Alşan LOGISTICS
A MEMBER OF THE PSA GROUP

Kişisel Verilerin Saklanması ve İmhası Politikası

ALIŞAN LOGISTICS

Kişisel Verilerin Saklanması ve İmhası Politikası

BİRİNCİ BÖLÜM KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI'NIN NİTELİĞİ VE AMACI

1.1. GİRİŞ

İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" ya da "Kanun") ve Kanun'un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca ALIŞAN LOJİSTİK A.Ş. ("ALIŞAN") olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin KVKK ve sair mevzuatı gereği, yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin ALIŞAN tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve herhangi bir nedenle ALIŞAN nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

1.2. TANIMLAR

Açık Rıza	:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.
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 kişilerdir.
Kişisel Veri/Veriler	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Özel Nitelikli Kişisel Veri/Veriler	:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.
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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.

Doğrudan tanımlayıcılar	:	Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılarıdır.
Dolaylı tanımlayıcılar	:	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılarıdır.
Kişisel Veri Sahibi/İlgili Kişi	:	Şirket iç ve dış paydaşları, Şirket yetkilileri, şirket iş ortakları, tedarikçiler, danışmanlarımız, çalışanlarımız ve çalışan adaylarımız, ziyaretçilerimiz, şirket ve grup şirket müşterileri, potansiyel müşteriler ve üçüncü kişiler, resmi kurumlar, bankalar, bağımsız denetim kuruluşları gibi kişisel verisi şirket tarafından işlenen gerçek kişileri ifade eder.
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan tüzel kişidir.
Veri İşleyen	:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir.
Kanun/KVKK	:	6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder.
Yönetmelik	:	28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliktir.
KVK Kurulu	:	Kişisel Verileri Koruma Kurulu'dur.
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 ortamdır.
Kişisel Verilerin İşlenmesi, Korunması ve Gizlilik Politikası	:	www.alisangroup.com adresinden ulaşılabilecek, ALIŞAN elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı ifade eder.
Veri kayıt sistemi	:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.
Anonim Hale Getirme	:	Daha öncesinde bir kişiyle ilişkilendirilmiş olan verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel Verilerin Silinmesi	:	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Kişisel Verilerin Yok Edilmesi	:	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Periyodik İmha	:	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.

İKİNCİ BÖLÜM
ORTAMLAR VE GÜVENLİK TEDBİRLERİ

2.1. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

ALIŞAN nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.
Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. ALIŞAN her halde veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri Kanun'a, Kişisel Verilerin İşlenmesi, Korunması ve Gizlilik Politikası'na ve işbu Kişisel Veri Saklama ve İmha Politikası'na uygun olarak işlemek ve korumaktadır.

a) Matbu ortamlar	:	Birim dolapları, arşiv gibi verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
b) Yerel dijital ortamlar	:	ALIŞAN bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler gibi sair dijital ortamlardır.
c) Bulut ortamlar	:	ALIŞAN bünyesinde yer almamakla birlikte, ALIŞAN'ın kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.
c) Elektronik ortamlar	:	OFFICE 365, LOGO TIGER – BORDRO, FILE SERVER, CRYPTOLOG, SHARE POINT PORTAL, ERP VE CRM SİSTEMLERİ, AD DC, DHCP, SAP SUCCESS FACTORS, ORACLE VE MS SQL DB, PDKS SİSTEMLERİ

2.2. ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nın 12. Maddesindeki ilkeler çerçevesinde ALIŞAN, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.
İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.
ALIŞAN tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

2.2.1. Teknik Tedbirler

ALIŞAN, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak başlıca aşağıdaki teknik tedbirleri almaktadır:

• Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.

• Kurulan sistemler kapsamında gerekli iç kontrolleri yapılmaktadır.

• Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.

• Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.

• Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.

• Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulması sağlanmaktadır. Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolü sağlanmaktadır.

• ALIŞAN bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.

• Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulması sağlanmaktadır

• Kişisel verilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanmaktadır.

• Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunmaktadır.

2.2.2. İdari Tedbirler

ALIŞAN, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak başlıca aşağıdaki idari tedbirleri almaktadır:

• Kişisel verilere erişimi olan tüm ALIŞAN çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmakta, personele kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimler verilmektedir.

• Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.

• Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.

• İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.

• Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta veya mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlamakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.

• Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapılmakta ve yaptırılmaktadır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetleri giderilmektedir.

