AKSOY GRUP ŞİRKETLERİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

AKSOY GRUP ŞİRKETLERİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI
BİLGİ FORMU

Doküman İsmi:
Aksoy Grup Şirketleri Kişisel Veri Saklama ve İmha Politikası

Hedef Kitle:
Aksoy Girişimcilik Enerji ve Turizm Anonim Şirketi, Aksoy Taşınmaz Yatırımları Anonim Şirketi, Aksoy International Dış Ticaret Anonim Şirketi, Aksoy International Holding Anonim Şirketi ve Aksoy Holding Anonim Şirketi tarafından kişisel verileri işlenen çalışanları dışındaki tüm gerçek kişiler.

Hazırlayan:
Aksoy Girişimcilik Enerji ve Turizm Anonim Şirketi, Aksoy Taşınmaz Yatırımları Anonim Şirketi, Aksoy International Dış Ticaret Anonim Şirketi, Aksoy International Holding Anonim Şirketi, Aksoy Holding Anonim Şirketi.

Versiyon:
1.0

Onaylayan:
Üst Yönetim

Yürürlük Tarihi:
11.01.2023

Politika'nın hazırlanmış olduğu Türkçe dilindeki hali ile herhangi bir çeviri hali arasında bir uyuşmazlık çıktığı hallerde, Türkçe metni dikkate alınmalıdır.

İçindekiler

AKSOY GRUP ŞİRKETLERİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

Kişisel verilerin korunması, Aksoy Grup Şirketleri ("**Şirketler**") (**Aksoy Girişimcilik Enerji ve Turizm Anonim Şirketi, Aksoy Taşınmaz Yatırımları Anonim Şirketi, Aksoy International Dış Ticaret Anonim Şirketi, Aksoy International Holding Anonim Şirketi ve Aksoy Holding Anonim Şirketi**) için büyük önem arz etmekte olup, bu konuda azami hassasiyet gösterilmektedir. Bu doğrultuda, kişisel verilerin kişilerin beklentileri ile tutarlı bir şekilde ve yasalara uygun olarak işlenmesi, Şirketlerimizin temel yapı taşlarından biridir.

Bu bakımdan Şirketler, faaliyetleri sırasında elde etmiş olduğu kişisel verileri başta Anayasa olmak üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**"), Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") ve diğer ilgili mevzuata uygun şekilde hazırlanan işbu Aksoy Grup Şirketleri Kişisel Veri Saklama ve İmha Politikası'nda ("**Politika**") belirtilen genel prensipler ve düzenlemelere uygun şekilde saklamakta ve imha etmektedir.

2. POLİTİKA'NIN AMACI VE KAPSAMI

İşbu Politika ile Şirketler, Kanun kapsamındaki kişisel veri işleme faaliyetlerine konu gerçek kişi verilerinin saklanması ve imha edilmesine ilişkin Şirketler'in genel ilke ve prensiplerinin ortaya konulması ve bu hususlarla ilgili mevzuatla belirlenen yükümlülüklerin yerine getirilmesi hedeflemiştir.

İşbu Politika, Şirketler'in Kanun kapsamındaki veri işleme faaliyetlerine konu tüm kişisel verileri kapsamaktadır. Ayrıca, işbu Politika'da aksi belirtilmedikçe, Politika ile atıf yapılan dokümanlar hem basılı hem de elektronik kopyaları kapsamaktadır.

3. TANIMLAR

İşbu Politika'da içerik aksini gerektirmedikçe:

"**Açık Rıza**"	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza,
"**Alıcı Grubu**"	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi,
"**Anayasa**"	Türkiye Cumhuriyeti Anayasası,
"**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,

"Karartma"	Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri,
"**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 (örn. ad-soyadı, TCKN, e-posta, adresi, doğum tarihi, kredi kartı numarası, banka hesap numarası - *Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir*),
"**İlgili Kişi**"	Kişisel verisi işlenen gerçek kişi,
"**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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,
"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 getirilmesi,
"Kişisel Verilerin Silinmesi"	Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi,
"Kişisel Verilerin Yok Edilmesi"	Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,
"**Kurul**"	Kişisel Verileri Koruma Kurulu,
"**Maskeleme**"	Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,
"**Özel Nitelikli Kişisel Veri**"	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler,
"**Periyodik İmha**"	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda işbu Politika'da belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi,
"**Veri kayıt sistemi**"	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
"**Veri Sorumlusu**"	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten kişi

anlamına gelmektedir.

