KİŞİSEL VERİ SAKLAMA VE İMHA PROSEDÜRÜ

İÇİNDEKİLER

1. AMAÇ

İşbu Kişisel Veri Saklama ve İmha Prosedürünün ("Prosedür") amacı, CK Boğaziçi Elektrik Perakende Satış A.Ş.'nin ("CK Boğaziçi" veya "Şirket") veri sahiplerine ait kişisel verilerin saklaması ve güvenliği hususundaki prensiplerin ve veri imhası standartlarının, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("Kanun"), 28.10.2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik"), Kişisel Verileri Koruma Kurumu tarafından Nisan 2025 tarihinde resmi Kurum internet sitesinde yayımlanan ve kişisel verilerin hukuka aykırı olarak işlenmesini, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla veri sorumlularının alması gereken teknik ve idari tedbirleri içerir Kişisel Veri Güvenliği Rehberi ("Rehber")ve diğer ilgili mevzuatlarda düzenlenen usul ve esaslara göre belirlenmesidir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler veri sorumlusu sıfatıyla Şirket tarafından bu doğrultuda hazırlanmış olan prosedüre uygun olarak gerçekleştirilir.

2. KAPSAM

Şirket çalışanları, çalışan adayları, stajyerler, ürün veya hizmet alan kişiler, potansiyel ürün veya hizmet alıcıları, tedarikçiler, tedarikçi yetkilileri, tüzel kişi temsilcileri, kamu kurum ve kuruluşları yetkilileri, ziyaretçilere ve diğer üçüncü kişilere ait kişisel veriler bu prosedür kapsamındadır. Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerinde bu prosedür uygulanır.

3. SORUMLULUK

Bu Prosedürün hazırlanması, güncellenmesi, geliştirilmesi ve yürütülmesinden CK Enerji Uyum Müdürlüğü ve Şirket KVKK Komitesi sorumludur. Şirket tüm birimleri ve çalışanları, prosedür kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi, güvenlik risklerinin belirlenebildiği bir ortam yaratılması, farkındalığının arttırılması, izlenmesi ve denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin, erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenilen ve erişilen bu verilerin kayıt altında tutulduğu tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir. Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlamalarına ait dağılım Tablo 1'de verilmiştir.

4. KISALTMALAR & TANIMLAR

a) **Şirket :** CK Boğaziçi Elektrik Perakende Satış A.Ş.
b) **Prosedür :** Kişisel Veri Saklama ve İmha Prosedürü
c) **Alıcı Grubu :** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
d) **Açık Rıza :** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
e) **Anonim Hale Getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
f) **Elektronik Ortam:** Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.

g) **Elektronik Olmayan Ortam:** Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
h) **Hizmet Sağlayıcı:** Kişisel Verileri Koruma ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
i) **İlgili Kişi:** Kişisel verisi işlenen gerçek kişi.
j) **İlgili Kullanıcı :** Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.
k) **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
l) **Kanun:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu.
m) **Kayıt Ortamı:** Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
n) **Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
o) **Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
p) **Kişisel Verilerin İşlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
q) **Kurul:** Kişisel Verileri Koruma Kurulu.
r) **KVKK Komitesi :** Kişisel verilerin korunması amacıyla, Şirket özelinde CK Enerji Uyum Müdürlüğü koordinasyonunda CK Uyum Müdürlüğü yönetici ve personellerinin daimi üyesi olduğu, Şirket ilgili birimlerinden yönetici ve ilgili mevzuata uyum süreçlerinin Şirket özelinde takibi ve uyumu ile koordinasyon amacıyla çalışan ve belirli periyotlarda toplanan komitedir.
s) **Kurum Arşiv ve İmha Komisyonu:** Kurum arşivlerinde yapılacak imha işlemlerinin yürütülmesinden sorumlu olmak üzere; Şirket Genel Koordinatörü, Avukatı, İnsan Kaynakları ve Endüstriyel İlişkiler Direktörlüğü, Arşiv Sorumlusu, imha başvurusu yapan departmanın üst yöneticisi ve imha başvurusu yapan departmanın bilgi ve tecrübe sahibi temsilcisinden oluşan komisyondur.
t) **Özel Nitelikli Kişisel Veri:** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
u) **Periyodik İmha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
v) **Veri İşleyen:** Veri Sorumlusu'nun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
w) **Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
x) **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

y) **Veri Sorumluları Sicil Bilgi Sistemi/VERBİS:** Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
z) **Yönetmelik:** 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

5. UYGULAMA

Şirket tarafından, çalışanlar, ürün ve hizmet sağladığı ve/veya tedarik ettiği gerçek kişiler ve tüzel kişilerin gerçek kişi temsilcileri, ziyaretçiler ve hizmet sağlayıcıları olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Şirket tarafından, kişisel veriler Kanun'un 5. Ve 6. Maddesindeki işleme şartlarına uygun olarak ve Şirket'in kişisel veri envanterinde kayıt edildiği şekilde işlenir ve işleme şartlarının tamamının ortadan kalkması halinde silinmesi, yok edilmesi veya anonim hale getirilmesi suretiyle imha edilir.

