KİŞİSEL VERİLERİ SAKLAMA ve İMHA POLİTİKASI

İÇİNDEKİLER

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Doküman Tarihi :

Düzenlenme Tarihi :

Revizyon Sayısı :

I. GİRİŞ

A. Amaç ve Kapsam

İşbu Politika, Veri Sorumlusu **AK ALÜMİNYUM** tarafından, KVKK'nın 7. maddesi uyarınca uyulması gereken usul ve esasları belirlemek amacıyla hazırlanmıştır.

AK ALÜMİNYUM, 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; **AK ALÜMİNYUM**'un kişisel verileri işlediği herhangi bir sürece dâhil olan Çalışan Adayı, Çalışan, Hissedar/Ortak, Potansiyel Ürün veya Hizmet Alıcısı, Tedarikçi Çalışanı, Tedarikçi Yetkilisi, Ürün veya Hizmet Alan Kişi, Ziyaretçi, Diğer (Çalışan Aile Bireyi ve Yakını, Referanslar, Veli/Vasi/Temsilci, İşbirliği İçinde Olduğumuz Kurumların Çalışanı/Yetkilisi/ Hissedarı), Kişisel Verilerini İşlediği Herhangi Bir Sürece Dâhil Olan Diğer 3. Kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

İşbu Politika; **AK ALÜMİNYUM**'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.

AK ALÜMİNYUM, 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 sürücüleri,
- **AK ALÜMİNYUM** adına kullanılan bilgisayarlar/sunucular,
- Flash hafızalar,
- Kâğıt,
- Mobil telefonlar ve içerisindeki tüm saklama alanları,
- Optik diskler,
- Yazıcı, Parmak izi okuyucu ve yüz tarama gibi çevre birimler.

B. Tanımlar

Tanım	Açıklama
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
AK ALÜMİNYUM	Ak Alüminyum Sanayi ve Ticaret A.Ş.
Çalışan	AK ALÜMİNYUM'da çalışanlar ve yöneticiler
Çalışan Adayı	AK ALÜMİNYUM'a herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini AK ALÜMİNYUM'un incelemesine açmış olan gerçek 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	AK ALÜMİNYUM 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 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
Politika	AK ALÜMİNYUM Kişisel Veri Saklama ve İmha Politikası
Talimat	AK ALÜMİNYUM Kişisel Verilerin Korunması Disiplin Talimatı
Tedarikçi Temsilcisi	Tedarikçi Yetkilisi ve Tedarikçi Çalışanı
Ürün veya Hizmet Alan	AK ALÜMİNYUM 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

II. SORUMLULUK ve GÖREV DAĞILIMLARI

AK ALÜMİNYUM'un tüm birimleri ve çalışanları, Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, çalışanların 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

UNVAN	BİRİM	GÖREV
AK ALÜMİNYUM Yönetim	AK ALÜMİNYUM	AK ALÜMİNYUM'un kişisel verilerin saklama ve imhası ile ilgili işlemlerin yapılmasını sağlamak
Satış Pazarlama Sorumlusu	Satış Pazarlama Birimi	Şirket pazarlama ve müşteri ilişkileri süreçlerinde müşteri ve diğer 3. Kişilerle ilgili saklama ve imha süreçlerinin uygulanması
İnsan Kaynakları Sorumlusu	İnsan Kaynakları Birimi	Çalışan ve çalışan adayı kişisel verilerinin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, Çalışanların Kanun'da belirtilen hakları ile ilgili aydınlatılması taleplerinin alınması ve cevaplandırılması
Muhasebe ve Finans Sorumlusu	Muhasebe ve Finans Birimi	Görevi dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürenin yönetimi, 6100 sayılı TTK ve Vergi Mevzuatından kaynaklanan defter, belge saklama yükümlülüklerinin devamının ve yükümlülüklerin ortadan kalkıp kalmadığının kontrolü
BT / IT Sorumlusu	Bilgi İşlem Birimi	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden, politikanın uygulanmasında gereksinim duyulan teknik çözümlerin belirlenmesi ve uygulanmasından sorumludur.
Diğer Birim Yöneticileri	Diğer Birimler	Kendi birimlerinde politikanın uygulanması ve uygulamanın izlenmesi ve denetlenmesinden sorumludur.

