

VERİ İHLALİ MÜDAHALE PLANI

Amaç, Kapsam ve Tanımlar

Amaç

Bu Planın amacı, BURSA TEMİZ ENERJİ ELEKTRİK ÜRETİM SAN. VE TİC. A.Ş. ("Şirket") tarafından kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerin korunması ve kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin muhafazasının sağlanması amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüklerini yerine getirmek amacıyla işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu sıfatıyla **Şirket** tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konulara ilişkin rolleri ve sorumlulukları tanımlamak, usul ve esasları düzenlemektir.

Kapsam

Bu Planın kapsamı, Şirket tarafından fiziki veya elektronik ortamda işlenen kişisel verilerin işlenmesinde görevli çalışanları içermektedir.

Tanımlar

Bu Planın uygulanmasında;

1. **Açık rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
2. **İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,
3. **Kanun:** 6698 sayılı Kişisel Verilerin Korunması Kanununu,
4. **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
5. **Kişisel verilerin işlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
6. **Kurul:** Kişisel Verileri Koruma Kurulunu,
7. **Plan:** Şirket Veri ihlali müdahale planını,
8. **Veri ihlali:** Veri sorumlusu tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesini,
9. **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
10. **Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

11. **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Veri İhlali

Kanun'un 12'nci maddesinin 5'inci fıkrası gereğince, Şirket tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesidir.

Yukarıdaki tanıma ilaveten; iletilen, saklanan veya işlenen kişisel verilerin kazara yasadışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması ve/veya bunlara erişime yol açan bir güvenlik ihlalinin meydana gelmesi de yine Plan kapsamında Veri İhlali olarak nitelendirilecektir.

Hedefler, Görevliler ve Sorumluluklar

Hedefler

Bir Veri İhlali yaşanması durumunda, Şirket'in Plan çerçevesinde hedefleri:

1. Veri İhlaline sebep olan olayı dâhili olarak tüm ilgili departmanlar nezdinde araştırmak (gerektiği hallerde kolluk kuvvetleri ve diğer kamu kurum ve kuruluşları ile iş birliği içerisinde),
2. Veri İhlalinin kaynağını tespit etmek,
3. Veri İhlalinden etkilenen kişisel veri kategorilerini tespit etmek,
4. Veri İhlalinden etkilenen kişi gruplarını/ tarafları tespit etmek,
5. Veri İhlalinden etkilenen tarafların mevcutta uğradıkları ve uğramaları muhtemel potansiyel etkileri tespit etmek ve varsa bu etkilerden doğan zararların en asgariye indirilmesini sağlamak,
6. Veri İhlali neticesinde Şirket'in organizasyonuna olan etkilerinin, ticari kaybın, operasyonlardaki azalmanın, itibarî kayıpların ve/veya finansal zararların boyutlarını tespit etmek ve hukuka uygun bir şekilde en asgariye indirilmesini sağlamak,
7. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek,
8. Eğer siber saldırı varsa;
 - a. Bilgi sistemlerinin siber saldırıdan etkilenip etkilenmediğini,
 - b. Saldırı sonucu gerçekleşen ihlal unsurunu,
 - c. Siber saldırının Şirket'in organizasyonuna olan etkilerini ve
 - d. Siber saldırı sonrasındaki iyileşmenin zamanını tespit etmek,
9. İhlalin tekrarlanmaması için atılan adımları belirlemek ve bunların tahminen ne kadar zamanda tamamlanacağını hesaplamak,
10. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı,
 - a. Kanuna uygun şekilde Kurula 72 saat içerisinde bildirmek,
 - b. Veri İhlalinden etkilenen ilgili kişilere en kısa sürede uygun yöntemlerle bildirmek,
 - c. Çalışanlara en kısa sürede bildirmek,
 - d. Eğer gerekiyorsa yurtiçinde bulunan diğer organizasyon veya kurumlara ilgili yasal yükümlülüklerle uygun sürede bildirmek,

11. Yurt dışında bulunan diğer veri koruma otoriteleri veya ilgili kurumlara ilgili yasal yükümlülüklerle uygun sürede bildirmek,
12. Gelecekte meydana gelmesi ihtimaline karşı olası Veri İhlallerinin en aza indirilmesi için Veri İhlaline yol açan olay sonrası iç denetimi tertiplemek, eğitim faaliyetleri düzenlemek ve iç iletişimi sağlamak ve
13. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurmaktır.

