AKSU MADENCİLİK SANAYİ VE ELEKTRİK ÜRETİM TİCARET A.Ş
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. Bu politikanın amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

2. Bu politika; 6698 sayılı Kanunun 7 nci maddesinin üçüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliğine uygun olarak hazırlanmıştır.

3. Şirket; Kişisel veri işleme envanterine uygun olarak bu kişisel veri saklama ve imha politikasını hazırlamıştır.

4. Tanımlar

4.1. **Alıcı grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

4.2. **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 kişileridir

4.3. **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

4.4. **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 ortamı ifade eder.

4.5. **Kişisel veri işleme 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 envanterdir.

4.6. **Kişisel veri saklama ve imha politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

4.7. **Periyodik imha:** 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 işlemini ifade eder.

4.8. **Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.

4.9. **Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

4.10. **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

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

4.12. **Kişisel verilerin yok edilmesi** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.13. **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, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

5. Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamları :

5.1. Kağıt ortamlar
- **5.1.1.** Kağıt
- **5.1.2.** Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)
- **5.1.3.** Yazılı, basılı, görsel ortamlar

5.2. Elektronik ortamlar
- **5.2.1.** Sunucular (Etki alanı, yedekleme, e-posta,
- **5.2.2.** veritabanı, web, dosya paylaşım, vb.)
- **5.2.3.** Yazılımlar
- **5.2.4.** Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
- **5.2.5.** Kişisel bilgisayarlar (Masaüstü, dizüstü)
- **5.2.6.** Mobil cihazlar (telefon, tablet vb.)
- **5.2.7.** Optik diskler (CD, DVD vb.)
- **5.2.8.** Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
- **5.2.9.** Yazıcı, tarayıcı, fotokopi makinesi

6. Saklamayı Gerektiren Hukuki Sebepler

6.1. 6698 sayılı Kişisel Verilerin Korunması Kanunu,
6.2. 6098 sayılı Türk Borçlar Kanunu,
6.3. 4734 sayılı Kamu İhale Kanunu,
6.4. 657 sayılı Devlet Memurları Kanunu,
6.5. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
6.6. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar
6.7. Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
6.8. 5018 sayılı Kamu Mali Yönetimi Kanunu,
6.9. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
6.10. 4982 Sayılı Bilgi Edinme Kanunu,

6.11. 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun
6.12. 4857 sayılı İş Kanunu,
6.13. 2547 sayılı Yükseköğretim Kanunu,
6.14. 5434 sayılı Emekli Sağlığı Kanunu,
6.15. 2828 sayılı Sosyal Hizmetler Kanunu
6.16. İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
6.17. Arşiv Hizmetleri Hakkında Yönetmelik
6.18. Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

7. Saklamayı Gerektiren İşleme Amaçları

7.1. Acil Durum Yönetimi Süreçlerinin Yürütülmesi
7.2. Bilgi Güvenliği Süreçlerinin Yürütülmesi
7.3. Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
7.4. Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
7.5. Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
7.6. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
7.7. Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
7.8. Denetim / Etik Faaliyetlerinin Yürütülmesi
7.9. Eğitim Faaliyetlerinin Yürütülmesi
7.10. Erişim Yetkilerinin Yürütülmesi
7.11. Faaliyetlerin Mevzuata Uygun Yürütülmesi
7.12. Finans Ve Muhasebe İşlerinin Yürütülmesi
7.13. Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
7.14. Fiziksel Mekan Güvenliğinin Temini
7.15. Görevlendirme Süreçlerinin Yürütülmesi
7.16. Hukuk İşlerinin Takibi Ve Yürütülmesi
7.17. İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
7.18. İletişim Faaliyetlerinin Yürütülmesi
7.19. İnsan Kaynakları Süreçlerinin Planlanması
7.20. İş Faaliyetlerinin Yürütülmesi / Denetimi
7.21. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
7.22. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
7.23. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
7.24. Lojistik Faaliyetlerinin Yürütülmesi
7.25. Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
7.26. Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
7.27. Mal / Hizmet Satış Süreçlerinin Yürütülmesi
7.28. Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
7.29. Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
7.30. Organizasyon Ve Etkinlik Yönetimi
7.31. Performans Değerlendirme Süreçlerinin Yürütülmesi
7.32. Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
7.33. Risk Yönetimi Süreçlerinin Yürütülmesi
7.34. Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
7.35. Sosyal Sorumluluk Ve Sivil Toplum Aktivitelerinin Yürütülmesi

7.36. Sözleşme Süreçlerinin Yürütülmesi
7.37. Sponsorluk Faaliyetlerinin Yürütülmesi
7.38. Stratejik Planlama Faaliyetlerinin Yürütülmesi
7.39. Talep / Şikayetlerin Takibi
7.40. Taşınır Mal Ve Kaynakların Güvenliğinin Temini
7.41. Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
7.42. Ücret Politikasının Yürütülmesi
7.43. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
7.44. Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
7.45. Yatırım Süreçlerinin Yürütülmesi
7.46. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
7.47. Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
7.48. Yönetim Faaliyetlerinin Yürütülmesi
7.49. Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

8. İmhayı Gerektiren Sebepler

8.1. Kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.

8.2. Türk Ceza Kanunu'nun 138. maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Şirket kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir.