4. POLİTİKA İLE DÜZENLENEN KAYIT ORTAMLARI

Şirketler, Kanun kapsamındaki veri işleme faaliyetlerine konu tüm kişisel verileri, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu ve aşağıda belirtilen ortamlarda saklamaktadır:

Kişisel veriler Şirketler'in veri tabanlarında, e-posta hesaplarında, dosya sunucularında (fileserver), sharepoint siteleri, kağıt ortamı, son kullanıcının kullanımına tahsis edilmiş bilgisayarlarında bulunmaktadır.

Fiziksel Kayıtlar:
Kâğıt dokümanlar veya hidrokarbon örnekler gibi fiziksel kayıtlar. Söz konusu kayıtlar, fiziksel eşya ve fiziksel eşyaları tanımlayan metaveriyi içermektedir.

Elektronik Ortamlar:
E-posta ve elektronik çizelge gibi elektronik dokümanlar. Kayıt, elektronik doküman ve elektronik dokümanı tanımlayan metaveriyi içermektedir. Hem doküman hem dokümanı tanımlayan metaveri Exchange Server, File Server ve LOGO Uygulaması içerisinde saklanmaktadır.

Uygulama Kayıtları:
Müşteri verileri gibi elektronik yapısal veri kayıtları. Yapı, düzen ve kayıtta tutulan veri unsurlarının toplulaştırılmış olarak sunumunu tanımlayan metaveriyi (tüm kayıt unsurları okunabilir duruma getirildiğinde) de içeren ve kaydın bütünlüğünü sağlayacak şekilde tüm veri unsurlarından oluşturmaktadır. Her bir tür kayıt için metaveri; bibliyografik, yönetimsel, denetim ve erişim verilerini içermektedir.

5. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

Şirketler, kişisel veri işleme faaliyetlerinde aşağıdaki ilkeleri esas almaktadır:

- Hukuka ve dürüstlük kuralına uygun olunması,
- Kişisel verilerin doğru ve gerektiğinde güncel olmasını sağlama,
- Belirli, açık ve meşru amaçlarla işleme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ve
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme.

Şirketler, kişisel verileri, yukarıda bahsi geçen ilkelerle uyumlu şekilde, Aksoy Grup Şirketleri Kişisel Verilerin Korunması ve İşlenmesi Politikası ile Aksoy Grup Şirketleri Çalışan Kişisel Verilerinin Korunması ve İşlenmesi Politikası'nın ilgili maddelerinde yer alan kişisel veri işleme amaçlarıyla ve aşağıda belirtilen Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarına istinaden kişisel verileri saklamakta ve kullanmakta olup, söz konusu şartların tamamının ortadan kalkması halinde, kişisel verileri re'sen veya ilgili kişinin talebi üzerine imha etmektedir.

(a) İlgili Kişinin Açık Rızasının Bulunması

Kişisel verilerin işlenme şartlarından biri ilgili kişinin açık rızasıdır. İlgili kişinin açık rızası belirli bir konuya ilişkin, bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklanmalıdır.

(b) Kanunlarda Açıkça Öngörülmesi

İlgili kişinin kişisel verileri, kanunlarda açıkça öngörülmesi halinde açık rızası alınmadan hukuka uygun olarak işlenebilecektir.

(c) Fiili İmkansızlık Sebebiyle İlgili Kişinin Açık Rızasının Alınamaması

Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınamayacak olan kişinin kendisinin ya da başka bir kişinin hayatı veya beden bütünlüğünü korumak için kişisel verisinin işlenmesinin zorunlu olması halinde ilgili kişinin kişisel verileri işlenebilecektir.

(d) Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde kişisel verilerin işlenmesi mümkündür.

(e) Hukuki Yükümlülük

Şirketler'in hukuki yükümlülüklerini yerine getirmesi için veri işlemenin zorunlu olması halinde ilgili kişinin verileri işlenebilecektir.

