TURCAS KUYUCAK JEOTERMAL ELEKTRİK ÜRETİM ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

TURCAS KUYUCAK JEOTERMAL ELEKTRİK ÜRETİM ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Doküman İsmi
Turcas Kuyucak Jeotermal Elektrik Üretim Anonim Şirketi Kişisel Veri Saklama ve İmha Politikası

Versiyon:
[0].[1]

Onaylayan:
Turcas Kuyucak Jeotermal Elektrik Üretim A.Ş. Üst Yönetimi tarafından onaylanmıştır.

Güncelleme Tarihi:
01/01/2021

İÇİNDEKİLER

1. BÖLÜM 1- GİRİŞ

İşbu Kişisel Veri Saklama ve İmha Politikası ("**İmha Politikası**"), Turcas Kuyucak Jeotermal Elektrik Üretim Anonim Şirketi ("**TKJ**" veya "**Şirket**") tarafından Kişisel Verilerin Korunması Kanunu'nun ("**Kanun**") 7. maddesi ile Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") uyarınca hazırlanmıştır.

İmha Politikasının amacı, işlenmesini gerektiren sebeplerin ortadan kalkması halinde, (i) kişisel verilerin muhafazası ve silinmesi amacıyla Kanun ve Yönetmelik'e uygun sürelerin belirlenmesi, (ii) çalışan ve bağımsız yüklenicilere, kişisel verilerin hangi süre ve koşullarda saklanacağına ilişkin bilgi sağlanması, (iii) tutulması gerekli kişisel verilerin Kanun ve Yönetmelik'e uygun olarak saklanmasını sağlanması, ve (iv) tutulan kayıt ortamlarının belirlenmesi suretiyle saklanan kişisel verilere hızlı, kolay ve etkili erişimin sağlanmasıdır.

2. BÖLÜM 2- ROLLER VE SORUMLULUKLAR

İşbu İmha Politikası'nın Şirket'in tüm işleyiş, faaliyet ve süreçlerinde uygulanmasından, Şirket Bilgi Teknolojileri Bölümü sorumlu olmakla birlikte; İmha Politikası'na uygun olarak hazırlanan prosedür, kılavuz, standart ve eğitim faaliyetlerinin Şirket bünyesinde uygulanmasında, Şirket'in Hukuk Direktörlüğü ve İnsan Kaynakları Müdürlüğü de görev alacaktır. Şirket genelindeki tüm çalışanlar, paydaşlar ve ilgili üçüncü kişiler, İmha Politikası'na uyum ile birlikte, hukuki yönden risklerin ve yakın tehlikenin önlenmesinde, Şirket'in Bilgi Teknolojileri Bölümü ile iş birliği yapmalıdırlar. Şirket'in tüm organ ve departmanları İmha Politikası'na uyulmasını gözetmekle yükümlüdür.

3. BÖLÜM 3- POLİTİKANIN ESASLARI

Kanun'un 7. maddesi uyarınca, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

İşbu İmha Politikası'nın hazırlanmış olması; kişisel verilerin Kanuna ve Yönetmelik'e uygun biçimde saklandığı, silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmez. Şirket, İmha Politikası'na uyum "Roller ve Sorumluluklar" bölümüne uygun olarak gözetmelidir.

3.1. KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASININ HAZIRLANMA AMACI

İmha Politikası, Şirket'in, Kanun'un 7. maddesi hükmü ile Yönetmelik uyarınca, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin ilgili kişinin talebi üzerine Veri Sorumlusu sıfatıyla Şirket tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğünün yerine getirilmesini sağlamak amacıyla, Şirket tarafından tutulan kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemlerinin dayanağını açıklamaktadır.

3.2. KAYIT ORTAMLARI

TKJ, aşağıda detayları açıklanan kayıt ortamlarında veri işleme faaliyetlerini sürdürmektedir:

- **Fiziksel Kayıtlar**: Kâğıt dokümanlar veya hidrokarbon örnekler gibi fiziksel kayıtlar. Söz konusu kayıtlar, fiziksel eşya ve fiziksel eşyaları tanımlayan metaveriyi içermektedir.

- **Elektronik Kayıtlar**: E-posta ve elektronik çizelge gibi elektronik dokümanlar. Kayıt, elektronik doküman ve elektronik dokümanı tanımlayan metaveriyi içermektedir. Hem doküman hem dokümanı tanımlayan metaveri Exchange Server, File Server ve LOGO Uygulaması içerisinde saklanmaktadır.

- **Uygulama Kayıtları**: Müşteri verileri gibi elektronik yapısal veri kayıtları. Yapı, düzen ve kayıtta tutulan veri unsurlarının toplulaştırılmış olarak sunumunu tanımlayan metaveriyi (tüm kayıt unsurları okunabilir duruma getirildiğinde) de içeren ve kaydın bütünlüğünü sağlayacak şekilde tüm veri unsurlarından oluşturmaktadır. Her bir tür kayıt için metaveri; bibliyografik, yönetimsel, denetim ve erişim verilerini içermektedir.

