

İÇİNDEKİLER

1. AMAÇ	2
2. KAPSAM	2
3. HUKUKİ DAYANAK VE YÜKÜMLÜLÜK	2
4. TANIMLAR	2
5. SORUMLULUK VE GÖREV DAĞILIMI	4
6. KAYIT ORTAMLARI	5
6.1. Elektronik Kayıt Ortamları	5
6.2. Elektronik Olmayan Kayıt Ortamları	6
7. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER	6
7.1. Saklama ve İmhaya İlişkin Hukuki Sebepler	6
7.2. Saklamayı Gerektiren Amaçlar	6
7.3. İmhayı Gerektiren Sebepler	8
8. İDARİ VE TEKNİK TEDBİRLER	8
8.1. İdari Tedbirler	9
8.2. Teknik Tedbirler	9
9. SAKLAMA VE PERİYODİK İMHA SÜRELERİ	10
10. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ	12
10.1. Kişisel Verilerin Silinmesi	12
10.2. Kişisel Verilerin Yok Edilmesi	13
10.3. Kişisel Verilerin Anonim Hale Getirilmesi	14
11. POLİTİKANIN YÜRÜRLÜĞÜ	15

1. AMAÇ

Kişisel Verileri Saklama ve İmha Politikası, Eltem-tek Elektrik Tesisleri Mühendislik Müteahhitlik Danışmanlık ve Ticaret A.Ş.'nin ("Şirket") "Veri Sorumlusu" sıfatıyla elinde bulundurduğu kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

2. KAPSAM

Bu Politika, Şirket tarafından kişisel verileri işlenen tüm gerçek kişilere ilişkin kişisel verileri kapsar ve Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları hakkında ve tüm veri işleme faaliyetlerinde bu Politika uygulanır. İşbu Politika, Şirket'in faaliyetleri çerçevesinde düzenlenmiş, asılları ve kopyaları dahil tüm elektronik ve elektronik olmayan ortamlarda bulunan belgeleri kapsar.

3. HUKUKİ DAYANAK VE YÜKÜMLÜLÜK

Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve ilgili diğer mevzuat gereğince, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ("Yönetmelik") 5. ve 6. maddesine dayanarak ve Veri Sorumlusu Şirket'in kişisel veri işleme envanterine uygun olarak hazırlanmıştır.

Bu kapsamda, herhangi bir nedenle Şirket nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri, Kişisel Verilerin Korunması ve İşlenmesi Politikası ile işbu Kişisel Verileri Saklama ve İmha Politikası çerçevesinde kanunlara ve ilgili diğer mevzuata uygun olarak yönetilmektedir.

Şirket'in bütün çalışanları işbu Politika'yı tam olarak anlamak ve uygulamakla yükümlüdür. Politikanın uygulanmasından Şirket'in Üst Yönetimi, İrtibat Kişisi, Kişisel Verilerin Korunması Komitesi sorumludur.

4. TANIMLAR

Bu Politika kapsamında kullanılan terimler aşağıdaki anlamları ifade eder.

İlgili Kişi	<i>Kişisel verisi işlenen gerçek kişiyi ifade eder.</i>
Veri Sorumlusu	<i>Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder</i>
Kişisel Veri	<i>Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.</i>

Kişisel Verilerin İşlenmesi	<i>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 ifade eder</i>
Özel Nitelikli Kişisel Veri	<i>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 özel nitelikli kişisel veriyi ifade eder.</i>
Açık Rıza	<i>Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.</i>
Kişisel Veri İşleme Envanteri	<i>Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 envanteri ifade eder.</i>
Veri İşleyen	<i>Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.</i>
Kurum	<i>Kişisel Verileri Koruma Kurumu'nu</i>
Kanun	<i>6698 Sayılı Kişisel Verilerin Korunması Kanunu'nu</i>
Çalışan	<i>Eltemtek Elektrik Tesisleri Mühendislik Müteahhitlik Danışmanlık ve Ticaret A.Ş.'nin çalışanı</i>
Aktif Kayıtlar	<i>Şirket'in işleyişi, idaresi ve yönetimi için halen kullanılmakta olan kayıtlardır.</i>
Aktif Olmayan Kayıtlar	<i>Kullanılmayan; ancak işlenmesi sonradan gerekebileceği için saklama süreleri sona ermemiş kayıtlardır.</i>
Elektronik Ortam	<i>Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlardır.</i>
Elektronik Olmayan Ortam	<i>Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlardır.</i>
Fiziksel Yok Etme	<i>Optik veya manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesidir.</i>

İkincil Mevzuat	Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüşü ifade eder.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.
Karartma/Maskeleye	Kişisel verilerin bütünü, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması, buzlanması, yıldızlanması gibi işlemlerdir.
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 ortamdır.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda bu Politikada belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemidir.