(f) İlgili Kişinin Kişisel Verisini Alenileştirmesi

İlgili kişinin, kişisel verisini kendisi tarafından alenileştirmiş olması halinde ilgili kişisel veriler alenileştirme amacıyla sınırlı olarak işlenebilecektir.

(g) Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde ilgili kişinin kişisel verileri işlenebilecektir

(h) Şirketlerin Meşru Menfaati İçin Veri İşlemenin Zorunlu Olması

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketler'in meşru menfaatleri için veri işlemesinin zorunlu olması halinde ilgili kişinin kişisel verileri işlenebilecektir.

Bu doğrultuda, kişisel veri işleme faaliyetinin dayanağı yukarıda belirtilen şartlardan yalnızca biri olabildiği gibi bu şartlardan birden fazlası da aynı kişisel veri işleme faaliyetinin dayanağı olabilmektedir.

6. KİŞİSEL VERİLERİN İMHA EDİLMESİ İŞLEMİ İLE İLGİLİ UYGULANAN YÖNTEMLER VE KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Şirketler, Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verileri aşağıdaki yöntemlerle silmekte, yok etmekte veya anonim hale getirmektedir. Şirketler, kişisel verilerin imhasında azami dikkat ve özeni göstermektedir. Bu kapsamda Şirketler, Kanun'un 12'nci maddesi ve Yönetmelik hükümleri, yukarıda belirtilen genel ilkeler ile işbu Politika ve Kurul kararları uyarınca aşağıda belirtilen

hususlar ile ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır. İmha kapsamında gerçekleştirilen tüm işlemler Şirketler tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanmaktadır. Şirketler, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını teknolojik imkanlar ve uygulama maliyetine göre seçmekte olup, ilgili kişinin talebi halinde uygun yöntemin gerekçesini açıklamaktadır.

(a) Kişisel Verilerin Silinme Yöntemleri

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketler, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda Şirketler, kişisel verileri silme işlemi için aşağıdaki yöntemleri uygulamaktadır:

(i) Hizmet olarak Uygulama Türü Bulut Çözümleri (Office 365, Salesforce, Dropbox)

SPK Mevzuatı gereği bulut yapılar kullanılmadığı için Bulut sistemler üzerinde uygulanan Bir çözüme ihtiyaç duyulmamıştır.

(ii) Merkezi Sunucuda Yer Alan Ofis Dosyaları

Merkezi sunucularda yer alan veri sınıflandırması matrisinde hassas veri olarak tanımlanan veriler belli periyotlar ile taranmakta ve veri sahiplerine raporlanmaktadır. Veri sahiplerinin KVKK yükümlülüklerine göre gerekli süreci tamamlaması talep edilmektedir.

(iii) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile manuel olarak silinmesi veya anonim hal getirilmesi işlemi yapılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

(b) Kişisel Verilerin Yok Edilme Yöntemleri

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketler, kişisel verilerin yok edilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda Şirketler, kişisel verileri yok etme işlemi için aşağıdaki yöntemleri uygulamaktadır:

(i) Yerel Sistemler

De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemleri kullanılmaktadır.

(ii) Çevresel Sistemler

• Ağ cihazları (switch, router vb.)
• Flash tabanlı ortamlar
• Manyetik bant
• Manyetik disk gibi üniteler
• Mobil telefonlar
• Optik diskler
• Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri
• Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri
• Kâğıt ve mikrofiş ortamları
• Bulut ortamı

(c) Kişisel Verilerin Anonim Hale Getirilme Yöntemleri

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, Şirketler, 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 gerekmektedir. Şirketler, kişisel verilerin anonim hale getirilmesiyle ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli her türlü teknik ve idari tedbirleri almaktadır.

