

ALMET ALÜMİNYUM LTD. ŞTİ.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

2020 İstanbul

İçindekiler

I.	Politika Amaç ve Kapsamı	1
II.	İlgili Mevzuat ve Diğer Belgeler	1
III.	Tanımlar	1
IV.	Genel Saklama Prensipleri	2
	Saklama Süresi	2
	Saklama Kuralları ve Tedbirler	2
V.	Kişisel Verilerin İmhası.....	3
	Genel Olarak Kişisel Verilerin İmha Şartları	3
	Kişisel Verilerin İmha Teknikleri	3
	Periyodik İmha	3
VI.	Politika Sorumluları	3
VII.	Politika'ya Uyum.....	3
VIII.	Yürürlük.....	3
	Ek-1: Saklama ve İmha Süreleri Tablosu.....	4
	EK-2: Özel Nitelikli Kişisel Verilerin İşlenmesi Prosedürü.....	5

I. Politika Amaç ve Kapsamı

Kişisel verilerin güvenliği Almet Alüminyum Ltd. Şti. (Şirket) için büyük önem taşımakta olup, kişisel verilerin mevzuatı öngördüğü şartlara uygun olarak, mümkün olan en güvenli şekilde ve hukuki yükümlülüklerin gerektirdiği süreyle işlenmesi ve mevzuata uygun koşullarda saklanması Şirket Kimya açısından yüksek önemi halizdir. Bu bağlamda Şirket, kişisel verilerin işlenmesi açısından mevzuata uygun hareket etmesi ve uyumluluğu tesis etmesi hukuka uygunluk açısından oldukça önemlidir.

6698 sayılı Kişisel Verilerin Korunması Kanununun 16'ncı maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5'inci maddesi kapsamında hazırlanan işbu Kişisel Veri Saklama ve İmha Politikası'nın ("Politika") amacı, Şirket tarafından işlenen,ürün veya hizmet alan kişi, çalışanlar, aday çalışanlar ve diğer üçüncü kişilerin kişisel verilerinin, gerekli saklama sürelerini ve imha edilmelerinde uygulanacak asgari standartları belirlemektir.

İşbu Politika kapsamındaki tüzel kişilik Almet Alüminyum Ltd. Şti.'dir.

İşbu Politika, veri sorumlusu Şirket'in işlediği kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak teşkil etmektedir.

İşbu politika, Şirket'in tüm birimlerine, süreçlerine ve diğer üçüncü kişilerle ilişkilerine uygulanır. Bu Politika tüm Şirket yöneticilerine, çalışanlarına, danışmanlara, hizmet sağlayıcılara ya da veri toplayabilen, işleyebilen ya da verilere erişebilen (kişisel verileri ve/veya özel nitelikli kişisel verileri içeren) hizmet sağlayıcılara uygulanır.

İşbu Politika Şirket tarafından toplanan tüm kişisel verilere ve bilgilere uygulanır. İşbu Politika ile düzenlenen ve kişisel verilerin yer aldığı, elektronik ve elektronik olmayankayıtlı ortamları ve/veya belgeler şunlardır:

- Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.)
- Yazılımlar (ofis yazılımları, portal)
- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti-virüs vb.)
- Kişisel bilgisayarlar (masaüstü, dizüstü)
- Mobil cihazlar (telefon, tablet vb.)
- Optik diskler (CD, DVD, Blu-Ray vb.)
- Çıkarılabilir bellekler (USB, Hafıza Kart, Taşınabilir Bellek vb.)
- Yazıcı, tarayıcı, fotokopi makinesi.
- Basılı ortamdaki bilgi ve belgeler,
- Video ve ses kayıtları,
- Fiziksel erişim kontrol sistemleri tarafından üretilen veriler.

II. İlgili Mevzuat ve Diğer Belgeler

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
- 30 Aralık 2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik
- 10 Mart 2018 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
- 6098 sayılı Türk Borçlar Kanunu
- 4857 sayılı İş Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- Şirket Grup Kişisel Verilerin Korunması ve İşlenmesi Politikası
- Kişisel Verilerin Korunması Mevzuatı İlgili Kişi Başvuru Prosedürü

III. Tanımlar

Bu Politika'da yer alan terimler, aşağıda yer verilen anlamları ifade eder.