Görevliler ve Sorumluluklar

Veri İhlali yaşanması halinde bu Plan gereğince Şirket bünyesinde görevli departmanlar, Veri İhlaline neden olan olayın niteliğine göre belirlenir; departmanlardan her birinden en az bir temsilci görevlendirilecektir. Temsilcilerin sorumluluklarına da aşağıda belirtilmiştir.

<u>Görevli Departman</u>	<u>Veri İhlali Halinde Sorumlulukları</u>
Yönetim	1. Veri İhlaline sebep olan olayı dâhili olarak tüm ilgili departmanlar nezdinde (gerektiği hallerde kolluk kuvvetleri ve diğer kamu kurum ve kuruluşları ile iş birliği içerisinde) araştırmak 2. Veri İhlalinin kaynağını tespit etmek 3. Veri İhlalinden etkilenen kişisel veri kategorilerini tespit etmek 4. Veri İhlalinden etkilenen kişi gruplarını/tafaları tespit etmek 5. Veri İhlalinden etkilenen tarafların mevcutta uğradıkları ve uğramaları muhtemel potansiyel etkileri tespit etmek ve varsa bu etkilerden doğan zararların en asgariye indirilmesini sağlamak 6. Veri İhlali neticesinde Şirket'in organizasyonuna olan etkilerinin, ticari kaybın, operasyonlardaki azalmanın, itibarî kayıpların ve/veya finansal zararların boyutlarını tespit etmek ve hukuka uygun bir şekilde en asgariye indirilmesini sağlamak 7. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek 8. İhlalin tekrarlanmaması için atılan adımları belirlemek ve bunların tahminen ne kadar zamanda tamamlanacağını hesaplamak 9. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı, Kanuna uygun şekilde Kurula 72 saat içerisinde bildirmek 10. Yurt dışında bulunan diğer veri koruma otoriteleri veya ilgili kurumlara ilgili yasal yükümlülüklerle uygun sürede, bildirmek

	11. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurmak 12. Gelecekte meydana gelmesi ihtimaline karşı olası Veri İhlallerinin en aza indirilmesi için Veri İhlaline yol açan olay sonrası iç denetimi tertiplemek, eğitim faaliyetleri düzenlenmesini ve iç iletişimi sağlamak 13. Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunması durumunda yine Kurula gerekli bildirimin yapılmasını sağlamak 14. Planın, yürürlük tarihinden itibaren her 6 (altı) ayda bir gözden geçirilmesini sağlamak
Bilgi İşlem Departmanı	Veri ihlalinin siber saldırı veya diğer başka bir elektronik yolla gerçekleşmesi halinde; 1. Bilgi sistemlerinin Veri İhlalinden etkilenip etkilenmediğini tespit etmek 2. Veri İhlali sonucu gerçekleşen ihlal unsurunu tespit etmek 3. Veri İhlalinin Şirket'in organizasyonuna olan etkilerini tespit etmek 4. Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek
İnsan Kaynakları Departmanı	1. Veri ihlalinin Şirket çalışanı tarafından gerçekleştirilip gerçekleştirilmediğini tespit etmek 2. Şirket çalışanlarının Veri İhlalinden etkilenip etkilenmediğini tespit etmek 3. Veri İhlali sonucu gerçekleşen ihlal unsurunu, Veri İhlalinin Şirket'in organizasyonuna olan etkilerini ve Veri İhlali sonrasındaki iyileşmenin zamanını tespit etmek 4. Veri İhlaline yol açan olay sonrası eğitim faaliyetleri hazırlamak ve iç iletişimi gerçekleştirmek 5. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı çalışanlara en kısa sürede bildirmek 6. Veri İhlaline yol açan olay sonrası iç denetimi gerçekleştirmek 7. Veri İhlaline sebep olan olayı veya olay sonucu ortaya çıkan kaybı, Veri İhlalinden etkilenen ilgili kişilere en kısa sürede uygun yöntemlerle bildirmek 8. Eğer gerekiyorsa yurtiçinde bulunan diğer organizasyon veya kurumlara ilgili yasal yükümlülüklerle uygun sürede bildirmek