Bu kapsamda Şirketler, kişisel verileri anonim hale getirme işlemi için aşağıdaki yöntemleri uygulamaktadır:

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri	• Değişkenleri çıkartma • Kayıtları çıkartma • Alt ve üst sınır kodlama • Bölgesel gizleme • Örnekleme
Değer düzensizliği sağlayan anonim hale getirme yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme • Tekrar Örnekleme
Anonim hale getirmeyi kuvvetlendirici istatistik yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

7. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Şirketler, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi konusunda azami dikkat ve özeni göstermekte olup, Kanun'un 12'nci maddesi ve Yönetmelik hükümleri, yukarıda belirtilen genel ilkeler ile işbu Politika ve Kurul kararları uyarınca aşağıda belirtilen hususlar ile ilgili teknolojik imkanlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır:

➢ **Teknik Tedbirler**
- Veri kaybı/sızıntısı önleme (DLP): Kişisel verilerin, yanlışlıkla ya da kötü niyetli kişilerce kurum dışına çıkarılmasına engel olan ya da engel olmadan işlemi raporlamaya yarayan güvenlik yazılımı kullanılmaktadır - Güvenli giriş katmanı (SSL): Sunucu ile istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikalar kullanılmaktadır - Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılmakta ve tüm yapının güncel olması sağlanmaktadır. - Şifre Yönetimi - Yazılım envanteri takibi ve gerekli güncellemelerin yapılması, - Sistem seviyesinde LOG tutulması - Yılda bir kez detaylı bir şekilde sızma ve güvenlik kontrolü çalışmaları yapılmaktadır. Tespit edilen açıklar risk ve öncelik durumuna göre giderilmektedir. - Disk Şifreleme Yazılımları Kullanılmaktadır. - Mobile Device Management Yazılımları kullanılarak Mobil cihazlardaki veri güvenliği sağlanmaktadır.
➢ **İdari Tedbirler**
- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir. - Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır. - Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır. - Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir. - Kişisel veri işleme envanteri hazırlanmıştır. - Şirket içi periyodik denetimler yapılmaktadır. - Her sene bir defa olmak üzere Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

Şirketler, kişisel verilerin saklanması ve imha edilmesi süreçlerinde yer alan kişileri, kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmekte ve eğitilmektedir. Bu kapsamda Şirket çalışanları ve görevleri dolayısıyla kişisel verileri öğrenen kişiler, bahse konu bilgileri Kanun ve diğer ilgili mevzuat hükümlerine uyun olarak saklamakta ve imha etmektedir. Bu yükümlülük, ilgili kişilerin görevden ayrılmalarından sonra da devam etmektedir.

Bu kapsamda, Şirketler'in saklama ve imha süreçlerinde yer alan kişilere ilişkin detaylar aşağıda açıklanmaktadır:

Unvan	**Birim**	**Görev**
CEO, Direktörler, C Yöneticiler, ve Tüm Bölüm Yöneticileri	Şirketin Tüm Bölümleri/ Birimleri	Çalışanların politikaya uygun hareket etmesinden sorumludur.
İnsan Kaynakları Hukuk Bilgi Teknolojileri	KVKK Kurul'unda bulunan Tüm Bölüm/ Birimler	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi Teknolojileri Müdürü Kıdemli Sistem Destek Uzmanı Sistem Destek Uzmanı	Bilgi Teknolojileri	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Tüm Bölüm/Birim Yöneticileri, Çalışanlar	Tüm Bölüm/ Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

9. SAKLAMA VE İMHA SÜRELERİ

Şirketler, kişisel verileri ancak ilgili uymakla yükümlü olduğu mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza ve imha etmektedir. Bu kapsamda Şirketler, kişisel verileri aşağıdaki EK-1 Saklama ve İmha Süreleri Tablosu'nda belirtilen azami süreler boyunca saklamakta ve imha etmektedir:

İlgili kişilerin Şirketler'e başvurarak kendisine ait kişisel verilerin imha edilmesini talep etmesi halinde Şirketler:

(a) kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa:

(i) ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir, ve
(ii) talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa, bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde gerekli işlemlerin yapılmasını temin eder.

(b) kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, ilgili kişinin talebini Kanun'un 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesini açıklayarak reddedilebilir ve ret cevabını ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

10. PERİYODİK İMHA SÜRELERİ

Şirketler, kişisel verileri imha etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde kişisel verileri imha etmektedir. Bu kapsamda Şirketler;

1- Elektronik ortamlarda yer alan ve saklama süresi dolan kişisel verileri iş bu Politika'nın 6'ncı maddesine göre imha etme yükümlülüğünün ortaya çıkması durumunda 6 (altı) aylık periyotlar halinde anonim hale getirme işlemine tabi tutulmaktadır.