1 *Veri güvenliğine ilişkin yükümlülükler*
MADDE-12 (1)Veri sorumlusu,
a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

2.2.3. Şirket İçi Denetim

ALIŞAN, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da sair bir şekilde ALIŞAN sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, ALIŞAN bu durumu en kısa sürede ilgilisine ve Kurula bildirir. kriptografik yöntemler ile korunmaktadır.

ÜÇÜNCÜ BÖLÜM KİŞİSEL VERİLERİN İMHASI

3.1. SAKLAMA VE İMHA NEDENLERİ

3.1.1. Saklama Nedenleri

ALIŞAN bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız (ilgili politikaya www.alisangroup.com adresinden ulaşabilirsiniz) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

3.1.2.İmha Nedenleri

ALIŞAN bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.
Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:
a) Kanunlarda açıkça öngörülmesi.
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
e) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

3.2.İMHA YÖNTEMLERİ

ALIŞAN, Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikası'na uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

ALIŞAN tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır.

3.2.1.1. Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Karartma	:	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilmesi şeklinde yapılır.

Uzman Tarafından Güvenli Olarak Silme Yöntemleri

Uzman Tarafından Güvenli Olarak Silme	:	Alışan, gerekli görmesi halinde, kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi veya kurum tarafından İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Yazılımdan güvenli olarak silme	:	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler; yasal zorunluluklar sebebi ile ilgili veriye ulaşması gereken yetkili kişiler hariç, diğer kullanıcılar için bir daha erişilemeyecek şekilde dijital komutlarla silinir. 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 ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile erişilemez hale getirilmesi; taşınabilir medyada bulunan verilerin uygun yazılımlar kullanılarak erişilemez hale getirilmesi, bu kapsamda sayılabilecektir. Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır. • Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması. • Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,

3.2.1.2. Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme	:	Matbu ortamda tutulan belgeler evrak imha makineleri ile veya yakılarak, tekrar bir araya getirilemeyecek şekilde yok edilir.

Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme	:	Kişisel veri barındıran optik 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.
De-manyetize etme (degauss)	:	Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.
Üzerine yazma	:	Özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Yazılımdan güvenli olarak silme	:	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

3.2.1.3. Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri çıkarma	:	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların (betimleyici nitelikteki verilerin) bir ya da bir kaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.

Örneğin, aşağıdaki tabloda veri setindeki değişkenlerden yüksek derecede betimleyici olan veri gruplarının çıkartılması ile anonimleştirme sağlanmıştır.

Çalışanın Adı	Yaşadığı İl	Yaşadığı İlçe	Yaşadığı Mahalle	Pozisyonu	Aylık Geliri	Kıdemi (Yıl)
Ahmet	İstanbul	Maltepe	Bağlarbaşı	Uzman	2.000 TL	5
Ayşe	Kocaeli	Gebze	Güzeller	Müdür	5.300 TL	3

Kayıtları çıkartma	:	Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.
Bölgesel gizleme	:	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir. Dolayısıyla tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır. Örneğin, şirketin futbol takımının yedek listesinde olan ilgili veri sorumluları arasında yalnızca bir kişi 65 yaşında ise yaş, cinsiyet ve sağlık durumu yönünden futbol oynayabilecek olup olmadığı bilgisinin birlikte saklandığı bir veri kümesinde 'Yaş:65' yerine 'Bilinmiyor' yazılması veya bu kısmın boş bırakılması anonimleştirmeyi sağlayacaktır.
Genelleştirme	:	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir. Dolayısıyla veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin; çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.
Alt ve üst sınır kodlama /	:	Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

Örneğin, bir işyerinde çalışan personelin işyerindeki çalışma yılının 5 yıldan az, 5 ile 10 yıl arasında veya 10 yıldan çok olmasına göre (çok deneyimli), (deneyimli) ya da (deneyimsiz) olarak birleştirilerek anonim hale getirilebilir:

Çalışanın Pozisyonu	Yaşı	Cinsiyeti	Aylık Geliri	Kıdemi (Yıl)
Uzman	30	E	2.000 TL	5
Müdür	43	K	5.300 TL	3

İkinci örnekte ise kıdem değişkenine belirlenen yıl ölçütüne göre alt ve üst sınır kodlaması uygulanarak üç kategoriye halinde anonimleştirilmiş şeklini göstermektedir.

