

CEYLAN-KARAVİL ALIŞVERİŞ MERKEZLERİ TURİZM VE TİCARET A.Ş.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

MADDE 1- AMAÇ

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), Ceylan-Karavil Alışveriş Merkezleri Turizm Ve Ticaret A.Ş. (“Şirket”) tarafından işlenen kişisel verilerin saklanması ve imhasına yönelik iş ve işlemler konusundaki usulleri ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket; şirket çalışanları, çalışan adayları, müşteriler, potansiyel müşteriler, ziyaretçiler, ortaklar, tedarikçiler, hizmet sağlayıcıları, iş birliği içinde olduğu kurumların/şirketlerin çalışanları, hissedarları ve yetkilileri ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

MADDE 2- KAPSAM

Şirket çalışanlarına, çalışan adaylarına, müşterilere, potansiyel müşterilere, ziyaretçilere, ortaklara, tedarikçilere, hizmet sağlayıcılara, iş birliği içinde olduğu kurumların/şirketlerin çalışanlarına, hissedarlarına ve yetkililerine ve diğer üçüncü kişilere ait, otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel veriler bu politika kapsamındadır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

MADDE 3- DAYANAK

Bu Politika 6698 sayılı Kişisel Verilerin Korunması Kanunu, Veri Sorumluları Sicili Hakkında Yönetmelik ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik dayanak alınarak hazırlanmıştır.

Kişisel verilerin saklanması ve imhası konusunda yürürlükte bulunan ilgili düzenlemeler öncelikle uygulama alanı bulacaktır. Mevzuat ile Politika arasında uyumsuzluk bulunması halinde ise öncelikle yürürlükteki mevzuat uygulama alanı bulacaktır.

MADDE 4- KISALTMALAR VE TANIMLAR

Alıcı Grubu	:Veri sorumlusu şirket tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi,
Açık Rıza	: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza,
Anonim Hale Getirme	: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi,
Çalışan	: Şirkete bağlı çalışan gerçek kişileri,
Çalışan Adayı	: Şirkete herhangi bir yolla iş başvurusunda bulunmuş ve Şirkete iş ilişkisi kurma isteğinde olan gerçek kişileri,

Diğer üçüncü kişiler	:Politika kapsamında açıkça ismi sayılmayan ancak kişiler verileri şirketçe işlenen gerçek kişileri,
Elektronik Ortam	: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar,
Elektronik Olmayan Ortam	: Elektronik ortamların dışında kalan tüm yazılı, basılı, görselvb. diğer ortamlar,
Hizmet Sağlayıcı	: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi,
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 ve KVKK	: 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 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,
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,

Kurul

: Kişisel Verileri Koruma Kurulu,

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,

Müşteri

: Şirketimizle herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirketimizin sunmuş olduğu ürün ve hizmetleri kullanan veya kullanmış olan gerçek kişiler,

Potansiyel Müşteri

: Ürün ve hizmetlerimize kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişiler,

Periyodik İmha

: Kanunda yer alan hallerde kişisel verilerin işleme 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,

Politika

: Kişisel Verileri Saklama ve İmha Politikası,

Şirket

: Ceylan-Karavil Alışveriş Merkezleri Turizm Ve Ticaret A.Ş.,

Şirket Hissedarı

: Şirketimizin hissedarı olan gerçek kişiler ya da tüzel kişi hissedarların gerçek kişi temsilcileri,

Şirket Yetkilisi

: Şirketimizce yetkilendirilen diğer gerçek kişiler,

İşbirliği İçinde

Olduğumuz Kurumların

Çalışanları, Hissedarları ve

Yetkilileri

: Şirketimizin her türlü iş ilişkisi içerisinde bulunduğu kurumlarda (iş ortağı, tedarikçi, grup şirketler, mağaza gibi, ancak bunlarla sınırlı olmaksızın) çalışan, bu kurumların hissedarları ve yetkilileri dahil olmak üzere gerçek kişiler,

Veri İşleyen

: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi,

Veri Kayıt Sistemi

: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi,

Veri Sorumlusu : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi,

Veri Sorumluları

Sicil Bilgi Sistemi : Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi,

VERBİS : Veri Sorumluları Sicil Bilgi Sistemi,

Yönetmelik : Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

Ziyaretçi : Şirketimizin sahip olduğu veya bir organizasyon gerçekleştirdiği fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler.