Tanım	Açıklama
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 kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
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 veya KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirilerek 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
Kurum	Kişisel Verileri Koruma Kurumu
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler
Periyodik İmha	Kanunda 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 işlemidir.
Şirket	Almet Alüminyum Ltd. Şti.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun 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 kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)	Veri sorumlularının Sicile başvuru ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kurum tarafından oluşturulan ve yönetilen bilişim sistemi.
Yönetmelik	28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

IV. Genel Saklama Prensipleri

Saklama Süresi

Şirket, kişisel veri saklama süresi boyunca saklanması gereken belgeler ve elektronik kayıtlar için süre tanımını Ek-1'de yer alan Saklama ve İmha Süreleri Tablosu'nda yapar ve günceller.

Bu Politika ve ekinde aksi belirtilmedikçe, Şirket Kişisel Veri İşleme Envanteri'ndeki veri kategorilerinde yer alan kişisel veriler, kural olarak ilgili kişisel verinin elde edildiği tarihten itibaren Ek-1'de belirtilen süreler ile saklanır.

İstisnai olarak, veri saklama süreleri aşağıdaki durumlarda uzatılabilir:

- Resmi mercilerce yürütülen soruşturma veya araştırmalarda talep edilmesi halinde ve/veya Şirket'in hukuki yükümlülüğü veya yasal haklarının gerektirdiği hallerde;
- Yargılama veya sair yasal süreçlerinde yürürlükteki mevzuat kapsamındaki hakların kullanılması için gerektiği hallerde.

Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken;

- İlgili veri kategorisinin işleme amacı kapsamında Şirket'in faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
- İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
- İlgili veri kategorisinin işleme amacına bağlı olarak Şirket'in elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
- İlgili veri kategorisinin işleme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukukun devam edeceği süre,
- Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
- Şirket'in hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,
- Şirket tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zaman aşımı süresi,

dikkate alınır.

Şirket, kişisel verilerin işlendikleri amaç için gerekli olan azami süreleri belirlerken ve uygulamada, söz konusu süreleri Şirket Kişisel Veri İşleme Envanteri'nde yer alan bilgilerle uyumunu ve azami sürelerin aşılmadığını takip eder. Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamında tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıttadır;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi tatbik edilir.

Saklama Kuralları ve Tedbirler

Kişisel verilerin saklanması sürecinde, ilgili kişisel verinin saklama veya arşivleme için kullanılan veri ortamının (yazılı, dijital vb.) yıpranma ihtimali göz önünde bulundurulur. Eğer kişisel verilerin elektronik ortamda depolama yöntemi ile saklanması seçilmiş ise, ağ bileşenleri arasında saklama süresince sınırlı ve sadece yetkili kişilerce erişim sağlanır.

Şirket'te yer alan cihazlarda ya da kağıt ortamında saklanan kişisel veriler, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunur. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamlar da dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunur. Bu ortamlara giriş / çıkışlar kontrol altına alınır.

Aynı seviyedeki önlemler, Şirket dışında yer alan ve Şirket' ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınır.

Şirket'in işlenen kişisel verilerin güvenliğine yönelik almış olduğu tedbirlere aşağıda yer verilmektedir:

- Şirket tarafından, sızma testleri ile bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler Şirket tarafından sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile güvenlik tanımları aracılığı ile yapılmaktadır.
- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişi sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygun olmayan erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde de durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanması sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlanmıştır.
- Özel nitelikli kişisel verilerin güvenliğine yönelik, İşbu Politikaya ek, "EK-2 Özel Nitelikli Kişisel Verilerin İşlenmesi Prosedürü" adıyla ayrı bir politika belirlenmiştir.

V. Kişisel Verilerin İmhası

Genel Olarak Kişisel Verilerin İmha Şartları

Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, resen veya ilgili kişinin talebi üzerine Şirket tarafından silinir, yok edilir veya anonim hale getirilir. Buna göre;

- Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Şirket ile ilgili kişi arasındaki sözleşmenin kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanunun 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyetle bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılabacak herhangi bir şartın mevcut olmaması,
- Kanunun 5 ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,

hallerinde kişisel verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi gerekir.