Burada yer verilmeyen terimlerin; Kanun, Yönetmelik ve diğer ikincil mevzuatta yer alan anlamda kullanıldığı kabul edilir.

5. SORUMLULUK VE GÖREV DAĞILIMI

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımları aşağıdaki şekildedir:

ÜNVANI	BİRİMİ	GÖREVİ
Üst Yönetim	Yönetim	Çalışanların Politika'ya uygun hareket etmesinin sağlanmasından sorumludur.
Veri Sorumlusu İrtibat Kişisi	-	Şirket'in Kişisel Verilerin Korunması Kurumu nezdinde temsil edilmesinden sorumludur.
Kişisel Verileri Koruma Komitesi	Genel Müdür, İnsan Kaynakları Müdürlüğü, Bilişim Teknolojileri ve Teknik Hizmetler Direktörlüğü, Hukuk Müşavirliği, tüm birim amirleri	Politika'nın hazırlanması, yürütülmesi, yayınlanması, geliştirilmesi ve güncellenmesinden sorumludur.
İnsan Kaynakları Yetkilisi	İnsan Kaynakları Müdürlüğü	Görev alanı çerçevesinde Politika'nın uygulanmasından sorumludur.
Bilgi Sistemleri Yetkilisi	Bilişim Teknolojileri ve Teknik Hizmetler Direktörlüğü	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve gerekli yatırımların sağlanması için yönetimin bilgilendirilmesinden sorumludur.
Mali İşler Yetkilisi	Mali İşler Müdürlüğü	Görev alanı kapsamında edinmiş oldukları kişisel verileri kanuna uygun şekilde işlemekten ve görev alanı çerçevesinde Politika'nın uygulanmasından sorumludur.
Teklif ve Sözleşmeler Yetkilisi	Teklif ve Sözleşmeler Şefliği	Görev alanı kapsamında edinmiş oldukları kişisel verileri kanuna uygun şekilde işlemekten ve görev alanı çerçevesinde Politika'nın uygulanmasından sorumludur.
Diğer Birim Yetkilileri	-	Görev alanı kapsamında edinmiş oldukları kişisel verileri kanuna uygun şekilde işlemekten ve görev alanı çerçevesinde Politika'nın uygulanmasından sorumludur.

6. KAYIT ORTAMLARI

Şirket bünyesinde kişisel verilerin kayıt ortamları aşağıda belirtilmiştir:

6.1. Elektronik Kayıt Ortamları

Ses kayıtları, fotoğraflar, videolar, görsel ve işitsel ortamlar dahil birçok ortamda yer alan kişisel veriler; doğru, güncel ve kişisel verileri işlemesi gereken kişilerce erişilebilir olacak

şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli elektronik ortamlarda saklanabilir.

Elektronik ortamlar; sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.), yazılımlar (ofis yazılımları, portal vb.), bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit, engelleme, günlük kayıt dosyası, anti virüs vb.), kişisel bilgisayarlar (masaüstü, dizüstü), mobil cihazlar (telefon, tablet vb.), optik diskler (CD, DVD vb.), çıkartılabilir bellekler (USB, hafıza kartı vb.) ve yazıcı, tarayıcı, fotokopi makinesi vb. diğer elektronik veri kayıt ortamlarıdır.

6.2. Elektronik Olmayan Kayıt Ortamları

- Yazılı, basılı ortamlar ve manuel veri kayıt sistemleri gibi elektronik olmayan kayıt ortamları, fiziksel kayıtlar, kâğıt üzerindeki kayıtlar, fotoğraflar ve sözleşmeler gibi kâğıt, kâğıt fatura ve benzeri ortamlarda bulunan kayıtlardan oluşur.
- Aktif kayıtlar ve kolayca erişilmesi gereken kayıtlar Şirket'in ofis ortamında depolanabilir.
- Aktif olmayan kayıtlar Şirket'in arşivlerine gönderilir.

7. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

7.1. Saklama ve İmhaya İlişkin Hukuki Sebepler

Şirket kişisel verileri;

- 213 sayılı Vergi Usul Kanunu,
- 2004 sayılı İcra İflas Kanunu,
- 4857 sayılı İş Kanunu,
- 3308 Mesleki Eğitim Kanunu,
- 5237 sayılı Türk Ceza Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 4735 sayılı Kamu İhale Sözleşmeleri Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- Kamu İhale Genel Tebliği,
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile ilgili yönetmelikleri ve bunlarla

sınırlı olmamak üzere yayınlanan diğer mevzuat hükümleri gereğince işlemekte, saklamakta ve ilgili şartların gerçekleşmesi durumunda imha yöntemlerini kullanarak silmekte, yok etmekte veya anonim hale getirmektedir.

7.2. Saklamayı Gerektiren Amaçlar

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklamaktadır:

- *Acil durum yönetimi süreçlerinin yürütülmesi,*
- *Aile üyesi bilgilerinin edinilmesi,*
- *Bilgi güvenliği süreçlerinin yürütülmesi,*

- Bilgi teknolojileri alt yapısının oluşturulması ve yönetilmesi,
- Bireysel emeklilik işlemlerinin yürütülmesi,
- Çalışan memnuniyeti ve bağlılığının artırılmasına ilişkin süreçlerin planlanması ve yürütülmesi,
- Çalışan temin süreçlerinin yürütülmesi,
- Çalışan yan haklar ve menfaatleri süreçlerinin yürütülmesi,
- Çalışanlar için iş akdi ve mevzuat kaynaklı yükümlülüklerin yerine getirilmesi,
- Denetim ve etik faaliyetlerinin sürdürülmesi,
- Disiplin süreçlerinin yürütülmesi,
- Eğitim faaliyetlerinin yürütülmesi,
- Erişim yetkilerinin yürütülmesi,
- Faaliyetlerin mevzuata uygun yürütülmesi,
- Faturalandırma süreçlerinin yürütülmesi,
- Finans ve muhasebe işlemlerinin yürütülmesi,
- Fiziksel mekân güvenliğinin temini,
- Görevlendirme süreçlerinin yürütülmesi,
- Güvenlik hizmetlerinin verimli şekilde yürütülmesi,
- Güvenlik soruşturması ile arşiv araştırmasının yürütülmesi,
- Hukuk işlerinin takibi ve yürütülmesi,
- İç ve dış emniyeti sağlama faaliyetinin yürütülmesi,
- İç yazışma ve evrak takibi işlemlerinin yürütülmesi,
- İletişim faaliyetlerinin yürütülmesi,
- İnsan kaynakları süreçlerinin planlanması,
- İnsan kaynakları ve istihdam politikasının yürütülmesi,
- İş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,
- İş faaliyetlerinin yürütülmesi ve denetimi,
- İş sağlığı ve güvenliği süreçlerinin yürütülmesi,
- İş süreçlerinin iyileştirilmesine yönelik önerilerin alınması ve değerlendirilmesi,
- İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi,
- İşe giriş ve çıkış kayıtlarının oluşturulması,
- İşten çıkarma, işe alım, terfi faaliyetlerinin yürütülmesi,
- İzin faaliyetlerinin yürütülmesi,
- Kiralama faaliyetlerinin yürütülmesi,
- Mal ve hizmet alım/satım süreçlerinin yürütülmesi,
- Müşteri ilişkileri yönetimi süreçlerinin yürütülmesi,
- Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi,
- Ödeme faaliyetlerinin yürütülmesi,
- Organizasyon ve etkinlik yönetimi süreçlerinin yürütülmesi,
- Ortaklık ilişkilerinin ve bilgi akışının yürütülmesi,
- Özlük faaliyeti süreçlerinin yürütülmesi,
- Performans değerlendirme süreçlerinin yürütülmesi,
- Piyasa ödemeleri faaliyetlerinin yürütülmesi,
- Proje ve sözleşme süreçlerinin belirlenmesi,
- Projenin ana işverenine bilgi verilmesi,
- Risk yönetimi süreçlerinin yürütülmesi,
- Saklama ve arşiv faaliyetlerinin yürütülmesi,
- Sipariş ve talep süreçlerinin yürütülmesi,
- Şirketin kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Şirketin kurumsal yönetim faaliyetlerinin planlanması ve icrası,
- Şirketin tanıtım faaliyetlerinin planlanması ve icrası,
- Sözleşme süreçlerinin yürütülmesi,
- Sözleşme ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,