III. KAYIT ORTAMLARI

A. Elektronik Ortamlar

- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
- Çıkartılabilir 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, veritabanı, web, dosya paylaşım vb.)
- Video kaydı ve ses kaydı
- Yazıcı, tarayıcı, fotokopi makinesi
- Yazılımlar (Ofis yazılımları, Netsis)

B. Elektronik Olmayan Ortamlar

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

IV. SAKLAMA ve İMHAYA İLİŞKİN AÇIKLAMALAR

AK ALÜMİNYUM tarafından; işbu Politika kişisel verilerinin işlediği herhangi bir sürece dâhil olan

Çalışan Adayı, Çalışan, Hissedar/Ortak, Potansiyel Ürün veya Hizmet Alıcısı, Tedarikçi Çalışanı, Tedarikçi Yetkilisi, Ürün veya Hizmet Alan Kişi, Ziyaretçi, Diğer (Çalışan Aile Bireyi ve Yakını, Referanslar, Veli/Vasi/Temsilci, İşbirliği İçinde Olduğumuz Kurumların Çalışanı/Yetkilisi/ Hissedarı), Kişisel Verilerini İşlediği Herhangi Bir Sürece Dâhil Olan Diğer 3. Kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

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

A. 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, **AK ALÜMİNYUM** faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

1. Saklamayı Gerektiren Hukuki Sebepler

- 2004 sayılı İcra İflas Kanunu
- 213 sayılı Vergi Usul Kanunu
- 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
- 6098 sayılı Türk Borçlar Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
- 6502 sayılı Tüketicinin Korunması Hakkında Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6769 sayılı Sınai Mülkiyet Kanunu
- Çalışanların İş Sağlığı ve Güvenliği Eğitimlerinin Usul ve Esasları Hakkında Yönetmelik
- Ekranlı Araçlarla Çalışmalarda Sağlık Ve Güvenlik Önlemleri Hakkında Yönetmelik
- İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
- İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği

- İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği
- Kişisel Koruyucu Donanımların İşyerlerinde Kullanılması Hakkında Yönetmelik
- Mesafeli Sözleşmeler Yönetmeliği
- Sosyal Sigortalar İşlemleri Yönetmeliği
- Ticaret Sicil Yönetmeliği
- Ücret, Prim, İkramiye ve Bu Nitelikteki Her Türlü İstihkakın Bankalar Aracılığıyla Ödenmesine Dair Yönetmelik
- Yıllık Ücretli İzin Yönetmeliği

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

2. Saklamayı Gerektiren İşleme Amaçları

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

- Acil Durum Yönetimi 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
- Eğitim Faaliyetlerinin 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
- İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
- İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- Lojistik Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
- Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
- Performans Değerlendirme Süreçlerinin Yürütülmesi

- Risk Yönetimi Süreçlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Talep / Şikâyetlerin Takibi
- Taşınır Mal ve Kaynakların Güvenliğinin Temini
- Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- Ücret Politikasının Yürütülmesi
- Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
- Yönetim Faaliyetlerinin Yürütülmesi
- Ziyaretçi Kayıtlarının Oluşturulması ve Takibi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Erişim Yetkilerinin Yürütülmesi
- Yatırım Süreçlerinin Yürütülmesi
- Diğer-Kurumsal Hafızanın Oluşturulması ve Korunması

B. İmhayı Gerektiren Sebepler

AK ALÜMİNYUM'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 saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- KVK Kurulu'na şikâyette 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 **AK ALÜMİNYUM** tarafından kabul edilmesi,

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

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

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 **AK ALÜMİNYUM** tarafından teknik ve idari tedbirler alınır.

A. Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Bilgi sistemleri güncel halde tutulmakta, kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışan için yetki matrisi oluşturulmuştur.
- Erişim yetki ve rol dağılımları için diğer düzenlemeler oluşturulmakta ve uygulanmaktadır.
- 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 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.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

B. 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/becerisi geliştirilmektedir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında diğer düzenlemeler hazırlanmış ve uygulamaya başlanmıştır. Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

- Diğer düzenlemelere uymayan Çalışan'a yönelik disiplin süreçleri uygulanmaktadır.
- İletişim teknikleri ve ilgili mevzuatlar hakkında eğitimler verilmektedir.
- Kişisel veri güvenliği diğer düzenlemeler ile 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 verileri işlemeye başlamadan önce İlgili Kişiler'i aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- 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.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik diğer düzenlemeler belirlenmiş ve uygulanmaktadır.
- İşbu Politika'ya uygun imha süreçleri tanımlanmakta ve uygulanmaktadır.

VI. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

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

A. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. **AK ALÜMİNYUM** 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.

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Kişisel veriler, **AK ALÜMİNYUM** tarafından veya gerekli görülür ise **AK ALÜMİNYUM**'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 anlaşabilir. 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.

B. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

a. Yerel Sistemler: Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır

b. Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

i) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

iii) Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c. **Kâğıt ve Mikrofiş Ortamları:** Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

d. **Bulut Ortamı:** Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir. Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

Kişisel veriler, **AK ALÜMİNYUM** tarafından aşağıda belirtilen yöntemlerle yok edilir.