MADDE 5- SORUMLULUK VE GÖREVLER

Şirketin tüm çalışanları, çalışan adayları, ortakları, tedarikçileri, hizmet sağlayıcıları, iş birliği içinde olduğu kurumların/şirketlerin çalışanları, hissedarları ve yetkilileri ve birimleri; Politika kapsamında alınan teknik ve idari tedbirlerin gereği gibi alınmasından ve uygulanmasından sorumludur. Şirketin tüm çalışanları, çalışan adayları, ortakları, tedarikçileri, hizmet sağlayıcıları, iş birliği içinde olduğu kurumların/şirketlerin çalışanları, hissedarları ve yetkilileri; kişisel verilerin korunması için gerekli eğitim ve farkındalığının artırılması, izlenmesi ve sürekli denetim ile kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun olarak saklanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek vermek zorundadır.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait bilgi TABLO: 1’de gösterilmiştir.

TABLO: 1- Saklama ve imha süreçleri görev dağılımı

UNVANI	BİRİMİ	GÖREVİ
Avm Müdürü	Şirket Merkezi	Çalışanların politikaya uygun davranmasından ve periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
Reklam ve Pazarlama Müdürü	Reklam ve Pazarlama Müdürlüğü	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması, güncellenmesinden ve idari tedbirlerin alınmasından ve periyodik imha süresi

		uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
İşletme Müdürü	İşletme Müdürlüğü	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve teknik tedbirlerin alınmasından ve periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.
Muhasebe Birimi, Finans Birimi vb.	Diğer Tüm Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden ve periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminden sorumludur.

MADDE 6- KAYIT ORTAMLARI

Kişisel veriler, şirket tarafından TABLO: 2’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

TABLO: 2- Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<p>Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)</p> <p>Yazılımlar (ofis yazılımları, portal, VERBİS.)</p> <p>Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)</p> <p>Kişisel bilgisayarlar (Masaüstü, dizüstü)</p> <p>Mobil cihazlar (telefon, tablet vb.)</p> <p>Optik diskler (CD, DVD vb.)</p> <p>Çıkarılabilir ve Taşınabilir bellekler (USB, Hafıza Kart vb.)</p> <p>Yazıcılar, tarayıcılar, fotokopi makineleri</p>	<p>Kağıtlar</p> <p>Yazılı ve basılı ortamlar</p> <p>Görsel kayıtlar</p> <p>Manuel veri kayıt sistemleri (ziyaretçi giriş defteri vb.)</p> <p>Birim Dolapları (Kilitli ve sınırlı erişimli)</p> <p>Arşiv (Özel korumalı)</p>

MADDE 7- SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, müşteriler, potansiyel müşteriler, ziyaretçiler, ortaklar, tedarikçiler, hizmet sağlayıcıları, iş birliği içinde olduğu kurumların/şirketlerin çalışanları, hissedarları ve yetkilileri ve diğer üçüncü kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı

maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirketimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

MADDE 8- SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirket faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda açık rıza hali dışında kişisel verileri saklamayı gerektiren sebepler şunlardır:

- a- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- b- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- c- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla şirketin meşru menfaatleri için saklanması zorunlu olması,
- d- Kişisel verilerin şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- e- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- f- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

MADDE 9- SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Şirket aşağıda belirtilen hallerde, ilgili kişinin kişisel verilerini çeşitli amaçlarla işleyebilir:

- a. Şirketimiz tarafında yürütülen ticari faaliyetlerin gerçekleştirilmesi için ilgili iş birimlerimiz tarafından gerekli çalışmaların yapılması ve buna bağlı iş süreçlerinin yürütülmesi,
- b. Şirketimizin Ticari ve/veya iş stratejilerinin planlanması ve icrası,
- c. Şirketimiz tarafından sunulan ürün ve hizmetlerden ilgili kişileri faydalandırmak için gerekli çalışmaların iş birimlerimiz tarafından yapılması ve ilgili süreçlerin yürütülmesi,
- d. Şirketimizin insan kaynakları politikaları ve süreçlerinin planlanması ve icra edilmesi,
- e. Şirketimizin ve Şirketimizle iş ilişkisi içerisinde olan ilgili kişilerin hukuki, teknik ve ticari iş güvenliğinin temini.

MADDE 10- İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re'sen Şirket tarafından silinir, yok edilir veya anonim hale getirilir:

- a- Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması,
- b- Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- c- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- d- Kanununun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu şirketveya şikayet üzerine Kurultarafından kabul edilmesi,

- e- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

MADDE 11- TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirket tarafından teknik ve idari tedbirler alınır.

