GÖKTAŞ YASSI HADDE MAM. SAN. VE TİC. A.Ş

KİŞİSEL VERİ SAKLAMA ve

İMHA POLİTİKASI

İçindekiler

1. GİRİŞ 4

1.1 Amaç 4

1.2 Kapsam 4

1.3 Kısaltmalar ve Tanımlar 4

2. SORUMLULUK VE GÖREV DAĞILIMLARI 5

3. KAYIT ORTAMLARI 6

4. SAKLAMA İLİŞKİN AÇIKLAMALAR 6

4.1. Saklamayı Gerektiren Hukuki Sebepler 8

4.2. Saklamayı Gerektiren İşleme Amaçları 8

5. İMHAYA İLİŞKİN AÇIKLAMALAR 9

5.1 İmhayı Gerektiren Sebepler 9

6. TEKNİK VE İDARİ TEDBİRLER 9

6.1 Teknik Tedbirler 9

6.2 İdari Tedbirler 11

7. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ 13

7.1. Kişisel Verilerin Silinmesi 11

7.2. Kişisel Verilerin Yok Edilmesi 11

7.3. Kişisel Verilerin Anonim Hale Getirilmesi 12

8. SAKLAMA VE İMHA SÜRELERİ 13

9. PERİYODİK İMHA SÜRESİ 13

10. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI 14

11. POLİTİKA'NIN GÜNCELLENME PERİYODU 14

12. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI 14

GÖKTAŞ YASSI HADDE MAM. SAN. VE TİC. A.Ş VERİ İMHA POLİTİKASI

1.GİRİŞ

1.1.Amaç

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), **GÖKTAŞ YASSI HADDE MAMÜLLERİ SAN. VE TİC.A.Ş.** ("Şirket") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket; Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Şirket çalışanları, çalışan adayları, 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.

1.2.Kapsam

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

1.3.Kısaltmalar ve Tanımlar

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	**:**	Kişisel Verileri Koruma Kurumu personeli.
EBYS	**:**	Elektronik Belge Yönetim Sistemi
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.
Hizmet Sağlayıcı	**:**	Kişisel Verileri Koruma Kurumu 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	**:**	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, 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 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 Anonim Hale Getirilmesi	**:**	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Kişisel Verilerin Silinmesi	**:**	Kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
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

Kurum	**:**	Kişisel Verileri Koruma Kurumu
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 işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
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 Sorumlusu	**:**	Kişisel verilerin işleme amaç ve yöntemlerini belirleyen, ilgili kanuna uygun olarak veriyi işleyen ve muhafaza eden gerçek veya tüzel kişi.
Veri Kayıt Sistemi	**:**	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sorumluları Sicil Bilgi Sistemi	**:**	Veri sorumlularının Sicile başvuruda ve Sicile ilişin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	**:**	Veri Sorumluları Sicili Bilgi Sistemi.
Yönetmelik	**:**	28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.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 arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla 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 alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVANI	BİRİMİ	GÖREVİ

Şirket Yönetimi	Yönetim Kurulu	Çalışanların politikaya uygun davranmasından sorumludur.
İnsan Kaynakları Birimi ,İdari İşler Birimi, Hukuk Departmanı	Diğer Birimler	Yönetmeliğin hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden ve İlgili Kişi başvurularının yanıtlanmasından sorumludur.
Bilgi İşlem Sorumlusu	Bilgi İşlem Servisi	Yönetmeliğin uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur. Görevlerine uygun olarak Yönetmeliğin yürütülmesinden sorumludur.
	Diğer Tüm Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

3.KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	**Elektronik Olmayan Ortamlar**
Yazıcılar, tarayıcılar, fotokopi makineleri Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Optik diskler(CD,DVD vb.) Yazılımlar(Ofis yazılımları, portal, EBYS, VERBİS.) Bilgi güvenliği cihazları(güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası,) antivirüs vb.) Çıkarılabilir ve taşınabilir bellekler(USB,Hafıza kartı vb.) Kişiseel bilgisayarlar (Masaüstü,Dizüstü) Mobil Cihazlar(Telefon,Tablet vb.)	Kağıtlar Yazılı ,basılı,görsel ortamlar Manuel veri kayıt sistemleri(anket formları, ziyaretçi giriş defteri)

4.SAKLAMAYA İLİŞKİN AÇIKLAMALAR

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.*

4.1.Saklamayı Gerektiren Hukuki Sebepler;

Şirket, kişisel verileri belirli ve meşru amaçlarla, Kanun'da ve Politika'da detaylandırılan ilkeler ışığında saklamaktadır. Şirketin kişisel verileri saklamasını gerektiren birincil sebep, yürürlükte olan kanun ve bu kanunlar uyarınca işleme konulan ikincil mevzuattan kaynaklı yükümlülüklerdir. Kişisel veriler öncelikle kanunlar çerçevesinde öngörülen süreler kadar saklanmaktadır. Süreye ilişkin kanuni bir düzenlemenin bulunmadığı durumlarda Şirket, ilgili kişisel veriyi, işleme süreci ve olası ihtilaflarda delil vasfı ve zamanaşımı def'i de göz önüne alarak kanuni zamanaşımı süresi kadar muhafaza eder. Herhangi bir ihtilafa konu olması mümkün görülmeyen süreçlerde ise kişisel verinin işlenmesini gerektiren sebeplerin varlığı ışığında teamül gereği makul bir süre ilgili verileri saklayabilecektir.