5.1. Kişisel Verilerin İşlenmesi

Şirket, kişisel verileri işleme faaliyetini Kanun'un 5. Ve 6. Maddesindeki işleme şartlarına uygun olarak Kişisel Veri Envanteri çerçevesinde, iş süreçlerine bağlı olarak kişisel veri işleme amaçlarını, kullandığı veri kategorilerini, verileri aktardığı alıcı grubunu, kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri gözeterek gerçekleştirmektedir.

5.2. Kişisel Veri Saklama Süre Matrisi

Şirket, Kişisel Veri Saklama Süre Matrisi ("Matris") içerisinde, iş süreçlerine bağlı olarak işlemekte olduğu kişisel verilerin yasal gereksinimler ve iş amaçları doğrultusunda ne kadar süre ile saklanması gerektiğini ilişkilendirmiş ve detaylandırmıştır.
Şirket, Matriste yer alan kişisel verilerin işlendikleri amaç için gerekli olan azami süreleri Veri Sorumluları Sicili Hakkında Yönetmelik ve Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkındaki Yönetmelik uyarınca aşağıda belirtilen kriterleri dikkate alarak belirler:
a) İlgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
b) İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
c) İlgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
ç) İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
d) Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
e) Şirket'in hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
f) Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi.
Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,

- 6098 sayılı Türk Borçlar Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 4857 sayılı İş Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Elektrik Piyasası Tüketici Hizmetleri Yönetmeliği
- 6446 sayılı Elektrik Piyasası Kanunu ve
- Şirket'in faaliyet alanı gereği tabii olduğu diğer mevzuat, ikincil mevzuat ve her türlü idari düzenleme uyarınca öngörülen saklama süreleri boyunca kişisel veriler saklanmakta ve işlenmektedir.

Şirket, kişisel verilerin işlendikleri ve saklandıkları amaç için gerekli olan azami süreleri belirlerken ve uygularken, söz konusu sürelerin Envanterde yer alan bilgilerle uyumunu ve azami sürelerin aşılıp aşılmadığını takip eder. Aşağıdaki hallerin mevcut olması durumunda, azami sürelere bakılmaksızın kişisel verilerin işlenme şartlarının ortadan kalktığı kabul edilerek; ilgili kişinin başvurusu üzerine veya Şirket tarafından ilk periyodik imha kontrolü sırasında söz konusu kişisel veriler silinir, yok edilir veya anonim hale getirilir:

İmhayı Gerektiren Sebepler:

a) Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
b) Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
c) Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
d) Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,
e) İlgili kişinin, Kanunun 11 inci maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
f) Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
g) Kanunun 5. ve 6. maddelerindeki kişisel verilerin ve özel nitelikli kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.

5.3. Saklama Ve İmha Süreleri

Şirket'in süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamında işlediği tüm kişisel verilerin ilgili kişisel veri bazında saklama süreleri Envanterde, veri kategorileri bazında saklama süreleri ise VERBİS'e kayıtta, süreç bazında saklama süreleri ise işbu prosedürün 5.8. maddesinde yer alan Tablo 2'de belirtilir. Saklama süreleri sona eren ve/veya yukarıda "İmhayı Gerektiren Sebepler" başlığı altında belirtilen sebeplerle imhası gereken kişisel veriler, yine

Tablo-2'de yer alan imha süreleri çerçevesinde prosedürde belirlenen periyotlarla Şirket Arşiv ve İmha Komisyonunca imha edilir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler kayıt altına alınır ve ilgili kayıtlar, diğer yükümlülükler hariç olmak üzere en az üç yıl süre ile ilgili birim tarafından saklanır.

5.4. Kişisel Verilerin Güvenli Saklanmasına Ve İmhasına İlişkin Alınan Önlemler

Şirket, kişisel verilere yetkisiz erişimin önlenmesi, kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmemesi, hukuka uygun olarak imha edilmesi için gereken teknik ve idari tedbirleri almakla yükümlü olmakla birlikte bu tedbirleri ilgili kişilere duyurmak ve uygulanmasını sağlamakla yükümlüdür.