Çalışanın Pozisyonu	Yaşı	Cinsiyeti	Aylık Geliri	Kıdemi (Yıl)
Uzman	30	E	2.000 TL	Çok Deneyimli
Müdür	43	K	5.300 TL	Deneyimsiz

Global Kodlama	**:**	Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Çalışanın Pozisyonu	İkamet Adresi	Çocuğu	Aylık Geliri	Kıdemi (Yıl)
Uzman	Bağlarbaşı Mah. Çiçek Sok. No:11/11 Maltepe/İstanbul	Var	2.000 TL	5
Müdür	Güzeller Mah. Çiçek Sok. No:11/11 Gebze/Kocaeli	Yok	5.300 TL	3

Aşağıdaki tabloda veri türetme yoluyla anonimleştirme yöntemi uygulanmıştır:

Çalışanın Pozisyonu	İkamet Adresi	Çocuğu	Aylık Geliri	Kıdemi (Yıl)
Uzman	İstanbul Anadolu Yakası	Var	2.000 TL	5
Müdür	Kocaeli Kuzey Bölge	Yok	5.300 TL	3

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	:	Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen / istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.
Mikro birleştirilme	:	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. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır. Örneğin, maaş bilgisi için; 10.000 TL altı ve üstü iki grup yapılır ise, 10.000 ve daha az maaş alan kişilerin maaşlarının toplamı kişi sayısına bölünür ve 10.000TL altında maaş alan herkesin maaş kümesine elde edilen bu değer yazılır.
Gürültü Ekleme	:	Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/−) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.
Veri karma ve bozma	:	Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.
Veri Değiş Tokuşu	:	Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir. Örneğin, aşağıdaki tabloda ‘Yaş: 45’, ‘Cinsiyet: Kadın’, ‘İl: Ankara’ verileri bulunan kişilere ait gelir bilgisi ‘Yaş: 30’, ‘Cinsiyet: Kadın’, ‘İl: İzmir’ olanlar ve ‘Yaş: 25’, ‘Cinsiyet: Erkek’ ‘İl: İzmir’ olanların gelir bilgileri ile ‘Yaş:35’, ‘Cinsiyet: Erkek’ ‘İl: İstanbul’ olanların gelir bilgileri birbirleri içerisinde değiştirilerek veri tabanı dönüştürülmüştür.

Örneğin, bir işyerinde çalışan personelin işyerindeki çalışma yılının 5 yıldan az, 5 ile 10 yıl arasında veya 10 yıldan çok olmasına göre (çok deneyimli), (deneyimli) ya da (deneyimsiz) olarak birleştirilerek anonim hale getirilebilir:

YAŞ	CİNSİYET	İL	GELİR
45	Kadın	Ankara	30.000 TL
30	Kadın	İzmir	20.000 TL
25	Erkek	İzmir	15.000 TL
35	Erkek	İstanbul	25.000 TL
55	Erkek	İzmir	18.000 TL
24	Erkek	İzmir	40.000 TL

Aşağıdaki tabloda veri değiş tokuş yöntemi uygulanmıştır:

YAŞ	CİNSİYET	İL	GELİR
45	Kadın	Ankara	20.000 TL
30	Kadın	İzmir	30.000 TL
25	Erkek	İzmir	25.000 TL
35	Erkek	İstanbul	15.000 TL
55	Erkek	İzmir	40.000 TL
24	Erkek	İzmir	18.000 TL

ALIŞAN, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. ALIŞAN, bu anonimleştirme yöntemlerini kullanırken K-Anonimlik (K-Anonymity), L-Çeşitlilik (L-Diversity) ve T-Yakınlık (T-Closeness) istatistik yöntemlerini kullanabilir.