Kişisel Verilerin İmha Teknikleri

Kişisel verilerin silinmesi;söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, silinen kişisel verilerin ilgili kullanıcılar tarafından erişilemez ve tekrar kullanılamaz olmasını temin eder.

Şirket tarafından kişisel verilerin silinmesi işleminde aşağıdaki süreç tatbik edilir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi;
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgilikullanıcıların 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.

Kayıt ortamlarına göre kişisel veriler aşağıdaki şekilde silme işlemine tabi tutulur:

- Sunucularda yer alan kişisel verilerden, saklanması gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
- Elektronik ortamda yer alan kişisel verilerden saklanması gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
- Fiziksel ortamda tutulan kişisel verilerden saklanması 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 verilerden saklanması gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Yok etme;bilgilerin saklandığı veri saklamaya elverişli tüm fiziksel kayıt ortamlarının tekrar geri getirilemeyecek ve kullanılmayacak hale getirilmesidir.

Kayıt ortamlarına göre kişisel veriler aşağıdaki şekilde yok etme işlemine tabi tutulur:

- Kağıt ortamında yer alan kişisel verilerden saklanması gerektiren süre sona erenler, kağıt kırma makinelerinde geri döndürülemez şekilde yok edilir.
- Optik medya ve manyetik medyada yer alan kişisel verilerden saklanması 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.

Kişisel verilerin anonim hale getirilmesi; kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Bu kapsamda, veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabilirse, bu verinin anonim hale getirildiği kabul edilemez.

Anonimleştirilen veri artık kişisel veri niteliklerine sahip olmayacağından, Kanun hükümlerine tabi olmayacaktır. Veri setleri anonimleştirme işlemlerine tabi tutuldukları ana kadar kişisel veri niteliklerine sahip olduklarından, bu veriler üzerinde gerçekleştirilecek her türlü işlem kişisel verilerin işlenmesi olarak kabul edilmektedir.

Kişisel verilerin silinmesi, yok edilmesi ve 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.

Periyodik İmha

Şirket bünyesinde işlenen kişisel veriler, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11'inci maddesi uyarınca, ilgili takvim yılının ilk günü itibarıyla altı ayda bir periyodik imha işlemine tabi tutulur.

İşbu Politika kapsamında, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinir, yok edilir veya anonim hale getirilir.

İlgili kişinin, KVKK'nın 13'üncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep etmesi halinde;

- 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.
- 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 ve ilgili mevzuat kapsamında gerekli işlemlerin yapılmasını temin eder.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

VI. Politika Sorumluları

İşbu Politika'nın hazırlanması, güncellenmesi ve uygulanmasından Şirket bünyesinde kişisel verilerin tutulduğu, işlendiği ve/veya aktarıldığı sistemleri kullanan/yöneten birimler ve ilgili çalışanlar sorumludur. Bu bağlamda Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğinin sağlanmaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Özel olarak, İnsan Kaynakları Birimi çalışanların politikaya uygun hareket etmesinden; Bilgi Teknolojileri Birimi Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumlu olup, bahse konu her iki birim ayrıca Politika'nın geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi açısından yetkili ve görevlidir.

VII. Politika'ya Uyum

Tüm Şirket çalışanları, kişisel verilerin işlenmesi ve muhafazası sırasında Politika hükümlerine tam ve gereği gibi riayet etmekle mükellef olup, mezkûr politika çalışanların iş sözleşmelerinin ayrılmaz bir parçasını teşkil etmektedir.

Bu Politika'da yer alan hükümlerin ihlaline ilişkin somut emarelerin varlığı halinde Şirket yönetim organı şüphelenilen Politika ihlallerini araştırarak gerekli tedbirleri alır. İşbu politikaya uyulmaması, müşteri güven kaybı, dava, prestij kaybı, finansal kayıp ve Şirket itibarına zarar veya kişisel zarar dahil ve bunlarla sınırlı olmaksızın çeşitli olumsuz sonuçlara neden olabilir. Bu sebeple, bu politikaya herhangi bir şekilde uyulmaması Şirket çalışanları ya da ilgili sair kişiler hakkında disiplin soruşturması veya işin ya da sözleşmenin sona ermesi ile sonuçlanabilir. Anılan ihlal aynı zamanda dahil olan kişiler aleyhine hukuki işlemde bulunulmasına dahi yol açabilir.

