KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

1.1 Amaç

Bu Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") 7. Maddesi ve Kanun'un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete'de yayınlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla Eretim Bilgisayar Hizmetleri ve Danışmanlık Limited Şirketi ("Eretim" veya "Şirket") tarafından hazırlanmıştır.

1.2 Kapsam

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve herhangi bir nedenle Şirket nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

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:** 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.
- **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:** 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.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

- **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.
- **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 işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
- **Veri 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

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 süreçleri Şirket bünyesinde kurulmuş olan Bilgi Güvenliği ve Kişisel Veri Komitesi (Tablo 1) tarafından yürütülmektedir.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

Tablo 1: Bilgi Güvenliği ve Kişisel Veri Komitesi Görev Dağılımı

Unvan	Görev	Sorumluluk
Genel Müdür	Bilgi Güvenliği ve Kişisel Veri Komitesi Başkanı	Çalışanların politikaya uygun hareket etmesi.
Genel Müdür Yrd.	Bilgi Güvenliği ve Kişisel Veri Komitesi Üyesi	Politikanın hazırlanması, yürütülmesi, yayınlanması ve güncellenmesi.
Genel Müdür Yrd. (Bilgi Güvenliği ve Altyapı)	Bilgi Güvenliği ve Kişisel Veri Komitesi Üyesi	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulması.
Birim Yöneticileri	İnsan Kaynakları, Muhasebe, Satış, Profesyonel Hizmetler, Ar-Ge	Görevlerine uygun olarak Politikanın yürütülmesi.

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
- Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) - Yazılımlar (ofis yazılımları, portal, vb.) - Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.) - Kişisel bilgisayarlar (Dizüstü) - Mobil cihazlar (telefon, tablet vb.) - Çıkartılabilir bellekler (USB, Hafıza Kart vb.) - Yazıcı, tarayıcı, fotokopi makinesi	- Kâğıt, - Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) - Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

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

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

4.1 Saklamaya İlişkin Açıklamalar

3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. 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. maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Şirketin faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Şirkette faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 4857 sayılı İş 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
- 5746 sayılı Araştırma ve Geliştirme Faaliyetlerinin Desteklenmesi Hakkında Kanun
- 6098 sayılı Türk Borçlar Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

Şirket faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Şirket güvenliğini sağlamak.
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Şirketin reklam ve tanıtımlarının yapılması ve arşiv faaliyetlerinin yürütülmesi.
- Yasal raporlamalar yapmak.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.2 İmhayı Gerektiren Sebepler

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Şirket tarafından resen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir.

- Kişisel verilerin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası sebebiyle gerekli olması hali,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanun'un 11. maddesindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili 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 şikâyette 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.

5. TEKNİK VE İDARİ TEDBİRLER

Şirket, kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12. maddesiyle Kanunun 6. maddesi 4. fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde gerekli teknik ve idari tedbirleri alır.

5.1 Teknik Tedbirler

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile güvenlik politikaları aracılığı ile yapılmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanım ve yazılım seviyesinde önlemler alınmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme süreçleri uygulanmaktadır.
- Kişisel veri içeren bilgi teknoloji sistemlerinin ve verilerin korunması amacıyla, SSL ve TLS bağlantıları, anti virüs ve güvenlik duvarı yazılım ve donanımları kullanılır.
- 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.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili kontrol çalışmaları yapılmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- 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 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 veri aktarımı gerçekleştirilmektedir. Kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizlilik dereceli belgeler” formatta gönderilmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.

5.2 İdari Tedbirler

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması ile ilgili eğitimler verilmektedir.
- Yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

- Saklanan kişisel verilere erişim, iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi dikkate alınır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Şirket ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir veya yok edebilir. Kişisel verilerin silinmesi akabinde ilgili kişiler hiçbir şekilde silinen verilere tekrardan erişemeyecek ve kullanamayacaktır.
Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır. Şirket, verilerin kaydedildiği ortama bağlı olarak aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir.

6.1 Kişisel Verilerin Silinmesi

Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Uygulanan yöntemler Tablo 3'te verilmiştir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
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.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi 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.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Uygulanan yöntemler Tablo 4'te verilmiştir.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süresi 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. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

- **Maskeleme (Masking):** Veri maskeleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.
- **Kayıtları Çıkartma:** Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.
- **Bölgesel Gizleme:** Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
- **Global Kodlama:** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; açık adres yerine ikamet edilen bölgenin belirtilmesi.
- **Veri Karma ve Bozma:** Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

7. 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 kayıtta,
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

yer alır.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Eretim Bilgi Güvenliği ve Kişisel Veri Komitesi tarafından güncellemeler yapılır.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Eretim Bilgi Güvenliği ve Kişisel Veri Komitesi tarafından seçilir.

Tablo 5: Süreç Bazında Saklama ve İmha Süreleri

Süreç	Saklama Süresi	İmha Süresi
Sözleşmeler	Hukuki İlişki Süresi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçleri	Hukuki İlişki Süresi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yasal Mevzuat Kaynaklı Süreçler (İş Sağlığı ve Güvenliği Mevzuatı)	Hukuki İlişki Süresi + 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yasal Mevzuat Kaynaklı Süreçler (Ar-Ge)	Hukuki İlişki Süresi + 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçleri	En fazla 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi Kaydı	En fazla 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İletişim Faaliyetleri	En fazla 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Sistemleri	En fazla 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

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

9. 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 Eretim Bilgi Güvenliği ve Kişisel Veri Komitesi dosyasında saklanır.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür

10. POLİTİKA'NIN GÜNCELLENME PERİYODU

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

11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirket internet sitesinde (www.ereteam.com) yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Eretim Bilgi Güvenliği ve Kişisel Veri Komitesi tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır.

Hazırlayan	Onaylayan
Bilgi Güvenliği ve Altyapı Yönetim Temsilcisi	Genel Müdür