve efektif bir şekilde uygulanması Şirketimizin kişisel verilerin korunması kapsamında ortaya koyduğu çabalara büyük bir destek sağlamaktadır.

Bildiğiniz üzere Şirket olarak Kişisel Verilerin Korunması Kanunu ve ilgili ikincil mevzuat kapsamında birtakım yükümlülüklerimiz mevcuttur. Bu yükümlülüklerden birisi de işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurula bildirme yükümlülüğü olup, aşağıda bu konuya ilişki detaylar ve yükümlülükleriniz bilginize sunulmuştur.

1. AMAÇ

İşbu Kişisel Veri Açığı Politikası ve Bildirim Prosedürü ("**Politika**"), yukarıdaki yükümlülüğümüzü yerine getirebilmek ve böyle bir durum ile karşılaşılması halinde atılması gereken adımları belirlemek üzere hazırlanmıştır.

2. KAPSAM

İşbu Politika, Şirketimizin kişisel verilerle ilgili işlem yapan her çalışanı için geçerlidir.

3. YÜKÜMLÜLÜKLER

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

4. KİŞİSEL VERİ AÇIĞI

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 Şirketimize bildirilmelidir. Kişisel Veri Açığı'na örnek olarak aşağıdakiler verilebilir:

- Verilerin depolandığı ekipmanın kazara kaybı, belirli bir süre denetimsiz ve erişilebilir bırakılması veya çalınması (basılı evrak, sd kart, usb, 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)
- Giriş bilgileri ifşa olmuş kullanıcı hesapları (örn. Yanlışlıkla kimlik avı yoluyla kullanıcı girişi bilgilerini ifşa etme)
- Şirketimizin bilgi veya bilgi sistemlerine yetkisiz erişim elde etmek için başarısız veya başarılı girişimler
- Ekipman arızası,
- Malware vb zararlı yazılımlar.

5. BİLDİRİM

Yukarıda örnekleri verilen ve kişisel verilere yetkisiz kişilerin erişme ihtimalini barındıran her olay ekli form doldurularak derhal ve en geç 24 saat içerisinde […] adresinde e-posta yoluyla bildirilmelidir. Bir olayın gerçekten kişisel verilere erişim riski oluşturup oluşturmadığı konusunda değerlendirme, bildirim sonrasında Şirketimiz yönetimi ya da görevlendireceği birimler 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 ve gerekiyorsa Şirketimiz tarafından Kişisel Verileri Koruma Kurulu'na yapılacak Veri İhlal Bildirimi için önem arz etmektedir.

6. İLETİŞİM

İşbu Politika hakkında herhangi bir sorunuz olması durumunda […] e-posta adresinden […] ile bağlantıya geçebilirsiniz.

7. POLİTİKA'NIN KABULÜ

İşbu Politika, Şirketimizin […] tarihli yönetim kurulunda onaya sunulmak üzere hazırlanmış olup, Yönetim Şirketimiz yönetim kurulunun onayı ile yürürlüğe girecektir. İşbu Politika, gerekli görüldüğü hallerde Şirket tarafından revize edilebilir. Revizyonun söz konusu olduğu hallerde, Politika'nın en güncel haline Şirket'in internet sitesinde yer verilecektir.

Ek-1: Olay Bildirim Formu

EK – 1 Olay Bildirim Formu

Olayı bildiren Şirketimiz çalışanının;

Adı	
Soyadı	
Departmanı	
Olay Tarihi	
Olay Saati	
Olay Tanımı	(aşağıdan seçiniz)

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

  _____

Olay Açıklaması

Adı - Soyadı

Tarih

İmza