3.3. KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASINDA YER VERİLEN HUKUKİ VE TEKNİK TERİMLERİN TANIMLARI

"EK-1 Tanımlar" bölümünde İmha Politikası'nda yer verilen hukuki ve teknik terimlerin tanımları bulunmaktadır.

3.4. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK YA DA DİĞER SEBEPLERE İLİŞKİN AÇIKLAMA

3.4.1. Kişisel Verilerin Saklanmasını Gerektiren Sebepler

Kişisel verilerin saklanmasını gerektiren sebepler, Kişisel Veri İşleme Envanteri'nde yer almaktadır.

3.4.2. Kişisel Verilerin İmhasını Gerektiren Sebepler

Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması durumunda (örneğin, kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması halinde) kişisel veriler resen Şirketimiz tarafından imha edilmektedir.

Bunun yanı sıra, veri işleme faaliyetinin kişisel veri işleme şartlarından yalnızca veri sahibinin açık rızasına bağlı olarak yürütüldüğü durumlarda, veri sahibinin açık rızasını geri alması halinde veya ilgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesini talep etmesi ve talebinin yerinde olması durumunda veya veri sahibinin yapmış olduğu başvurunun Şirketimiz tarafından reddedilmesi, Şirketimizin verdiği cevabın veri sahibi tarafından yetersiz bulunması veya Kanun'da öngörülen süre içinde kendisine cevap verilmemiş olduğu hallerde; Kurul'a şikâyette

bulunması ve bu talebin Kurul tarafından uygun bulunması durumunda Şirketimiz tarafından imha edilmektedir.

3.5. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Teknik Tedbirler
- **Veri kaybı/sızıntısı önleme (DLP): Kişisel verilerin, yanlışlıkla ya da kötü niyetli kişilerce kurum dışına çıkarılmasına engel olan ya da engel olmadan işlemi raporlamaya yarayan güvenlik yazılımı kullanılmaktadır** - **Güvenli giriş katmanı (SSL): Sunucu ile istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikalar kullanılmaktadır** - **Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılmakta ve tüm yapının güncel olması sağlanmaktadır.** - **Şifre Yönetimi** - **Yazılım envanteri takibi ve gerekli güncellemelerin yapılması,** - **Sistem seviyesinde LOG tutulması** - **Yılda bir kez detaylı bir şekilde sızma ve güvenlik kontrolü çalışmaları yapılmaktadır. Tespit edilen açıklar risk ve öncelik durumuna göre giderilmektedir.** - **Disk Şifreleme Yazılımları Kullanılmaktadır.** - **Mobile Device Management Yazılımları kullanılarak Mobil cihazlardaki veri güvenliği sağlanmaktadır.**
İdari Tedbirler
- **Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.** - **Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.** - **Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.** - **Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.** - **Kişisel veri işleme envanteri hazırlanmıştır.** - **Şirket içi periyodik denetimler yapılmaktadır.** - **Her sene bir defa olmak üzere Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.**

3.6. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN UYGULANAN YÖNTEMLER VE ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin imha edilmesi, Şirket tarafından silme, yok etme veya anonim hale getirme yöntemlerinden biri seçilerek gerçekleştirilmektedir.

3.6.1. Kişisel Verilerin Silinmesi Yöntemleri

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır. Bu kapsamda TKJ, kişisel verilerin güvenli bir şekilde silinmesini sağlamak için aşağıdaki yöntemleri uygulamaktadır:

a. Hizmet olarak Uygulama Türü Bulut Çözümleri (Office 365, Salesforce, Dropbox)

SPK Mevzuatı gereği bulut yapılar kullanılmadığı için Bulut sistemler üzerinde uygulanan Bir çözüme ihtiyaç duyulmamıştır.

b. Merkezi Sunucuda Yer Alan Ofis Dosyaları

Merkezi sunucularda yer alan veri sınıflandırması matrisinde hassas veri olarak tanımlanan veriler belli periyotlar ile taranmakta ve veri sahiplerine raporlanmaktadır. Veri sahiplerinin KVKK yükümlülüklerine göre gerekli süreci tamamlaması talep edilmektedir.

c. Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile manuel olarak silinmesi veya anonim hal getirilmesi işlemi yapılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

3.6.2. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimiz, kişisel verilerin yok edilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır. Bu kapsamda TKJ, kişisel verilerin güvenli bir şekilde yok edilmesini sağlamak için aşağıdaki yöntemleri uygulamaktadır:

a. Yerel Sistemler

De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemleri kullanılmaktadır.

b. Çevresel Sistemler
   - Ağ cihazları (switch, router vb.)
   - Flash tabanlı ortamlar
   - Manyetik bant

- Manyetik disk gibi üniteler
- Mobil telefonlar
- Optik diskler
- Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri
- Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri
- Kâğıt ve mikrofiş ortamları
- Bulut ortamı

3.6.3. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

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, Şirketimiz, alıcı veya alıcı grupları tarafından geri döndürme ve 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 gerekmektedir. Şirketimiz, kişisel verilerin anonim hale getirilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır. Bu kapsamda TKJ, kişisel verilerin güvenli bir şekilde anonim hale getirilmesini sağlamak için aşağıdaki yöntemleri uygulamaktadır:

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri	• Değişkenleri çıkartma • Kayıtları çıkartma • Alt ve üst sınır kodlama • Bölgesel gizleme • Örnekleme
Değer düzensizliği sağlayan anonim hale getirme yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme • Tekrar Örnekleme
Anonim hale getirmeyi kuvvetlendirici istatistik yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

Gelen talebe göre söz konusu yöntemler teknik açıdan uygun olması durumuna göre manuel olarak uygulanmaya çalışılmaktadır.

