

Kişisel Verileri Saklama ve İmha Politikası

İÇİNDEKİLER

1. GİRİŞ.....	2
1.1. Amaç ve Kapsam.....	2
1.2. Tanımlar	2
2. KAYIT ORTAMLARI.....	4
2.1. Elektronik Ortamlar	4
2.2. Elektronik Olmayan Ortamlar	4
3. SAKLAMA ve İMHAYA İLİŞKİN AÇIKLAMALAR.....	4
3.1. Saklamaya İlişkin Açıklamalar	4
3.1.1. Saklamayı Gerektiren Hukuki Sebepler.....	4
3.1.2. Saklamayı Gerektiren İşleme Amaçları	5
3.2. İmhayı Gerektiren Sebepler	5
4. TEKNİK ve İDARİ TEDBİRLER.....	6
4.1. Teknik Tedbirler	6
4.2. İdari Tedbirler	6
5. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ	7
5.1. Kişisel Verilerin Silinmesi	7
5.2. Kişisel Verilerin Yok Edilmesi	8
5.3. Kişisel Verilerin Anonim Hale Getirilmesi	9
6. SAKLAMA ve İMHA SÜRELERİ.....	9
6.1. Saklama Süresi	9
6.2. İmha Süresi.....	9
7. POLİTİKANIN YAYINLANMASI ve SAKLANMASI	9
8. POLİTİKANIN İHLALİ ve YAPTIRIMLAR	9
9. POLİTİKANIN YÜRÜRLÜĞÜ.....	9

1. GİRİŞ

1.1. Amaç ve Kapsam

İşbu Politika, Veri Sorumlusu **PCX** (bundan böyle "**Kurum**" olarak anılacaktır.) tarafından, KVKK'nın 7. maddesi uyarınca uyulması gereken usul ve esasları belirlemek amacıyla hazırlanmıştır.

Kurum, bünyesinde bulundurduğu, tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi sırasında işbu Politika 'ya ve Politika 'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.

İşbu Politika; **Kurum** 'un kişisel verileri işlediği herhangi bir süreçte dahil olan Çalışan, Çalışan Adayı, Çalışan Yakını, Tedarikçi Yetkilisi, Tedarikçi Çalışanı, Ürün veya Hizmet Alan Kişi, Potansiyel Ürün veya Hizmet Alan Kişi, Stajyer, Ziyaretçi, Çalışan Yakını, Çalışanın Eski İşyerindeki Yetkili, İşveren, İşyeri Hekimi, Kamu Görevlisi, Kurum Yetkilisi, Referans Olan Kişi, Teslim Alan ve Teslim Eden Kişi ve Kişisel Verilerini İşlediği Herhangi Bir Sürece Dâhil Olan Diğer 3. Kişilere ait kişisel verileri kapsamaktadır.

İşbu Politika; **Kurum** 'un kişisel veri üzerinde uygulayacağı tüm imha faaliyetlerini kapsamakta olup, her türlü imha gereksinimi sonucunda uygulanacaktır.

İşbu Politika kişisel veri olmayan veriler hakkında uygulanmayacaktır.

Konuyla alakalı yeni mevzuatlar yayımlanması veya ilgili mevzuatın güncellenmesi durumunda, işbu Politika ilgili mevzuatlara uyumlu olacak şekilde güncellenerek mevzuat gerekliliklerine uyulacaktır.

Kurum, işbu Politika ile aşağıda belirtilen ortamlardaki ve belirtilen ortamlara ek ortaya çıkabilecek tüm ortamlardaki kişisel verileri kapsadığını kabul eder.

- Ağ cihazları,
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücülerini,
- Kurum adına kullanılan bilgisayarlar/sunucular,
- Flash hafızalar,
- Kâğıt,
- Manyetik bantlar,
- Mikrofiş,
- Mobil telefonlar ve içerisindeki tüm saklama alanları,
- Optik diskler,
- Yazıcı, Parmak izi okuyucu ve yüz tarama gibi çevre birimler.

1.2. Tanımlar

Tanım	Açıklama
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Kurum	PCX Operasyon Yazılım ve Danışmanlık Hizmetleri Anonim Şirketi
Çalışan	Kurum 'da çalışanlar
Çalışan Adayı	Kurum 'a iş başvurusunda bulunan kişiler
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 Sorumlusu

	'ndan aldığı yetki ve düzenlemeler doğrultusunda kişisel verileri işleyen kişiler
İmha	Kişisel verilerin silinmesi veya yok edilmesi
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 Verinin 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 getirilmesi
Kişisel Verinin İmha Edilmesi	Kişisel verilerin silinmesi, anonim hale getirilmesi veya yok edilmesi işlemi
Kişisel Verinin Silinmesi	Kişisel verilerin İlgili Kullanıcı için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Kişisel Verinin Yok Edilmesi	Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Komite	Kişisel Verileri Koruma Komitesi
KVKK	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurulu	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 veriler
Periyodik İmha	KVKK 'da yer alan 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 Veri Saklama ve İmha Politikası
Talimat	Kişisel Verilerin Korunması Disiplin Talimatı
Ürün veya Hizmet Alan	Kurum ile sözleşme ilişkisi bulunan gerçek veya tüzel kişiler
Veri Kayıt Sistemi	Kişisel Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistem
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