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.2.Saklamayı Gerektiren İşleme Amaçları

Şirket, Kişisel Veri İşleme Envanteri'nde detaylı bir biçimde yer verdiği ve kategorize ettiği kişisel verileri, hukuki yükümlülükleri yerine getirilebilmek, çalışan haklarını ve yan haklarını planlayabilmek, müşteri ilişkilerini yönetilebilmek ve ticari faaliyetlerini sürdürülebilmek amacıyla madde 4'te belirtilen fiziki yahut elektronik ortamlarda kanunda öngörülen ilke ve süreler ışığında ve aşağıdaki amaçlar doğrultusunda saklamakadır:

- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesinin sağlanması,

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Satış oranları yahut performans değerlendirmeleri gibi hususlarda gerekli istatistiksel çalışmaların ve yasal raporlamaların yapılabilmesi
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- İnsan kaynakları süreçlerinin yürütülmesi ile şirket içi yahut şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibatın sağlanması,
- Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması yahut mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Şirket güvenliğinin sağlanması,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü gereği,
- Acil durum yönetimi süreçlerinin yürütülmesi,
- Bilgi güvenliği süreçlerinin yürütülmesi,
- Çalışan adayı, stajyer ve öğrenci seçme ve yerleştirme süreçlerinin yürütülmesi,
- Çalışan adaylarının başvuru süreçlerinin yürütülmesi,
- Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi,
- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,
- Çalışanlar için yan haklar ve menfaatleri süreçlerinin yürütülmesi,
- Denetim ve etik faaliyetlerinin yürütülmesi,
- Eğitim faaliyetlerinin yürütülmesi,
- Erişim yetkilerinin yürütülmesi,
- Faaliyetlerin mevzuata uygun yürütülmesi,
- Finans ve muhasebe işlerinin yürütülmesi,
- Firma, ürün ve hizmetlere bağlılık süreçlerinin yürütülmesi,
- Fiziksel mekân güvenliğinin temini,
- Görevlendirme süreçlerinin yürütülmesi,
- Hukuk işlerinin takibi ve yürütülmesi,
- İç denetim, soruşturma ve istihbarat faaliyetlerinin yürütülmesi,
- İletişim faaliyetlerinin yürütülmesi,
- İş faaliyetlerinin yürütülmesi ve denetimi,
- İş sağlığı ve güvenliği faaliyetlerinin yürütülmesi,
- İş süreçlerinin iyileştirilmesine yönelik önerilerin alınması ve değerlendirilmesi,
- İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi,
- Lojistik faaliyetlerinin yürütülmesi,
- Mal ve hizmet satın alım süreçlerinin yürütülmesi,
- Mal ve hizmet satış sonrası destek hizmetlerinin yürütülmesi,
- Mal ve hizmet satış süreçlerinin yürütülmesi,
- Mal ve hizmet üretim ve operasyon süreçlerinin yürütülmesi,
- Müşteri ilişkileri yönetimi süreçlerinin yürütülmesi,
- Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi,
- Organizasyon ve etkinlik yönetimi,
- Pazarlama analiz çalışmalarının yürütülmesi,
- Performans değerlendirme süreçlerinin yürütülmesi,
- Reklam, kampanya ve promosyon süreçlerinin yürütülmesi,

- Risk yönetimi süreçlerinin yürütülmesi,
- Saklama ve arşiv faaliyetlerinin yürütülmesi,
- Sözleşme süreçlerinin yürütülmesi,
- Sponsorluk faaliyetlerinin yürütülmesi,
- Stratejik planlama faaliyetlerinin yürütülmesi,
- Talep ve şikâyetlerin takibi,
- Taşınır mal ve kaynakların güvenliğinin temini,
- Tedarik zinciri yönetimi süreçlerinin yürütülmesi,
- Ücret politikasının yürütülmesi,
- Ürün ve hizmetlerin pazarlama süreçlerinin yürütülmesi,
- Veri sorumlusu operasyonlarının güvenliğinin temini,
- Yatırım süreçlerinin yürütülmesi,
- Yetenek / kariyer gelişimi faaliyetlerinin yürütülmesi,
- Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi,
- Yönetim faaliyetlerinin yürütülmesi,
- Ziyaretçi kayıtlarının oluşturulması ve takibi.

5.İMHAYA İLİŞKİN AÇIKLAMALAR

5.1.İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması 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,

durumlarında, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

6.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.

6.1.Teknik Tedbirler

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

- Sızma (Penetrasyon) testleri ile Şirketimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- 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.
- Kurumun 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 saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- 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 alınması,

- 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.

