Ek -5 Kişisel Veri Açığı Politikası ve Bildirim Prosedürü

1. Giriş

Değerli çalışanlarımız,

LİTERATUR M.I.C.E. olarak kişisel verilerin korunmasına büyük bir önem vermekteyiz. Şirketimiz 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 LİTERATUR M.I.C.E.' ın kişisel verilerin korunması kapsamında ortaya koyduğu çabalara büyük bir destek sağlamaktadır.

Bildiğiniz üzere LİTERATUR M.I.C.E. 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.

2. Amaç

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

3. Kapsam

İşbu Politika, LİTERATUR M.I.C.E.'ın kişisel verilerle ilgili işlem yapan her çalışanı için geçerlidir.

4. Yükümlülükler

LİTERATUR M.I.C.E.'ın kişisel veriler ile ilgili işlem yapan her çalışanı işbu Politika'yı incelemek ve uygulamakla yükümlüdür. Buna ek olarak, LİTERATUR M.I.C.E. çalışanları, bu Politika'da belirtilen bildirimleri bu Politika'da belirtildiği usulde ve belirtilen sürede yapmalıdır.

5. Kişisel Veri Açığı

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 LİTERATUR M.I.C.E. 'a 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)
- LİTERATUR M.I.C.E. bilgi veya bilgi sistemlerine yetkisiz erişim elde etmek için başarısız veya başarılı girişimler

- Ekipman arızası,
- Malware vb. zararlı yazılımlar.

6. Bildirim

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 …… 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.

İşbu Politika hakkında herhangi bir sorunuz olması durumunda …….. ile bağlantıya geçebilirsiniz.

EK – 1 Olay Bildirim Formu

Olayı bildiren 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 Incejtion)
- 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

Ad- Soyad
Tarih
İmza