5.4.1. Alınan Teknik / İdari Tedbirler ve Veri Güvenliğinin Takibinin Sağlanması

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki ve yetki kontrol matrisi oluşturulmuştur. Çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmakta ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmaktadır.Erişim logları düzenli olarak tutulmaktadır.
- İşletim sistemi, ağ cihazı ve güvenlik sistemlerine ait tüm loglar SIEM ile entegre edilerek syslog/WMI/ajan tabanlı yöntemlerle toplanmaktadır. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu gerekliliklerine uygun şekilde zaman damgalı, değiştirilemez formatta en az 2 yıl saklanmakta olup, korelasyon senaryoları ve raporlamalar ile 7/24 izlenip incelenmektedir. Ayrıca Müşteri Bilgi Sistemleri seviyesinde Okuma/Ekleme/Güncelleme ve Silme işlemlerine ait tüm log kayıtları mevcut uygulama üzerinde toplanmakta ve tutulmaktadır.
- Kişisel verilerin yetkisiz şekilde dışarıya aktarılmasını önlemek amacıyla, elektronik posta, çıkarılabilir medya ve bulut tabanlı hizmetler gibi kanallar üzerinden veri hareketleri Data Loss Prevention (DLP) çözümü ile izlenmekte, politika ihlali teşkil eden işlemler engellenmekte ve kayıt altına alınmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar/prosedürler/taahhütler vb. hazırlanmış ve uygulamaya başlanmıştır.
- Şirketimiz bilişim ve bilgi işlem sistemlerinin işletimi (kurulum, konfigürasyon, ağa dahil etme, yönetim) sırasında uyulması gereken güvenlik kurallarını içerir Ağ ve Sistemlerin Güvenli İşletimi Prosedürü uygulanmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

- Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden anti-virüs, antispam sistemleri kullanılmaktadır. Bu sisteler güncel tutularak gereken dosyaları düzenli olarak taranmaktadır. Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri ve gizlilik taahhütleri içermektedir.
- Veri işleyenler ile imzalanan sözleşmeler yazılı olup, veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ve veri sorumlusunun denetim yetkisine ilişkin hükümler içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri envanterleri güncel tutulmakta olup, kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde resmi bir şekilde Bilgi Güvenliği Denetim Prosedürü uyarınca üst yönetime ve gerekli mercilere raporlanmaktadır. Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmakta ve güvenli bir şekilde saklanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Kullanıcı işlem kayıtları (Log kayıtları vb.) kullanıcı müdahalesi olmayacak şekilde düzenli olarak tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve söz konusu işlemler Bilgi Teknolojileri Grup Direktörlüğü'nce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.
- Aylık olarak mailler ve 3 günlük periyotlar ile Microsoft Teams görüşmeleri silinmektedir.

- Şirketimiz bünyesindeki endüstriyel kontrol sistemleri ve bilgi işlem sistemlerinin tümünü kapsayacak şekilde haftalık/aylık/gerektiğinde habersiz bilgi güvenliği denetimi faaliyetleri gerçekleştirilmektedir.

5.5. Periyodik İmha Süresi

Yönetmeliğin 11. maddesine uyumlu olarak Şirket, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha döneminde kişisel verileri imha eder. Periyodik imha süresi 6 ay olarak belirlemiştir. Buna göre, Şirket tarafından her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir. 5.3. başlığında bahsi geçen mailler hariç olmak üzere tüm maillerin aylık olarak ve Teams konuşmalarının 3 günlük periyotlar halinde silinmesine karar verilmiştir.

5.6. Kişisel Veri İmha Teknikleri

Şirket tarafından saklanan kişisel veriler, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sona ermesi veya İmhayı Gerektiren Sebepler maddesinde belirtilen hallerin mevcut olması durumunda, ilgili kişinin başvurusu üzerine veya Şirket tarafından belirlenen ilk periyodik imha kontrolü sırasında mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle silinir, yok edilir veya anonim hale getirilir.