6.2.İdari Tedbirler

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

- 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 ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

7.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Şirket, kanunda öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sona ermesi halinde kişisel verileri, yine ilgili kanun hükümlerine uygun bir biçimde aşağıda belirtilen tekniklerle imha eder.

7.1.Kişisel Verilerin Silinmesi

- **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.

- **Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office365 vb.):** Bulut sisteminde verileri silme komutu vererek silinir. Anılan işlem gerçekleştirirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına özellikle dikkat edilecektir.
- **Elektronik Ortamda Yer Alan Kişisel Veriler:** Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yönetici hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
- **Fiziksel Ortamda Yer Alan Kişisel Veriler:** Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
- **Taşınabilir Medyada Bulunan Kişisel Veriler:** Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır;

- Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

7.2.Kişisel Verilerin Yok Edilmesi

- **Fiziksel Ortamda Yer Alan Kişisel Veriler:** Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
- **Optik / Manyetik Medyada Yer Alan Kişisel Veriler:** Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır.
- **De-manyetize Etme:** Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.
- **Üzerine Yazma:** Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

7.3.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; Şirket'in, verilerin aktarıldığı üçüncü kişi veya kişiler 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 gerekir.

Şirket kişisel verileri anonim hale getirmek için "Değişkenleri Çıkartma, Kayıtları Çıkartma, Alt ve Üst Sınır Kodlama, Bölgesel Gizleme, Örnekleme, Mikro-Birleştirme, Veri Değiş-Tokuşu, Gürültü Ekleme, K-Anonimlik, L-Çeşitlilik, T-Yakınlık" yöntemlerden bir veya birkaçını kullanabilir: Veri Sorumlusu sıfatı ile Şirket, ilgili süreçlerde hangi yöntemi uygulayacağına, ilgili verinin kayıt ortamı, niteliği, büyüklüğü, sağlanmak istenen fayda ve işleme amacı gibi özellikleri tespit ederek karar verir.

8.SAKLAMA VE İMHA SÜRELERİ

Şirket, KVKK ve mevzuata uygun biçimde elde ettiği kişisel verilerin saklama ve imha süreçlerindeki süre tespitine ilişkin olarak; öncelikle mevzuatta bir süre öngörülmüş ise bu süreye riayet etmektedir.

Belirtilen sürenin sona ermesi halinde veya mevzuatta saklamaya ilişkin herhangi bir süre öngörülmemiş ise; kişisel veriler, KVKK'nın 6. maddesi dikkate alınarak kişisel veriler ve özel nitelikli kişisel veriler olarak ayrıma tabi tutulur. Özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir.

KVKK'nın 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler veya verinin saklanmasında Şirket'in meşru bir amacının olmadığı durumlarda silinir, yok edilir ya da anonim hale getirilir.

Verinin saklanması KVKK'nın 5. ve 6. maddelerinde öngörülmüş olan istisna kapsamında ise gereken makul süreler tespit edilir ve makul sürenin bitiminde ilgili veriler silinir, yok edilir ya da anonim hale getirilir.

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

1. Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
2. Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
3. Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde güncellemeler yapılır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ

Genel kurul ve yönetim kurulu işlemleri, şirket ortakları ve yönetim kurulu üyelerine ilişkin bilgiler	10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin akdedilmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği uygulamaları	İş akdinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel muhasebe süreçleri, ödeme ve tahsilat işlemleri	İş ilişkisinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan kaynakları dair süreçlerin yürütülmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel muhasebe süreçleri, ödeme ve tahsilat işlemleri	İş ilişkisinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanların sistem ve Yazılımlar atanımlanması, tahsis ve erişimyetkisi verilmesi (e-mail adresi, kullanıcı adı, şifre, parola gibi)	İş akdinin bitiminden itibaren 3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel kalite süreçlerine ilişkin faaliyetlerdeki bilgiler, çalışanların şirket içi/dışı eğitim kayıtları	İş akdinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan adaylarına ilişkin veriler	Başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mahkeme, icra, idari mercilerin bilgi taleplerinin cevaplanması	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel finansman süreçleri	İş ilişkisinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Rehber kayıtları, kurumsal iletişim faaliyetleri, planlanması ve icrası	İş ilişkisinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Silme, yok etme, anonim hale getirme kayıt süreci	İşlem tarihinden itibaren 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı Katılımcılarının Kaydı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log kayıtları	2 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	3 AY	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
KVK Süreçleri (Aydınlatma, AçıkRıza, Başvuru ve Şikayetler)	İlgili sürecin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sevkiyat kayıtları (nakliye, irsaliye vb.)	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarik ve satış süreçleri, teknik bilgi talepleri, müşteri şikayetlerinin yanıtlanması	Ticari ilişkinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

9.PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirkette her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

10. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Kişisel Verileri Koruma Ekibi'nin dosyasında saklanır.

11.POLİTİKA'NIN GÜNCELLENME PERİYODU

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

11.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Şiret Kararı ile Kişisel Veri Koruma Ekibi tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Kişisel Veri Koruma Ekibi tarafından saklanır.