2. KAYIT ORTAMLARI

2.1. Elektronik Ortamlar

- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
- Çıkarılabilir bellekler (USB, hafıza kartı vb.)
- Kişisel bilgisayarlar (Masaüstü, dizüstü)
- Mobil cihazlar (telefon, tablet vb.)
- Optik diskler (CD, DVD, vb.)
- Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.)
- Video kaydı ve ses kaydı
- Yazıcı, tarayıcı, fotokopi makinesi
- Yazılımlar (Ofis yazılımları...)

2.2. Elektronik Olmayan Ortamlar

- Kâğıt
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi girişi defteri)
- Yazılı, basılı, görsel ortamlar

3. SAKLAMA ve İMHAYA İLİŞKİN AÇIKLAMALAR

Kurum tarafından; işbu Politika kişisel verilerinin işlediği herhangi bir sürece dâhil olan Çalışan, Çalışan Adayı, Çalışan Yakını, Tedarikçi Yetkilisi, Tedarikçi Çalışanı, Ürün veya Hizmet Alan Kişi, Potansiyel Ürün veya Hizmet Alan Kişi, Stajyer, Ziyaretçi, Çalışan Yakını, Çalışanın Eski İşyerindeki Yetkili, İşveren, İşyeri Hekimi, Kamu Görevlisi, Kurum Yetkilisi, Referans Olan Kişi, Teslim Alan ve Teslim Eden Kişi, Habere Konu Kişi ve Kişisel Verilerini İşlediği Herhangi Bir Sürece Dâhil Olan Diğer

3. Kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

3.1. Saklamaya İlişkin Açıklamalar

KVKK 'nın 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, KVKK 'nın 4. maddesinde işlenen kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, KVKK 'nın 5 ve 6. maddelerinde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, **Kurum** faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

3.1.1. Saklamayı Gerektiren Hukuki Sebepler

- 213 sayılı Vergi Usul Kanunu
- 2004 sayılı İcra İflas Kanunu
- 4458 sayılı Gümrük Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6098 sayılı Türk Borçlar Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- 6362 sayılı Sermaye Piyasası Kanunu
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun
- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6769 sayılı Sınai Mülkiyet Kanunu

- İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
- İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği
- Kişisel Koruyucu Donanımların İşyerlerinde Kullanılması Hakkında Yönetmelik
- Ticaret Sicil Yönetmeliği
- Ücret, Prim, İkramiye ve Bu Nitelikteki Her Türlü İstihkakın Bankalar Aracılığıyla Ödenmesine Dair Yönetmelik

Kişisel veriler, bu kanunlar ile yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

3.1.2. Saklamayı Gerektiren İşleme Amaçları

Kurum, faaliyetleri çerçevesinde işlemekte olduğu kişisel veriyi aşağıdaki amaçlar doğrultusunda saklar:

- Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayı / Stajyer / Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
- Diğer (Zimmet Faaliyetlerinin Yürütülmesi)
- Eğitim Faaliyetlerinin Yürütülmesi
- Erişim Yetkilerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi
- Finans ve Muhasebe İşlerinin Yürütülmesi
- Fiziksel Mekân Güvenliğinin Temini
- Görevlendirme Süreçlerinin Yürütülmesi
- Hukuk İşlerinin Takibi ve Yürütülmesi
- İç Denetim / Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İnsan Kaynakları Süreçlerinin Planlanması
- İş Faaliyetlerinin Yürütülmesi / Denetimi
- İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- Organizasyon ve Etkinlik Yönetimi
- Pazarlama Analiz Çalışmalarının Yürütülmesi
- Performans Değerlendirme Süreçlerinin Yürütülmesi
- Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Tedarik Zinciri Yönetimi Süreçlerinin Yönetilmesi
- Yabancı Personel çalıştırma ve Oturma İzni İşlemleri
- Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
- Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

3.2. İmhayı Gerektiren Sebepler

Kurum 'un, İlgili Kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya KVKK 'da öngörülen süre içinde cevap vermemesi hallerinde;

- 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, İlgili Kişi 'nin açık rızasını geri alması,
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- KVK Kurulu'na şikâyetle bulunması ve bu talebin KVK Kurulu tarafından uygun bulunması,
- KVKK 'nın 11. maddesi gereği İlgili Kişi 'nin hakları çerçevesinde kişisel verilerin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,

durumlarında, **Kurum** tarafından İlgili Kişi 'nin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4. 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 KVKK 'nın 12. maddesiyle KVKK 'nın 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için KVK Kurulu tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde **Kurum** tarafından teknik ve idari tedbirler alınır.