3.7. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALAN GÖREVLİLERİN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

Unvan	**Birim**	**Görev Tanımı**

CEO, Direktörler ve Tüm Bölüm Yöneticileri	Şirketin Tüm Bölümleri/ Birimleri	Çalışanların politikaya uygun hareket etmesinden sorumludur.
İnsan Kaynakları Hukuk Bilgi Teknolojileri	KVKK Kurul'unda bulunan Tüm Bölüm/ Birimler	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi Teknolojileri Müdürü Kıdemli Sistem Destek Uzmanı Sistem Destek Uzmanı	Bilgi Teknolojileri	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Tüm Bölüm/Birim Yöneticileri, Çalışanlar	Tüm Bölüm/ Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

EK 1- TANIMLAR

İşbu Politika'da kullanılan terimler aşağıda yer alan anlamlara gelmektedir:

Açık rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Alıcı grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi;
Anonim hale getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi;
İlgili kişi	Kişisel verisi işlenen gerçek kişi;
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;
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi;
Kanun	24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu;
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;
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi;
Kişisel veri işleme envanteri	Şirketin iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırılmış olan envanter.
İmha politikası	Şirket tarafından kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılmış olan politika.
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 işlem.
Kurul	Kişisel Verileri Koruma Kurulu.
Kurum	Kişisel Verileri Koruma Kurumu.
Periyodik imha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden

	aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
Veri işleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi;
VERBİS	Veri Sorumluları Sicili
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi;
Veri sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

EK 2- SAKLAMA VE PERİYODİK İMHA SÜRELERİ

Kişisel Veri Kategorisi	**Azami Saklama Süresi**
Finansal Bilgi	Ticari defterlere son kaydın yapıldığı veya muhasebe belgelerinin oluştuğu takvim yılının bitişinden itibaren 10 yıl İş ilişkisinin bitiminden itibaren 10 yıl
İletişim Bilgisi	İş akdinin veya sözleşme ilişkisinin bitmesinden itibaren 10 yıl
Kimlik Bilgisi	İş ilişkisinin bitiminden itibaren 10 yıl
Eğitim Bilgisi / Performans ve Kariyer Gelişim Bilgisi - Mesleki Deneyim (VERBİS)	İş akdinin sona ermesinden itibaren 10 yıl
Hukuki İşlem ve Uyum Bilgisi	Sözleşme ilişkisinin bitmesinden itibaren 10 yıl Dava sürecinin tamamlanmasından itibaren 10 yıl
Müşteri Bilgisi / Talep Şikayet Bilgisi – Müşteri İşlem	Satışa dönüşmemesi durumunda kaydın yapılmasından itibaren 3 yıl Sipariş tarihinden itibaren 10 Yıl Talep ve şikayetin sonuçlandırılmasından itibaren 10 yıl Sözleşmenin süresinin sona ermesinden itibaren 10 yıl
Özlük Bilgisi	İş akdinin sona ermesinden itibaren 10 yıl
Görsel İşitsel Bilgi	Talep ve şikayetin sonuçlandırılmasından itibaren 10 yıl Dava sürecinin tamamlanmasından itibaren 10 yıl
Çalışan İşlem Bilgisi - İşlem Güvenliği Bilgisi (VERBİS)	İş akdinin sona ermesinden itibaren 10 yıl

	Dava sürecinin tamamlanmasından itibaren 10 yıl
Sağlık Bilgileri	İş akdinin sona ermesinden itibaren 10 yıl
Çalışan Adayı Bilgisi – İşe Alım ve Mülakat Dğerlendirme Bilgileri (VERBİS)	Başvurunun reddinden itibaren 2 yıl
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	İş akdinin sona ermesinden itibaren 10 yıl
Aile Bireyleri ve Yakın Bilgisi	İş akdinin sona ermesinden itibaren 10 yıl
Araç Bilgisi	2 yıl
Fiziksel Mekan Güvenliği Bilgisi	Dava sürecinin tamamlanmasından itibaren 10 yıl
Denetim ve Teftiş Bilgisi	2 yıl
Risk Yönetimi	6 ay

Kişisel verilerin saklandığı asgari ve azami sürelere ilişkin Kişisel Veri Envanteri'nde yer almaktadır.

Şirketimiz, kişisel verileri imha etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri imha etmektedir. Bu kapsamda Şirketimiz, kişisel verileri imha etme yükümlülüğünün ortaya çıkması halinde kişisel verileri 6 aylık periyotlar halinde imha işlemine tabi tutmaktadır. Anılan süre, her hal ve koşulda Yönetmelikte belirtilen azami periyodik imha süresini aşmamaktadır.