VIII. Yürürlük

Kişisel verilerin işlenmesi faaliyetlerinde yürürlükteki mevzuata tam uyumluluk hedefiyle tarafından hazırlanan İşbu Politika, Şirket yönetimi organı tarafından onaylanarak yürürlüğe girmiştir.

Politika, basılı kağıt ve elektronik ortamda olmak üzere iki farklı ortamda yayınlanır. İç iletişime özgünlük elektronik ortamda çalışanlara açıklanır, basılı kağıt nüshası da İnsan Kaynakları Departmanında saklanır. Politika, ihtiyaç hasıl oldukça gözden geçirilir ve gerektiğinde ilgili bölümler güncellenir.

Ek-1: Saklama ve İmha Süreleri Tablosu

İlgili Süreç ve Veri Kategorisi	Saklama Süresi	Açıklama
Çalışanlara ait kişisel sağlık verileri	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	İş akdinin devamında ve hitamından itibaren olası meslek hastalığı/iş kazası tespit ve ihbarı ihtimaline karşılık 10 yıl süreyle saklanmaktadır.
Çalışanların işe alım dosyaları, özlük verileri	İş ilişkisinin sona erme tarihinden itibaren 30 yıl	Akdin kurulması için kullanılan veriler; olası bir hizmet/ücret tespiti talebi ile Sosyal Güvenlik Kurumu'nun alacak talebine istinaden hizmet akdinin devamınca ve hitamından itibaren 30 yıl süreyle muhafaza edilir.
Çalışan aday başvuru formları, özgeçmişleri	Başvuru tarihinden itibaren 1 yıl	En fazla 2 yıl olmak üzere özgeçmişin ve başvuru formlarının güncelliğini kaybedeceği süre kadar saklanır.
İş sağlığı ve güvenliği uygulamaları kapsamında elde edilen kişisel veriler	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	İş akdinin taraflara yüklediği sorumluluklar kapsamında herhangi bir sağlık sorunu iddiasına karşılık iş ilişkisinin sona erme tarihinden itibaren 15 yıl süre ile saklanır.
Potansiyel müşteri bilgileri	Bilgilerin alındığı tarihten itibaren 5 yıl	Satış sözleşmesinin kurulabilmesi için aday müşterilerden elde edilen veriler 5 yıl müddetle muhafaza edilmektedir.
Müşteri talep ve şikâyet yönetimi sırasında elde edilen veriler	İlk kaydın yapıldığı tarihten itibaren 5 yıl	Hizmetin devamını, kalitesini artırmak ve alıcının taleplerini değerlendirmek amacıyla alınan kişisel veriler ilk kaydın yapıldığı tarihten itibaren 5 yıl süre ile saklanmaktadır.
Finansal/Ödeme işlemlerine ait kayıtlar	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Akdin taraflara yüklediği yükümlülükler altında çalışanlara ücret ödemek için alınan veriler 10 yıl süre ile saklanmaktadır.
Şirkete ve şirketin projelerine ilişkin bilgiler	Bilgilerin alındığı tarihten itibaren 10 yıl	Şirketin ve şirketin proje süreçlerine ilişkin kişisel veriler 10 yıl müddetle saklanmaktadır.
Şirket'in iş birliği içinde olduğu firmalar/kurumlar ile paylaşılan bilgiler	İş akdi süresince ve bitiminden itibaren 10 yıl	İş akdi süresince aktarılan veriler ilgili iş süresince ve bitiminden itibaren sözleşme zaman aşımı olarak belirtilen 10 yıl süre ile saklanmaktadır.
Satış sözleşmesinin muhafazası	İş ilişkisinin sona ermesinden itibaren 10 yıl	Sözleşmeden doğabilecek itirazlar için sözleşme zaman aşımı süresince saklanmaktadır.
Üçüncü kişilerle imzalanan sözleşmeler	Sözleşmenin sona ermesinden itibaren 10 yıl	Sözleşme ilişkisi gereği 10 yıllık zaman aşımı süresince saklanmaktadır.
Çalışanlar için yurtiçi ve yurtdışı organizasyonları düzenlenmesi için alınan veriler	Organizasyonun sona ermesini takiben 5 yıl	Alınan veriler şirketin yurtiçi ve yurtdışında temsil edilebilmesi için alınmakta ve 5 yıl süre ile muhafaza edilmektedir.