4.1. Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi sistemleri güncel halde tutulmakta, kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır. Çalışan için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim yetki ve rol dağılımları için düzenlemeler oluşturulmakta ve uygulanmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Görev değişikliği olan ya da işten ayrılan Çalışan 'ın bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte, güvenlik duvarları kullanılmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan yedekleme programları kullanılmakta ve elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

4.2. İdari Tedbirler

- Çalışan için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışan için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışan 'a gizlilik sözleşmeleri imzalatılmaktadır.
- Çalışan 'ın niteliği ve teknik bilgi/beceri geliştirilmektedir.

- Kurum düzenlemelerine uymayan Çalışan 'a yönelik uygulanacak disiplin süreçleri uygulanmaktadır, İlgili Kişiler 'i aydınlatma yükümlülüğü yerine getirilmekte, kurum içi periyodik ve rastgele denetimler yapılmakta ve Çalışan 'a yönelik bilgi güvenliği eğitimleri verilmektedir.
- Gizlilik taahhütnameleri yapılmaktadır. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- İletişim teknikleri ve ilgili mevzuatlar hakkında eğitimler verilmektedir.
- Kişisel veri güvenliği politikaları, talimatları ve prosedürleri belirlenmiştir.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel verilere hukuka aykırı erişilmesi önlenmektedir.
- Kişisel verilerin hukuka aykırı işlenmesi önlenmektedir.
- Kişisel verilerin muhafazası sağlanmaktadır.
- Kurum içi periyodik ve rastgele denetimler yapılmakta ve Çalışan 'a yönelik bilgi güvenliği eğitimleri verilmektedir.

5. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, **Kurum** tarafından re 'sen veya İlgili Kişi 'nin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir veya anonimleştirilir.

5.1. Kişisel Verilerin Silinmesi

Kişisel veriler, **Kurum** tarafından veya gerekli görülür ise Kurum 'un belirlediği başkaca bir 3. kişi tarafından aşağıda belirtilen yöntemlerle imha edilir.

Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer Çalışan (İlgili Kullanıcı) 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 Çalışan için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Kâğıt Ortamında Bulunan Kişisel Verilerin Karartılması	Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından İlgili Kullanıcı 'nın erişim yetkisi kaldırılarak silme işlemi yapılır.

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.
Uzman Tarafından Güvenli Olarak Silme	Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veri bu konuda uzman olan kişi tarafından İlgili Kullanıcı için hiçbir şekilde, erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.
Yazılımdan Güvenli Olarak Silme	Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır. Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde İlgili Kullanıcı 'nın erişim hakkının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

5.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, **Kurum** tarafından aşağıda belirtilen yöntemlerle yok edilir.

Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemez şekilde yok edilir.
Fiziksel Yok Etme	Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verilerin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kâğıt ortamındaki verilerin yok edilmesi de başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.
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.

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.
----------------------	--

Yukarıda sayılan durumların gerçekleşmesi sırasında **Kurum**; KVKK, Yönetmelik ve ilgili diğer mevzuat hükümlerine veri güvenliğinin sağlanması amacıyla tam uyum sağlamakta ve gerekli tüm idari ve teknik tedbirleri almaktadır.

5.3. Kişisel Verilerin Anonim Hale Getirilmesi

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

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya 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.

6. SAKLAMA ve İMHA SÜRELERİ

6.1. Saklama Süresi

Kurum tarafından, kişisel verilerin saklanma süreleri belirlenirken yürürlükte bulunan mevzuat ve süreç konusu verilerin işleme amaçları göz önünde tutularak bir belirleme yapılmaktadır.

Saklama süreleri, her halükârda kanuni yükümlülükler ve ilgili zamanaşımı süreleri ışığında tespit edilmektedir.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde **Kurum** tarafından güncellemeler yapılabilmektedir. Veri işleme amacının ortadan kalkması halinde, verilerin tutulmasına olanak sağlayan başka bir hukuki sebep veya dayanak bulunmadığı sürece veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

6.2. İmha Süresi

Yönetmeliğin 11. maddesi gereğince **Kurum**, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, her yıl 6. ve 12. aylarında periyodik imha işlemi gerçekleştirilir.

7. POLİTİKANIN YAYINLANMASI ve SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, resmi internet sayfasında açıklanır. Basılı kâğıt nüshası da **Kurum** 'da saklanır.

8. POLİTİKANIN İHLALİ ve YAPTIRIMLAR

Bu Politika 'nın ihlali halinde, Talimat gereğince; o tarihte geçerli disiplin süreci işletilerek, uyarma, kınama, para cezasının tahsili yoluna gidilebilir ve sözleşme feshi yaptırımlarından bir ya da birkaçı birden uygulanabilir, ayrıca yasal işlem başlatılabilir.

9. POLİTİKANIN YÜRÜRLÜĞÜ

Kurum tarafından düzenlenen İşbu Politika, 26/06/2020 tarihinde yürürlüğe girmiş olup, Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda gerekli güncellemeler yapılacaktır.

İşbu Politika'nın uygulanmasını, güncellenmesini, duyurulmasını **Komite** yürütür.