5.6.1. Kişisel Verilerin Silinmesi

Sunucularda Yer Alan Kişisel Veriler : Kişisel Veriler Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler : Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler : Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler : Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

5.6.2. Kişisel Verilerin Yok Edilmesi

Fiziksel Ortamda Yer Alan Kişisel Veriler: Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler: Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

5.6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

5.7. Kayıt Ortamları

Kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
• Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) • Yazılımlar (ofis yazılımları, portal, DYS, EBYS, VERBİS.) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Yazıcı, tarayıcı, fotokopi makinesi	• Kağıt • Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) • Yazılı, basılı, görsel ortamlar

5.8. Denetim ve İhlal Hali

Kişisel Veri Saklama ve İmha Dokümanı' nın, Şirket çalışanları tarafından uyumunun denetiminden CK Enerji Uyum Müdürlüğü sorumlu olup, talimat ihlalinin tespiti halinde buna ilişkin ihlalde bulunan çalışanların disiplin ve insan kaynakları süreçleri için CK Enerji İç Denetim Direktörlüğü ve CK Enerji İnsan Kaynakları ve Endüstriyel İlişkiler Grup Direktörlüğü ile koordineli olarak çalışma yürütülecek olup, idari ve İş Kanunu'ndan doğan hak ve yükümlülükler, Genel Müdür'ün nihai kararıyla uygulanacaktır.

Tablo 1: Personel Unvan, Birim ve Görev Listesi

UNVAN	BİRİM	GÖREV
BT Uygulamaları Direktörü	Portföy Yönetim Grup Direktörlüğü	Bilgi sistemlerinden sorumlu birimler süreç bazında işlenmekte olan kişisel verilerin elektronik ortamlarda saklanması halinde saklama ve imha yükümlülüğü konusunda ilgili iş birimlerine teknik desteği sağlamakla yükümlüdür.

Kıdemli Uyum Müdürü	Uyum Müdürlüğü	Kişisel verilerin işlenmesi, saklanması ve imha edilmesine yönelik gerekli önlemlerin alınması sürecini koordine etmekle ve bu süreci denetlemekle yükümlüdür. Kanun ve ilgili mevzuat çerçevesinde Şirket'nin mevcut yükümlülüklerini takip etmek ve bu yükümlülüklerin yerine getirilmesi sürecini sorumlu birimlerle iş birliği içinde çalışmak suretiyle yürütmekle yükümlüdür. Aynı zamanda Dokümanda yapılan bütün revizyon ve değişiklikleri incelemek, onaylamak ve Doküman'ın yorumlanması konusunda çalışanlara yol göstermekle yükümlüdür.
Diğer Tüm Birimler	Diğer Birimler	Kendi yürüttükleri iş süreçlerinde kişisel verileri Kanuna ve Doküman'a uyumlu şekilde işlemek ile bu verilerin saklanması ve imha edilmesi için gerekli tedbirleri almakla ve veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere destek olmakla yükümlüdür.
KVKK Komite Üyesi	KVKK Komitesi	CK Uyum Müdürlüğü koordinasyonunda, kişisel verilerin işlenmesi, saklanması ve imha edilmesine yönelik KVKK Komitesinde alınan kararlar çerçevesinde gerekli önlemlerin alınması sürecini Şirketin ilgili birimleri ile koordine etmekle ve bu süreci denetlemekle yükümlüdür. CK Uyum Müdürlüğü tarafından Doküman'da yapılan bütün revizyon ve değişiklikleri incelemek, görüş bildirmek onaylamak ve Doküman'ın uygulanması ve yorumlanması konusunda çalışanlara yol göstermekle yükümlüdür.

Tablo 2: VERBİS Kaydı Baz Alınarak Hazırlanan Saklama Ve İmha Süreler

VERİ TÜRÜ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kimlik	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

İletişim	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Lokasyon	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Özlük	Sözleşme ilişkisi sona erdikten sonra 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlem	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri İşlem	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekan Güvenliği	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem Güvenliği	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Risk Yönetimi	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mesleki Deneyim	Sözleşme ilişkisi sona erdikten sonra 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Pazarlama	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Görsel ve İşitsel Kayıtlar	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık	Sözleşme İlişkisi Sona Erdikten Sonra 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	Lisans bitim tarihi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Diğer Bilgiler-Araç Bilgisi	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

6. RAPORLAMA

-

7. REFERANSLAR/İLGİLİ DOKÜMANLAR

Anayasa	**:**	Türkiye Cumhuriyeti Anayasası
Kanun	**:**	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Yönetmelik	**:**	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
Rehber	**:**	Kişisel Veri Güvenliği Rehberi- Teknik ve İdari Tedbirler

8. KAYIT

Bu Doküman gereği oluşturulan kayıtlar **UYM.PR.02_Kişisel Veri Saklama ve İmha Prosedürü ’ne** göre saklanır ve muhafaza edilir.

9. YÜRÜRLÜK

Bu doküman dağıtımının yapıldığı tarihten itibaren yürürlüğe girer.