MADDE 12- TEKNİK TEDBİRLER

Şirket tarafından işlenen kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- a- Sızma (Penetrasyon) testleri ile şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- b- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- c- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- d- Şirketin bilişim sistemleri, teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- e- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- f- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- g- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- h- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- i- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- j- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- k- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- l- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- m- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- n- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

- o- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- p- Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrlenmektedir.
- q- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- r- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- s- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması işlemleri yapılmaktadır.
- t- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- u- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrlenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

MADDE 13- İDARİ TEDBİRLER

Şirket tarafından işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- a- Saklanan kişisel verilere, şirket içi erişim iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- b- Kişisel verilerin paylaşılması ile ilgili olarak, şirket çalışanları ve kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin gizlilik sözleşmeleri imzalanır yahut mevcut sözleşmelere eklenen hükümlerle veri güvenliği sağlanır. Şirket güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin işlemleri uygulanmaktadır.
- c- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam edilir ve personele kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimler verilir.
- d- Şirket, kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri;periyodik ve rastgele denetimler şeklinde yapmakta ve ortaya çıkan gizlilik ve güvenlik zafiyetlerini hemen gidermektedir.
- e- Kişisel veri işlemeye başlamadan önce şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmekte ve kişisel veri işleme envanteri düzenlenmektedir.

- f- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede ilgisine ve en geç 72 saat içinde Kurul'a bildirilir.
- g- Şirketimizle ilişkileri kesilen çalışanlar ve diğer ilgililer için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişim tamamen sınırlandırılmaktadır.

MADDE 14- KİŞİSEL VERİLERİN İMHASI

Şirket, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel verileri, re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha eder.

MADDE 15- KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

Kişisel veriler TABLO: 3'te belirtilen yöntemlerle silinir.

TABLO: 3 - Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak ve silme komutu ile 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 silme komutu ile 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 uygulanır.
Taşınabilir Medyada Yer Alan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve bu ortamlara uygun yazılımlar kullanılarak ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

MADDE 16- KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel veriler TABLO: 4'te belirtilen yöntemlerle yok edilir.

TABLO: 4 - Kişisel Verilerin Yok Edilmesi Yöntemleri

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha 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, üzerine yazılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, De-manyetize Etme yönetimiyle manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

MADDE 17- KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Şirket; kişisel verileri, 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 getirebilmektedir.

MADDE 18- SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bunun haricinde; TABLO: 5'te yer alan saklama ve imha süresi tablosu esas alınır.

TABLO: 5 - Saklama ve İmha Süresi Tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Üçüncü kişilerle imzalanan sözleşmeler (Kira sözleşmeleri, Hizmet Sözleşmeleri vb.)	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlar İçin İş Akdi ve Mevzuat Kaynaklı Yükümlülüklerin Yerine Getirilmesi	İş ilişkisinin veya varsa dava sürecinin bitimini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi	İş ilişkisinin veya varsa dava sürecinin bitimini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan adayları başvuru formları, özgeçmişleri vb.	Başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Güvenlik amaçlı işlenen Kamera kayıtları	İlk kaydın yapıldığı tarihten itibaren 30 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği uygulamaları kapsamında	İş ilişkisinin bitimini takiben 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik

elde edilen kişisel veriler		imha süresinde
Ziyaretçi, Müşteri ve Etkinlik Katılımcılarının Kaydı	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Satış, satın alma, pazarlama aktiviteleri ve talep/ şikayet yönetimi sırasında elde edilen veriler (satış, pazarlama ve işlem verileri vb.)	İlk kaydın yapıldığı tarihten veya hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe, Finansal / Ödeme işlemlerine ait kayıtlar	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Durum tespit raporu, olay tutanağı gibi güvenliğe ilişkin tutanak ve raporlar	İlk kaydın yapıldığı tarihten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ticari Elektronik Posta Kayıtları ve Şirket İçi Yazışmalar	İlk kaydın yapıldığı tarihten itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi (Web sitesi girişleri, Log kayıtları vb.)	İlk kaydın yapıldığı tarihten itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Operasyon yönetimi için formlar aracılığı ile işlenen veriler (giriş kartı formu, gece iş takip formu, araç çizelgesi vb.)	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
KVKK aydınlatma bildirimi, rıza beyanı ve diğer onay alma evrakları	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

MADDE 19- PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre Şirket her yıl Nisan ve Ekim aylarında periyodik imha işlemi gerçekleştirir.

MADDE 20- POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

İşbu Politika'da yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar Politika'nın sonunda açıklanır.

MADDE 21- YÜRÜRLÜK

Politika, Şirket Yönetim Kurulunun onayına müteakiben yürürlüğe girer ve şirketin internet sitesinde yayınlanır. Yürürlükten kaldırılmasına karar verilmesi halinde, Politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile şirket tarafından saklanır.

Değişiklikler:

30.11.2020 : Kişisel Verileri Saklama Ve İmha Politikası onaylanıp yayınlanmıştır.