Çalışan eğitimleri ve çalışan performans değerlendirmesi için alınan veriler	İş akdi süresince ve sona ermesini takiben 10 yıl	İş akdi kapsamında, çalışanların performans süreçlerini takip etmek, iş hayatındaki eksiklerini tamamlamak için eğitimler düzenlenmek amacıyla elde edilen kişisel veriler 10 yıl süre saklanmaktadır.
Çalışanlara araç tahsis edilmesi	Araç kullanımının bitimini takiben 10 yıl	İş ilişkisinden doğan yükümlülükleri ifa etmek amacıyla çalışanlara araç tedarik edilmesi için alınan kişisel veriler 10 yıl süre ile saklanmaktadır.
Sosyal medya süreçleri (çekiliş vb.) sırasında alınan veriler	Süreç bitimini takiben 10 yıl	İlgili sözleşme kapsamında veriler 10 yıl saklanır.
Kablosuz internet hizmet kullanımına ilişkin veriler	İlk kaydın yapıldığı tarihten itibaren 5 yıl	İnternet erişim hizmetinin sağlanması için elde edilen veriler yasa gereği 5 yıl süre ile saklanmaktadır.
Log kayıt takip sistemleri	Kaydın alındığı tarihten itibaren 2 yıl	İnternet erişim hizmetinin güvenli bir ortamda sağlanması amacıyla elde edilen kişisel veriler yasa gereği 2 yıl müddetle saklanmaktadır.
Güvenlik kamerası kayıtları	30 gün	İş yeri güvenliğini sağlamak amacıyla 30 gün süre ile muhafaza edilmektedir.

EK-2: Özel Nitelikli Kişisel Verilerin İşlenmesi Prosedürü

Özel nitelikli kişisel veriler öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle, diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir. Özel nitelikli kişisel veriler ilgili kişinin açık rızası ile ya da Kanunda sayılan sınırlı hallerde işlenebilir.

Kanunda özel nitelikli kişisel veriler, sınırlı sayma yoluyla belirlenmiştir. Bunlar; 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 verileridir. Özel nitelikli kişisel verilerin kıyas yoluyla genişletilmesi mümkün değildir.

Kanun, özel nitelikli kişisel veriler arasında da bir ayırım yapmıştır. Buna göre sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi ile bunlar dışındaki özel nitelikli kişisel verilerin, açık rıza olmaksızın işlenebileceği haller farklı düzenlenmiştir.

Kanuna göre, özel nitelikli kişisel verilerin işlenmesi, ilgili kişinin açık rızası dışında aşağıdaki hallerde mümkündür:

- Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde,
- Sağlık ve cinsel hayata ilişkin kişisel veriler, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilir.

Özel Nitelikli Kişisel Verilerin İşlenmesi Sırasında Alınacak Tedbirler

Şirket'in işlenen özel kişisel verilerin güvenliğine yönelik alınması gereken tedbirlere aşağıda yer verilmektedir:

- Şirket bünyesinde, özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler düzenlenir, iş sözleşmelerinde gizlilik maddelerine yer verilir ve verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilir, kriptografik anahtarlar güvenli ortamlarda tutulur;
- Tüm işlem kayıtları loglanır;
- Ortamların güvenlik güncellemeleri sürekli takip edilir;
- Gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanır;
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınır ve fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenir.
- Özel nitelikli kişisel verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmalıdır.
- Özel nitelikli kişisel veriler taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmeli ve kriptografik anahtar farklı ortamda tutulmalıdır.
- Farklı fiziksel ortamlardaki sunucular arasında özel nitelikli kişisel veri aktarımı gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmelidir.
- Kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmalı ve evrak "gizli" formatta gönderilmelidir.