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

C. 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. **AK ALÜMİNYUM**, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

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.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır. Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki tabloda gösterilmektedir:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	a. Değişkenleri Çıkartma b. Kayıtları Çıkartma c. Bölgesel Gizleme d. Genelleştirme e. Alt ve Üst Sınır Kodlama f. Global Kodlama g. Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	a. Mikro-Birleştirme b. Veri Değiş-Tokuşu c. Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler	a. K-Anonimlik b. L-Çeşitlilik c. T-Yakınlık

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri:

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

a. Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

b. Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır. Örneğin anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

c. Bölgesel Gizleme

Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az

görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

d. Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkansız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir. Örneğin TC Kimlik No xyx olan bir kişi e-ticaret platformundan çocuk bezi aldıktan sonra aynı zamanda ıslak mendil de almış olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan çocuk bezi alan kişilerin %xx'i aynı zamanda ıslak mendil de satın alıyor şeklinde bir sonuca ulaşılabilir.

e. Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

f. Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

g. Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır. Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri
Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak;

mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

a. Mikro Birleştirme

Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

b. Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

c. Gürültü Ekleme

Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler
Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir.
Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a. K-Anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır

b. L-Çeşitlilik

K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

c. T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

Bir veri anonim hale getirilirken, Şirketimiz kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmektedir.

Anonimlik Güvencesi

Şirketimiz, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilirken, anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması, bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması, anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi noktalarını dikkate almakta olup, Şirketimizce anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapılmakta ve anonimliğin korunduğundan emin olunmaktadır.

Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirmenin Bozulmasına Dair Risklerin Değerlendirilmesi ve Önlenmesi

Anonim hale getirme işlemi, kişisel verilere uygulanan ve veri kümesinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir. Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır. Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere “anonimliğin bozulmasına yönelik saldırılar” denilmektedir. Bu kapsamda, Şirketimizce anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği

tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmektedir.

VII. KİŞİSEL VERİ İŞLEME ŞARTLARININ ORTADAN KALKMASI HALİNDE YAPILACAKLAR

Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının oradan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir. Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi Şirket birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç altı aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildirimi üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır.

Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır. Merkezi Bilgi Sistemlerinde yer alan çok paydaşlı veri sahipliği bulunan kişisel verilerin imhasına yönelik karar alınması gerektiğinde ise Kişisel Verileri Koruma Komitesi'nin görüşü alınacak ve söz konusu kişisel veri hakkında işbu politikaya göre verinin saklanmasına veya silinmesine, yok edilmesine veya anonim hale getirilmesine ilgili veri sahibi iş birimi tarafından karar verilecektir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4.maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden Şirket 'e başvurarak kendisine ait kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini talep

ettiğinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Bu durumda detayları Prosedürde belirleneceği şekilde; talep, başvuru tarihinden itibaren en geç otuz gün içinde sonuçlandırılır ve ilgili kişiye bilgi verilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, ilgili veri sahibi iş birimi bu durumu derhal aktarım yapılan üçüncü kişiye bildirir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, kişisel veri sahiplerinin verilerinin silinmesi veya yok edilmesine yönelik talepleri Şirket tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı ilgili kişiye en geç 30 gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara yönlendirilecektir.

VIII. SAKLAMA ve İMHA SÜRELERİ

A. Saklama Süresi

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

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

AK ALÜMİNYUM 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.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde **AK ALÜMİNYUM** 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.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
AK ALÜMİNYUM Faaliyetleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşme Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlem Faaliyetleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekân Güvenliği (Kamera Kayıtları)	15 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem Güvenliği Faaliyetleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Sağlığı ve Güvenliği Süreçlerinin Yürütülmesi	15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kurumsal Hafıza Süreçlerinin Yürütülmesi	15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

B. İmha Süresi

Yönetmeliğin 11. maddesi gereğince **AK ALÜMİNYUM**, periyodik imha süresini **6 ay** olarak belirlemiştir. Buna göre, her yıl Mart ve Eylül aylarında periyodik imha işlemi gerçekleştirilir.

IX. 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 **AK ALÜMİNYUM**'da saklanır.

X. 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.

XI. POLİTİKANIN YÜRÜRLÜĞÜ

AK ALÜMİNYUM tarafından düzenlenen İşbu Politika, Ekim 2021 tarihinde yürürlüğe girmiş olup, Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda gerekli güncellemeler yapılacaktır. İşbu Politika'nın uygulanmasını, güncellenmesini, duyurulmasını **Komite** yürütür.