

ÇOKYAŞAR HOLDİNG ANONİM ŞİRKETİ

KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI

İÇİNDEKİLER

I. GİRİŞ	
i) Amaç	3
ii) Kapsam	3
iii) Kısaltmalar ve Tanımlar	3 - 4
II. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINA İLİŞKİN GENEL İLKELER	5
III. KAYIT ORTAMLARI	5
i) Elektronik ortamlar	5
ii) Elektronik olmayan (fiziki) ortamlar	5 - 6
IV. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR	6
V. TEKNİK VE İDARİ TEDBİRLER	7
i) Teknik Tedbirler	7 - 8
ii) İdari Tedbirler	8 - 9
VI. SORUMLULUK VE GÖREV DAĞILIMLARI	9
VII. KİŞİSEL VERİLERİN İMHA USULLERİ	10
i) Kişisel Verilerin Silinmesi	10
ii) Kişisel Verilerin Yok Edilmesi	10
iii) Kişisel Verilerin Anonim Hale Getirilmesi	10
VIII. SAKLAMA VE İMHA SURELERİ	11 - 12
IX. PERİYODİK İMHA SURESİ	12
X. POLİTİKANIN YAYINLANMASI VE SAKLANMASI	12
XI. POLİTİKANIN GÜNCELLENME PERİYODU	12
XII. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI	12
XIII. DİĞER HUSUSLAR	12

I. GİRİŞ

i. Amaç

Kişisel Verilerin Saklanması ve İmhası Politikası ("Politika"), Çokyaşar Holding Anonim Şirketi ("Şirket" veya "Çokyaşar") tarafından gerçekleştirilmekte olan saklanma ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket, Şirket çalışanları, çalışan adayları, müşteriler, hizmet sağlayıcıları, ziyaretçiler 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.

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

ii. Kapsam

Şirket çalışanları, çalışan adayları, müşteriler, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup, Şirketin sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

iii. Tanımlar

Şirket	ÇOKYAŞAR HOLDİNG ANONİM ŞİRKETİ
Alıcı Grubu	Veri sorumlusu 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	Şirket personeli.
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
İlgili Kişi/Veri Sahibi	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	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.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
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.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme 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.
Politika	Kişisel Verileri Saklama ve İmha Politikası
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	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

II. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINA İLİŞKİN GENEL İLKELER

Şirket tarafından kişisel verilerin saklanması ve imhasında usul ve esasların belirlenmesinde ve uygulanmasında aşağıdaki ilkeler geçerli olacaktır:

- Şirket, kişisel verileri saklarken yahut silerken, yok ederken veya anonim hale getirirken, Kanunun 4. Maddesinde yer alan genel ilkelere uygun hareket etmektedir.
- Şirket, kişisel verileri saklarken yahut silerken, yok ederken veya anonim hale getirirken, Kanunun 12. maddesinde yer alan güvenlik tedbirlerine, ilgili mevzuatta yer alan hükümlere, Kurul'un alacağı kararlara ve bu Politika'ya uygun hareket etmektedir.
- Şirket, bünyesinde bulundurduğu kişisel verilerin amacı tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin imhası sırasında işbu Politika'ya ve Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.
- Şirket, Kişisel verileri saklama ve imha süreçlerinde hazır bulunacak çalışanları olacaksa, bunların unvan, birim ve görev tanımlarını belirler.
- Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilmektedir. Ancak, İlgili Kişinin talebi halinde uygun yöntem, gerekçesi açıklanarak seçilecektir.
- Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından re'sen veya İlgili Kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta ilgili kişi tarafından şirketimize başvurulması halinde;
 - İletilen talepler en geç 30 (otuz) gün içerisinde cevaplandırılmaktadır.
 - Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.
- Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.

III. KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır.

i. Elektronik Ortamlar

- ✓ Sunucular
- ✓ Yazılımlar (ofis yazılımları)
- ✓ 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.)
- ✓ Çıkarılabilir bellekler (USB, hafıza kart vb.)
- ✓ Yazıcı, tarayıcı, fotokopi makinesi.

ii. Elektronik olmayan (fiziki) ortamlar

- ✓ Kağıt
- ✓ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri vb.)
- ✓ Yazılı, basılı ve görsel ortamlar

IV. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından çalışanlar, çalışan adayları, müşteriler, ziyaretçileri, hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Kişisel veriler, Şirket tarafından güvenli bir biçimde, KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde Politika'nın III. maddesinde belirtilen fiziki veya elektronik ortamlarda özellikle aşağıda sayılan amaçlar doğrultusunda saklanmaktadır.

- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi.
- Ticari faaliyetlerin sürdürülebilmesi.
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat kurmak.
- Çalışan haklarının ve yan haklarının planlanması ve ifası.
- Müşteri ilişkilerinin yönetilebilmesi ve müşterilere daha iyi hizmet sunabilmek.
- Şirket güvenliğini sağlamak.
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler neticesinde iş ve işlemleri ifa edebilmek.
- Kişisel verilerin, sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması.
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanması zorunlu olması.
- Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

İlgili Kişilere ait kişisel veriler, Yönetmelik uyarınca, aşağıda sayılan hallerde Şirket tarafından re'sen veya talep üzerine silinir, yok edilir veya anonim hale getirilir.

- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması.
- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası.
- Kanunun 5 ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, İlgili Kişinin rızasını geri alması.
- İlgili kişinin, Kanun'un 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun Veri Sorumlusu tarafından kabul edilmesi.
- Veri Sorumlusu'nun, İlgili Kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması.
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

V. 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. maddesinde yer alan ilkeler ile Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirket tarafından tüm teknik ve idari tedbirler alınmıştır.

i) Teknik Tedbirler

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

- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- 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.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- 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.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

- Kişisel verilerin güvenli olarak saklanması sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- 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.
- 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 alınmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- 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 şifrelenmekte 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.

ii) İdari Tedbirler

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

- Saklanan kişisel verilere Şirket içi erişimi, iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar. Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

- Kişisel veri işleme envanteri hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.

VI. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin 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 sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alan personelin unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda düzenlenmiştir.

PERSONEL	GÖREV	SORUMLULUK
İnsan Kaynakları Sorumlusu	İnsan Kaynakları Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İş Sağlığı ve Güvenliği Sorumlusu	İş Sağlığı ve Güvenliği Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe-Finans Sorumlusu	Muhasebe-Finans Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satın Alma Sorumlusu	Satın Alma Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satış Sorumlusu	Satış Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Sevkiyat Sorumlusu	Sevkiyat Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

VII. KİŞİSEL VERİLERİN İMHA USULLERİ

Şirket tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler, Kanun ve Yönetmelikte sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde Şirket tarafından re'sen veya İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen usuller/teknikler ile imha edilecektir.

i) Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda belirtilen yöntemlerle silinir.

- a) **Sunucularda Yer Alan Kişisel Veriler:** Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
- b) **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.
- c) **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.
- d) **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.

ii) Kişisel Verilerin Yok Edilmesi

Kişisel veriler aşağıda belirtilen yöntemlerle yok edilir.

- a) **Fiziksel Ortamda Yer Alan Kişisel Veriler:** Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir.
- b) **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 değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

iii) 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.

VIII. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde,
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıta,
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

yer alır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Şirket'in İlgili Birimi tarafından yerine getirilir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kurumsal iletişim faaliyetlerinin planlanması ve icrası	İş ilişkisinin sona ermesine müteakip 10 yıl	Veri sahibinin imha başvurusunu takiben 30 gün içerisinde
Genel Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel ile ilgili mahkeme /icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşe alım	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş başvuru evrakları	İşe başvuru tarihini müteakip 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bordrolama	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İhale/işyeri açma/ bakanlıklar-müştaşarlıklar evrak hazırlama süreçleri her türlü yazışma	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log/Kayıt/Takip Sistemleri	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket kredi kartı tahsisi	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ödeme işlemleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Personel Finansman Süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşme sürecinin bir bölümü ve sözleşmenin muhafazası	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Toplantı notlarının katılımcılar ile paylaşılması	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Doküman hazırlanması	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Eğitim kayıtlarının dosyalanması	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kaza Raporlama, sağlık verileri	15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşterilere İlişkin Kişisel Veriler	6563 Sayılı Kanun ve ilgili mevzuat çerçevesinde ise 3 yıl, Hukuki ilişki son erdikten sonra 10 Yıl.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarikçilere İlişkin Kişisel Veriler	Hukuki ilişki sona erdikten sonra 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmeler	Sözleşmenin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

IX. PERİYODİK İMHA SÜRESİ

Yönetmelik'in 11. maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket'te her yıl haziran ve aralık aylarında periyodik imha işlemi gerçekleştirilir.

X. POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Yönetim Kurulu'nun ıslak imzasının bulunduğu işbu Politika Şirket KVK Klasörünün içinde bulunur ve veri işleyenlere mail ortamında aktarılır.

XI. POLİTİKANIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

XII. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket'in Yönetim Kurulu tarafından onaylanmış ve .../.../2020 tarihinde yürürlüğe girmiş kabul edilir.

Politikanın yürürlükten kaldırılmasına Yönetim Kurulu tarafından karar verilir.

XIII. DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır.

Politikada değişiklik olması durumunda, Politikanın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

Onay: YK Kaşe - İmza