- *Stajyer temin süreçlerinin yürütülmesi,*
- *Stajyerler için mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,*
- *Stajyerler için yan haklar ve menfaatleri süreçlerinin yürütülmesi,*
- *Stajyerlerin performans değerlendirme süreçlerinin yürütülmesi,*
- *Talep ve şikayetlerin takibi,*
- *Tedarik işlemlerinin yürütülmesi,*
- *Teklif süreçlerinin yürütülmesi,*
- *Temsil ve yetki işlemlerinin yürütülmesi,*
- *Ücret politikasının yürütülmesi,*
- *Ürün ve hizmetlerin pazarlama süreçlerinin yürütülmesi,*
- *Veri sorumlusu operasyonlarının güvenliğinin temini,*
- *Yapılan sözleşmenin yetkili kurum ve kuruluşlara ibrazı,*
- *Yasal zorunlulukların yerine getirilmesi,*
- *Yazışma ve evrak takibi işlerinin yürütülmesi,*
- *Yetenek ve kariyer gelişimi faaliyetlerinin yürütülmesi,*
- *Yetkili kişi kurum ve kuruluşlara bilgi verilmesi,*
- *Yönetim faaliyetlerinin sürdürülmesi,*
- *Yönetim Kurulu üyelerine tanımlanan hakların kullanılabilmesi,*
- *Yönetim Kurulu üyeliği görev ve yetkilerinin yürütülmesi,*
- *Zimmet işlemlerinin yürütülmesi,*
- *Ziyaretçi kayıtlarının oluşturulması ve takibi.*

7.3. İmhayı Gerektiren Sebepler

Kişisel veriler aşağıda belirtilen hallerde Şirket tarafından re'sen veya ilgili kişinin talebi üzerine imha yöntemleri kullanılarak silinir, yok edilir veya anonim hale getirilir:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin ilgası veya işlenme gerekliliğini kaldırır şekilde değiştirilmesi,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin kişisel veri işlenme rızasının geri alması,
- Kanunun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilerek söz konusu kararın şirkete bildirilmesi/ ulaştırılması,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, Şirket tarafından ilgili kişiye verilen cevabın ilgili kişi tarafından yetersiz bulunması veya Şirket tarafından KVKK'de öngörülen süre içinde cevap verilmemesi hallerinde; ilgili kişi tarafından Kişisel Verileri Koruma Kurumu'na şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- *Kişisel verilerin işlenmesini veya saklanmasını öngören ilgili mevzuat hükümlerinin değiştirilmesi, mülgası veya ilgası.*

8. İDARİ VE TEKNİK TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi amacıyla; KVKK'nin "Veri Güvenliğine İlişkin Hükümler" başlıklı 12'nci maddesi ile KVKK'nin "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlıklı 6'ncı maddesinin dördüncü fıkrasında yer alan "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurum tarafından belirlenen yeterli önlemlerin alınması şarttır." hükmü

gereğince; veri sorumlusu sıfatı taşıyan Şirket'in, işlediği kişisel verilerin hukuka uygun olarak almış olduğu idari ve teknik tedbirler aşağıdaki gibidir.

8.1. İdari Tedbirler

Şirket, işlediği kişisel verilerin hukuka uygun olarak işlenmesi ve muhafazasının sağlanması ile kişisel verilere hukuka aykırı erişimin engellenmesi için aşağıdaki idari tedbirleri almaktadır:

- *Kişisel verilerin korunması ve işlenmesi ile kişisel verilerin saklanması ve imhası konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.*
- *Şirket çalışanının yürüttüğü iş ve işlemler sırasında kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri kazanmaları adına personelin tabi olduğu mevzuat ile ilgili diğer mevzuat hakkında eğitimler verilmektedir.*
- *Kişisel veri işleme envanteri hazırlanmıştır.*
- *Benimsenen "veri minimizasyonu" ilkesi kapsamında işlenen kişisel veriler yalnızca yetkili ve ilgili personelin erişimine açıktır.*
- *Kişisel veri içeren belge ve kayıtlar KVKK'de belirtilen usullere uygun şekilde muhafaza edilmektedir.*
- *Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.*
- *Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.*
- *Kişisel Veri Sahibi Başvuru Formu üzerinden Şirket'e yönlendirilen talep ve şikayetlerin kontrolü düzenli şekilde gerçekleştirilip; ilgili kişiye talebini yönelttiği tarihten başlayarak en geç 30 (otuz) gün içerisinde gerekçeli dönüş yapılmaktadır.*
- *Şirket herhangi bir veri ihlaliyle karşılaşması halinde durumun tespitinin ardından; veri güvenliği sorunları raporlanarak söz konusu ihlal durumu Kişisel Verileri Koruma Kurumu'nun resmi internet sitesinde yer alan Veri İhlal Formu' nu usulüne uygun şekilde doldurmaya özen gösterecektir.*
- *Kişisel Verileri Koruma Kurumu'nun aldığı kararlar takip edilerek, bu kararlara göre Şirket'in alması gereken önlemler belirlenmektedir.*
- *Çalışanın kullanımına bırakılmış tüm cihaz, portal, uygulama ve yazılımlarda çalışana özgü atanmış kullanıcı adı ve parola bulunmaktadır.*
- *Şirket, çalışanlarından işten ayrılımlarından sonra da geçerli olacak şekilde, görevleri gereği öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak bir başkasına açıklamayacakları ve işleme amacı dışında kullanmayacakları konusunda taahhüt almaktadır.*
- *Görev değişikliği veya personelin Şirket ile ilişkisinin kesilmesi halinde; kendisine tanımlanan erişim yetkisi derhal düzenlenmektedir.*
- *Şirket tarafından, Sözleşme ve diğer belgeler gereği olarak sözleşme yapılan taraf ile paylaşılmış olan kişisel veriler ile ilgili olarak sözleşmelerde bu verilerin gizliliğine, ne şekilde işleneceğine ve saklanacağına ilişkin veri güvenliği hükümleri konulmaktadır.*
- *Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.*
- *Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.*
- *Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.*

8.2. Teknik Tedbirler

Şirket, işlediği kişisel verilerin hukuka uygun olarak işlenmesi ve muhafazasının sağlanması ile kişisel verilere hukuka aykırı erişimin engellenmesi adına aşağıdaki teknik tedbirleri almaktadır:

- *Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.*
- *Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.*
- *Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri*

alınmaktadır.

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerekliğinde veri maskeleyme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- 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.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde 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 farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Şirket, kişisel verilere erişimi, veri işleme konusunda açıkça yetkilendirilmiş çalışanları ile sınırlandırmaktadır. Şirket çalışanlarının görevleri gereği kullanmadıkları kişisel verilere erişimleri sınırlandırılmaktadır.
- 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.

9. SAKLAMA VE PERİYODİK İMHA SÜRELERİ

Kişisel verinin saklanması ve imhasına ilişkin olarak KVKK veya yönetmeliklerde öngörülmüş olan sürelerle uyulmaktadır. Anılan sürenin sona ermesi halinde; saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Kişisel Verileri Koruma Komitesi tarafından yerine getirilir.

KVKK'de veya yönetmeliklerde söz konusu verinin saklanması ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda;

- KVKK'nin 6'ncı maddesine göre özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanması Veri Sorumlusu açısından önem derecesine göre belirlenir.
- Verinin saklanması KVKK'nin 4'üncü maddesinde belirtilen ilkelere uygunluğu sorgulanır. Saklanması KVKK'nin 4'üncü maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
- Verinin saklanması KVKK'nin 5 ve 6'ncı maddelerinde öngörülmüş olan istisnalardan hangileri kapsamında değerlendirilebileceği tespit edilir. Bu istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde ise silme, yok etme veya anonim hale getirme işlemleri uygulanır.

Kişisel verilerin saklanma ve imha süreleri aşağıda yer alan tabloda gösterilmiştir.

VERİ TÜRÜ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş / Staj Başvurusu Süreçlerinin Yürütülmesi	Başvurunun yapıldığı tarihten itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Verileri	Çalışanın işten ayrılmasından itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Özel Nitelikli Kişisel Veriler	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Stajyer Verileri	Stajın sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mal/Hizmet Satın Alınan Gerçek Kişi/Tüzel Kişi Çalışanları ve Yetkilileri Verileri	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mal/Hizmet Satın Alan Gerçek Kişi/Tüzel Kişi Çalışanları ve Yetkilileri Verileri	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarikçi Yetkilisi	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnternet Log Kayıtları ve Kullanım Verileri	Kayıt tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri İşlem Verileri	Siparişin veya talebin alınmasından itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Ziyaretçi Kayıtları	Veri türüne göre kayıt tarihinden itibaren kamera kayıtları için 20 gün (Ankara Ofis), 16 gün (Eskişehir Ofis) veya 20 gün (İstanbul Ofis) / diğer kişisel veriler için 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Lokasyon	Kayıt tarihinden itibaren 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket Hissedarları ve Ortakların Çalışanları ve Yetkilileri	Ticari ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yönetim Kurulu Üyelerine İlişkin Veriler	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Saklama süresi dolmuş kayıtlar Şirkette her yıl haziran ve aralık aylarında olmak üzere iki kez gerçekleştirilen periyodik imhaya tabi tutulur. Bir kişisel verinin işleme amacının ortadan kalktığı tarih bu iki dönemden hangisine daha yakınsa o dönemde imha edilir.

10. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

Şirket tarafından KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenen kişisel veriler, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak silinerek, yok edilerek veya anonim hale getirilerek imha edilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde;

- İlgili mevzuatta kişisel verilerin işlenmesinde uyulması gerekli görülen genel ilkelere,
- Veri sorumlularının veri güvenliğine ilişkin yükümlülükleri kapsamında alınması gereken idari ve teknik tedbirlere,
- Kişisel Verileri Koruma Kurumu kararlarına,
- Kişisel verilerin saklanması ve imhası politikasına uygun hareket edilmektedir.

10.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Silme işlemi için öncelikle silme işlemine konu teşkil edecek kişisel veriler belirlenmekte ve her bir kişisel veri için ilgili kullanıcılar tespit edilmektedir. Bunu takiben ilgili kullanıcıların erişim, geri getirme ve tekrar kullanma gibi yetkileri ve kullandıkları yöntemler tespit edilerek işbu yetkiler ortadan kaldırılmaktadır.

Verilerin silinmesi ile ilgili olarak aşağıdaki yöntemler kullanılır:

a) Kâğıt Ortamında Bulunan Kişisel Veriler

Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

b) Merkezi Sunucuda Yer Alan Kişisel Veriler

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması sağlanır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına da dikkat edilir.

c) Taşınabilir Medyada Bulunan Kişisel Veriler

Taşınabilir medyalarla taşınan veriler şifreli olarak saklanmakta ve bu araçlarda gizli seviyede hiçbir veri taşınmamaktadır. Taşınabilir ortamda olan kişisel veriler, söz konusu donanıma uygun yazılımlar ile silinir.

d) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

10.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel veriler, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilir.

a) Yerel Sistemler

Yerel sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntem kullanılır.

- **Fiziksel Yok Etme:** Optik veya manyetik medyayı bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

b) Çevresel Sistemler

Ortam türüne bağlı olarak kullanılan yok etme yöntemleri aşağıda yer almaktadır:

- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.

- **Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikromiknatıs parçaları yardımı ile saklayan ortamlardır. Fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.
- **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Küçük parçalara ayırma fiziksel yok etme gibi yöntemiyle yok edilmesi sağlanır.
- **Kâğıt Ortamlar:** Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi sağlanır. Bu işlem gerçekleştirilirken ortam kâğıt imha veya kırpma makineleri ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür. Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

Yukarıdakilere ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin Yukarıda 'Yerel Sistemler' için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmekte,
- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanmakta, arızalı diğer parçalar üretici, satıcı, servis gibi üçüncü kurumlara gönderilmektedir.

10.3. 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 alıcı grupları 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. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiyi işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Şirket, kişisel verilerin silinmesi veya yok edilmesi yerine anonim hale getirilmesi sürecinde gerekli her türlü teknik ve idari tedbirleri alır. Kişisel verilerin anonim hale getirilmesi, Yönetmelik'te belirtilen esaslara ve Kişisel Verilerin Korunması Kurumu'nun konuya ilişkin yayınladığı rehberdeki yöntemlere uygun olarak yapılır.

Şirket, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmek için aşağıdaki şartların yerine getirilmesini arar ve işbu şartların yerine getirilmiş olmasını sağlar:

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin

bozulmaması,

- Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

11. POLİTİKANIN YÜRÜRLÜĞÜ

Bu politika Şirketin internet sayfasında yayınlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur. Bu Politika, kurumsal ya da mevzuattan kaynaklanan içerik değişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilip gerektiğinde güncellenir.

İşbu Politika'da yapılan değişiklikler, derhal metne işlenir ve tekrar yayınlanarak yürürlüğe girer.