Veri Sorumlusu Tarafından Bildirim

Veri İhlali bildirimleri, ihlalden etkilenen kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkân verecek önlemler alınmasını sağlamak amacıyla Kurul'a ve ihlalden etkilenmiş kişilere yapılmalıdır. Buna ilişkin Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı doğrultusunda hazırlanan işbu Plan gereğince şirketin;

1. Veri İhlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesi,
2. Söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliriyorsa doğrudan, ulaşamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapması,
3. Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması,
4. Kurula yapılacak bildirimde <https://ihlalbildirim.kvkk.gov.tr/> adresinde yer alan "Kişisel Veri İhlal Bildirim Formu'nun veya işbu Planın ekinde yer alan "EK-1 Kişisel Veri İhlal Bildirim Formu'nun kullanılması,
5. Kurula yapılacak bildirimde <https://ihlalbildirim.kvkk.gov.tr/> adresinde yer alan "Kişisel Veri İhlal Bildirim Formu'nun kullanılması halinde işbu Planın ekinde yer alan "EK-2 Kişisel Veri İhlali Bildirim Formu (Internet) Kılavuzu'nun okunması,
6. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanması ve
7. Veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması gerekmektedir.

Şirket bildirimine ilişkin yukarıda sayılı tüm işlemleri yukarıda belirtilen birimlerce yürütür.

İlgili Kişiye Bildirim Esasları

Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarih ve 2019/271 Sayılı Kararı doğrultusunda, veri ihlalden etkilenen veya etkilenmiş olduğundan şüphelenilen ilgili kişilere yapılacak bildirim açık ve sade bir dille yapılacak ve bildirimde asgari olarak şu unsurlar bulunacaktır:

1. İhlalinin ne zaman gerçekleştiği,
2. Kişisel veri kategorileri bazında (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
3. Kişisel veri ihlalinin olası sonuçları,
4. Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
5. İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları

Veri İşleyen Tarafından Bildirim

Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusu olan Şirket'e bildirimde bulunması gerekmektedir. Veri işleyen bildirimini müteakip Şirket tarafından, Kurul'a bildirim yapılacaktır.

Yurt Dışı Veri İhlali

Veri ihlalinin yurt dışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye’de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye’de faydalanmaları durumunda, bu veri sorumlusu tarafından da Planın 6’ncı maddesinde belirtilen esaslar çerçevesinde Kurula bildirimde bulunulacaktır.

Yürürlük

Şirket tarafından hazırlanan bu Plan yönetim organı tarafından alınan karar doğrultusunda yürürlüğe girdiği tarihten itibaren geçerlidir.

Planın Gözden Geçirilmesi

Hazırlanan ve yürürlüğe konulan bu Plan, yılda bir periyodik olarak gözden geçirilir.

**BURSA TEMİZ ENERJİ ELEKTRİK
ÜRETİM SAN. VE TİC. A.Ş.**
Esentepe Mah. Okul Cad. No:2/7 Nilüfer/BURSA
Tel:(0 224) 249 17 27 Fax:(0 224) 249 17 89
Nilüfer V. D. Q90 018 6867