KVKK'nın 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

3.3.SAKLAMA VE İMHA SÜRELERİ
3.3.1. Saklama Süreleri

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	1)Hizmet akdi süresince iş kazası/meslek hastalığına maruz kalmamış çalışanlar açısından hizmet ilişkisinin sona erdiği tarihten itibaren 10 yıl süreyle muhafaza edilir. Süre, fasılalı çalışmalarda son çalışma döneminin sona erdiği tarihten itibaren işlemeye başlar. 2)Hizmet akdi süresince iş kazası/meslek hastalığına maruz kalmış yahut bu riski taşıyan çalışanlar açısından özlük kayıtları, iş kazası tarihi/meslek hastalığı tespit tarihini müteakip 15 yıl süreyle saklanabilir. Bu durumda saklama süresi olarak uzun olan süre (hizmet ilişkisinin hitamından itibaren 10 yıl / kaza-tespit tarihinden itibaren 15 yıl) uygulanır.
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10 yıl müddetle muhafaza edilir.
Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Çalışanın işten ayrılma tarihinden itibaren 15 yıl süreyle çalışanların kişisel sağlık dosyaları saklanır.
İş Ortağı/ Çözüm Ortağı/ Danışman	İş Ortağı/ Çözüm Ortağı/ Danışman ile ALIŞAN arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/ Çözüm Ortağı/ Danışman çalışanı verileri	İş Ortağı/ Çözüm Ortağı/ Danışmanın, ALIŞAN ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
Ziyaretçi	ALIŞAN' a ait fiziki mekana girişte alınan ziyaretçiye ait ad, soyad, T.C.K.N., araç plakası ile kamera kayıtları, telefon aramalarında alınan ses kayıtları	En fazla 2 yıl süre ile saklanır.

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
İnternet Sitesi Ziyaretçisi	İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	En fazla 2 yıl süre ile saklanır.
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.
Stajyer(öğrenci)	Stajyere ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 5 (beş) yıl müddetle muhafaza edilir.
Müşteri	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri, Araç plaka bilgisi	Müşteri'nin, satın almış olduğu her bir ürün/ hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
Müşteri	Kamera görüntüleri	En fazla 1 yıl süre ile saklanır.
Potansiyel Müşteri	Potansiyel Müşteri ile ALIŞAN arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları	En fazla 5 yıl süre ile saklanır.
ALIŞAN' ın İşbirliği İçinde Olduğu Kurum/ Firmalar (Tedarikçi, Fason Üretici, Bayi/ Franchise	ALIŞAN' ın İşbirliği İçinde Olduğu Kurum/Firmalar ile ALIŞAN arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, ALIŞAN' ın İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri	ALIŞAN' ın İşbirliği İçinde Olduğu Kurum/ Firmaların, ALIŞAN ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.
* Ayrıca evrakın niteliği gereği, ticari veya yasal gerekçelerle, daha uzun süre saklama ihtiyacının hasıl olması halinde, yukarıdaki sürelere tabi olmaksızın, azami 20 yıla kadar ilgili evrakların saklanması mümkündür.

3.3.2. İmha Süreleri

ALIŞAN, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu 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.

İlgili kişi, Kanunun 13'ncü maddesine istinaden ALIŞAN'a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; ALIŞAN talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. ALIŞAN'ın talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi,

Korunması ve Gizlilik Politikasına uygun olarak yapmış olması gerekir. ALIŞAN, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep ALIŞAN tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

3.4. PERİYODİK İMHA

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; ALIŞAN işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir. Periyodik imha süreçleri ilk kez 01.01.2019 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

3.5. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

ALIŞAN, gerek talep üzerine gerekse periyodik imha süreçlerinde resen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.
ALIŞAN, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

3.5.1. Teknik Tedbirler

• ALIŞAN, işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
• ALIŞAN, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
• ALIŞAN, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
• ALIŞAN, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

3.5.2. İdari Tedbirler

• ALIŞAN, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
• ALIŞAN, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
• ALIŞAN, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
• ALIŞAN, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
• ALIŞAN, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

DÖRDÜNCÜ BÖLÜM

4.1. KİŞİSEL VERİ KOMİTESİ

ALIŞAN bünyesinde bir Kişisel Veri Komitesi kurar. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi bir yönetici, bir hukuk uzmanı, üç idari uzman ve iki teknik uzman olmak üzere yedi kişiden oluşur. Kişisel Veri Komitesinde görevli ALIŞAN çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

ÜNVAN		GÖREV TANIMI
Kişisel Veri Komitesi Yöneticisi	:	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
KVK Uzmanı (Hukuk, Teknik ve İdari)	:	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

BEŞİNCİ BÖLÜM GÜNCELLEME VE UYUM

ALIŞAN, Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda Kişisel Verilerin İşlenmesi ve Korunması Politikasında ya da işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.

İşbu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır.

5.1. DEĞİŞİKLİK NOTLARI

11/01/2019:Kişisel Veri Saklama ve İmha Politikası yayınlanmıştır.
daha eski tarihli bir değişiklik bulunmamaktadır.

ALIŞAN LOJİSTİK A.Ş.


Olson
LOGISTICS
A MEMBER OF THE PSA GROUP