8.3. İlgili kişi, Şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.

8.4. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

8.5. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.

8.6. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

9. Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler

9.1.1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
9.1.2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
9.1.3. Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
9.1.4. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
9.1.5. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

9.1.6. Erişim logları düzenli olarak tutulmaktadır.
9.1.7. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
9.1.8. Gizlilik taahhütnameleri yapılmaktadır.
9.1.9. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
9.1.10. Güncel anti-virüs sistemleri kullanılmaktadır.
9.1.11. Güvenlik duvarları kullanılmaktadır.
9.1.12. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
9.1.13. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
9.1.14. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
9.1.15. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
9.1.16. Mevcut risk ve tehditler belirlenmiştir.
9.1.17. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
9.1.18. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
9.1.19. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
9.1.20. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

10. Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler

10.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılır ve kayıt altına alınır.

10.2. Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

11. Kişisel Verilerin Silinmesi, Yok Edilmesi Ve Anonimleştirilmesi Teknikleri

11.1. **Fiziksel Olarak Yok Etme** Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Örnek: İlgili dosyanın, belgenin parçalanarak çöpe atılması.

11.2. **Yazılımdan Güvenli Olarak Silme** Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; çok yüksek ihtimalle bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

11.3. **Uzman Tarafından Güvenli Olarak Silme** Şirket bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

11.4. Kişisel Verileri Anonim Hale Getirme Teknikleri

11.4.1. Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Şirket, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

11.4.2. KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler

KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.

11.4.3. **Maskeleme (Masking)** Veri maskeleme, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, TC Kimlik No, ad, soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkansız hale geldiği bir veri setine dönüştürülmesi.

11.4.4. **Toplulaştırma (Aggregation)** Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.

11.4.5. **Veri Türetme (Data Derivation)** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehirin belirtilmesi.

11.4.6. **Veri Karma (Data Shuffling, Permutation)** Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

12. Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimleri ve görev tanımları:

12.1. ***Bilgi İşlem Birimi Yöneticisi;*** Şirketin tüm Bilgi İşlem süreçlerini yönetir.

12.2. ***Personel Müdürlüğü*** *(Personel ile ilgili konularda)*, Şirketin tüm personel süreçlerini yönetir.

13. Saklama ve imha sürelerini gösteren tablo

NO	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
1	Kimlik	15 YIL
2	İletişim	15 YIL
3	Lokasyon	6 AY
4	Özlük	15 YIL
5	Hukuki İşlem	10 YIL
6	Müşteri İşlem	10 YIL
7	Fiziksel Mekân Güvenliği	6 AY
8	İşlem Güvenliği	2 YIL
9	Risk Yönetimi	10 YIL
10	Finans	10 YIL
11	Mesleki Deneyim	15 YIL
12	Görsel ve İşitsel Kayıtlar	15 YIL
13	Sağlık Bilgileri	15 YIL
14	Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	15 YIL

***Yukarıdaki süreler, çalışanlar için iş sözleşmesinin feshi tarihinden, tedarikçi ve müşteriler için sözleşmenin sona erme tarihinden veya sözleşme yoksa son işlemin yapıldığı tarihten, diğer ilgili kişiler için kişisel verilerin elde edilme tarihinden itibaren başlar.**

14. Periyodik imha süreleri,

14.1. Şirket saklama süresi dolan kişisel verileri saklama süresinin dolduğu tarihten itibaren en geç 180 gün içerisinde imha eder.

14.2. Şirket; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

14.3. Periyodik imhanın gerçekleştirileceği zaman aralığı veri sorumlusu tarafından kişisel veri saklama ve imha politikasına, prosedürlere ve şirketin iş akışına uygun olarak belirlenir. Bu süre her halde altı ayı geçemez.

15. Politikanın Yayınlanması ve Saklanması

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır.

16. Güncelleme Periyodu

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

17. Yürürlük

Politika, Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Veri Sorumlusu Unvan: AKSU MADENCİLİK SANAYİ VE ELEKTRİK ÜRETİM TİCARET A.Ş

Mersis no : 8458 2516 4621 3678

E-posta adresi : personel@aksugroup.com

Kayıtlı Elektronik Posta Adresi: aksu.madencilik@hs03.kep.tr

E Tebligat Adresimiz : 25999-16990-56660

Fiziki Posta adresi : Mebusevleri Mahallesi İller cad. No:5 06570 Çankaya ANKARA