2- Fiziksel ortamlarda yer alan ve saklama süresi dolan kişisel veriler, iş bu Politika'nın 6'ncı maddesine göre imha etme yükümlülüğünün ortaya çıkması durumunda 6 (altı) aylık periyotlar halinde imha işlemine tabi tutulmaktadır.

Yukarıda anılan süreler, her hal ve koşulda Yönetmelik'in 11'inci maddesinde belirtilen azami periyodik imha süresini aşmamaktadır.

11. **YÜRÜRLÜK**

İşbu Politika 11.01.2023 tarihinde yürürlüğe girmiştir. Politika değişen şartlara ve mevzuata uyum sağlamak amacıyla zaman zaman güncellenebilecektir. Güncel Politika QDMS'de yayımlandığı tarihte yürürlüğe girecektir.

İşbu Politika ile Kanun, Yönetmelik ve Aksoy Grup Şirketleri Kişisel Verilerin Korunması ve İşlenmesi Politikası hükümleri arasında herhangi bir çelişki olması halinde, Kanun, Yönetmelik ve Aksoy Grup Şirketleri Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda yer alan hükümler geçerli olacaktır.

EK – 1 Saklama ve İmha Süreleri Tablosu

Veri Kategorisi	Azami Veri Saklama Süresi
Kimlik Bilgisi	10 yıl
Finansal Bilgi	Ticari defterlere son kaydın yapıldığı veya muhasebe belgelerinin oluştuğu takvim yılının bitişinden itibaren 10 yıl İş ilişkisinin bitiminden itibaren 10 yıl
İletişim Bilgisi	İş akdinin veya sözleşme ilişkisinin bitmesinden itibaren 10 yıl
Kimlik Bilgisi	İş ilişkisinin bitiminden itibaren 10 yıl
Eğitim Bilgisi / Performans ve Kariyer Gelişim Bilgisi - Mesleki Deneyim (VERBİS)	İş akdinin sona ermesinden itibaren 10 yıl
Hukuki İşlem ve Uyum Bilgisi	Sözleşme ilişkisinin bitmesinden itibaren 10 yıl Dava sürecinin tamamlanmasından itibaren 10 yıl
Müşteri Bilgisi / Talep Şikayet Bilgisi – Müşteri İşlem	Satışa dönüşmemesi durumunda kaydın yapılmasından itibaren 3 yıl Sipariş tarihinden itibaren 10 Yıl Talep ve şikayetin sonuçlandırılmasından itibaren 10 yıl Sözleşmenin süresinin sona ermesinden itibaren 10 yıl
Özlük Bilgisi	İş akdinin sona ermesinden itibaren 10 yıl
Görsel İşitsel Bilgi	Talep ve şikayetin sonuçlandırılmasından itibaren 10 yıl

Veri Kategorisi	Azami Veri Saklama Süresi
	Dava sürecinin tamamlanmasından itibaren 10 yıl
Çalışan İşlem Bilgisi - İşlem Güvenliği Bilgisi (VERBİS)	İş akdinin sona ermesinden itibaren 10 yıl Dava sürecinin tamamlanmasından itibaren 10 yıl
Sağlık Bilgileri	İş akdinin sona ermesinden itibaren 10 yıl
Çalışan Adayı Bilgisi – İşe Alım ve Mülakat Değerlendirme Bilgileri (VERBİS)	Başvurunun reddinden itibaren 2 yıl
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	İş akdinin sona ermesinden itibaren 10 yıl
Aile Bireyleri ve Yakın Bilgisi	İş akdinin sona ermesinden itibaren 10 yıl
Araç Bilgisi	2 yıl
Fiziksel Mekan Güvenliği Bilgisi	Dava sürecinin tamamlanmasından itibaren 10 yıl
Denetim ve Teftiş Bilgisi	2 yıl
Risk Yönetimi	6 ay

EK – 2 Versiyon Takip Tablosu

VERSİYON TAKİP TABLOSU		
Versiyon No.	**Güncellenme Tarihi**	**Değişiklik Açıklaması**
1.0	04.04.2024	Yürürlük tarihidir.