

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. Anonim Şirketi (“YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.”) gerçekleştirilen saklama ve imha faaliyetlerine istinaden iş ve işlemler konusunda usul ve esasları belirlemek amacıyla bu politikayı hazırlamıştır.

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.; 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında “ Kişisel Verilerin Silinmesi, Yok Edilmesi, veya Anonim Hale Getirilmesi hakkında çıkarılan 28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Yönetmeliğin 3. 5. Ve 6. Maddeleri gereğince kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve yönetmelik’te belirtilen sair yükümlülüklerin yerine getirilmesi amacıyla (YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.) olarak uygulanacak kurallar ve sorumluluklar yer almaktadır.

1.2 KAPSAM

(YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.);

- Çalışanlar
- Çalışan Adayları
- Stajyer
- Ziyaretçi
- Tedarikçi ve Tedarikçi Çalışanı
- Hizmet Sağlayıcıları
- Müşteri

Ve diğer üçüncü kişilere ait kişisel verilerin söz konusu politika kapsamının olup (YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.) tarafından yönetilen ve sahip olunan bütün kayıt ortamları ve kişisel verilerin işlenmesiyle ilgili faaliyetler bu politika ile uygulanmaktadır.

1.3 TANIMLAR

ALICI GRUBU	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
AÇIK RIZA	Açık Rıza belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza.
SİLME	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
ANONİM HALE GETİRME	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

YOK ETME	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
ÇALIŞAN	YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. Personeli
ÇALIŞAN ADAYI	YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından açık pozisyonlarda değerlendirilmek üzere kariyer web sitelerinden/online sistemlerinden bilgisi edinilen kişiler
TEDARİKÇİ	YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. ile belirli bir sözleşme ile hizmet veya mal sağlayan gerçek veya tüzel kişi ve kurumlar. Tedarikçilerle olan ilişkilerde, verilerin saklanması ve imhası faaliyetinde, bunların yetkilileri, ortakları, çalışanların ve temsilcilerinin kişisel verileri bu Politika kapsamındadır.
MÜŞTERİ	YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. veya grup firmalarından mal veya hizmet alan gerçek veya tüzel kişi ve kurumlar. Tüzel kişi müşterilerle olan ilişkilerde, verilerin saklanması ve imhası faaliyetinde, bunların yetkilileri, ortakları, çalışanları ve temsilcilerinin kişisel verileri bu Politika kapsamındadır.
MÜŞTERİ ADAYI	YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. veya grup firmalarından mal veya hizmet alması potansiyel öngörülen gerçek veya tüzel kişi ve kurumlar. Tüzel kişi müşteri adaylarıyla olan ilişkilerde, verilerin saklanması ve imhası faaliyetinde, bunların yetkilileri, ortakları, çalışanları ve temsilcilerinin kişisel verileri bu Politika kapsamındadır.
İLGİLİ KİŞİ	Kişisel verileri işlenen kişi.
İLGİLİ KULLANICI	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.
KANUN	6698 Sayılı Kişisel Verilerin Korunması Kanunu
İMHA	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
KİŞİSEL VERİ	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
KİŞİSEL VERİ İŞLEME	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

KİŞİSEL VERİLERİN SİLİNMESİ	açıklayarak detaylandırdıkları envanter. 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
ÖZEL NİTELİKLİ KİŞİSEL VERİ	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 verileri.
PERİYODİK İMHA	Kanunda yer alan kişisel verilerin işleme 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 işlemi.
POLİTİKA VERİ İŞLEYEN	Kişisel Verileri Saklama ve İmha Politikası Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
VERİ KAYIT SİSTEMİ	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.; 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 saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda verilmiştir.

UNVAN	BİRİM	GÖREV
İNSAN KAYNAKLARI UZMANI	İNSAN KAYNAKLARI	Çalışanların politikaya uygun hareket etmesinden sorumludur
İNSAN KAYNAKLARI MÜDÜRÜ	İNSAN KAYNAKLAR	Görevlerine uygun olarak politikanın yürütülmesinden sorumludur
BİLGİ İŞLEM MÜDÜRÜ	BİLGİ İŞLEM	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve gerekli

		yatırımların sağlanması için yönetimin bilgilendirilmesinden, Elektronik kayıt ortamlarında gerçekleştirilen silme, yok etme, anonimleştirme işlemleri bakımından yürütüm ve iç denetimlerden sorumludur.
Kurumsal İletişim, Satış ve Pazarlama, Muhasebe ve Finans, Tedarik Zinciri, Proje ve Yatırımlar, Kalite Güvence Müdürlüklerinde yer alan çalışanlar	Kurumsal İletişim ve Satış ve Pazarlama Müdürlüğü, Muhasebe ve Finans Müdürlüğü, Tedarik Zinciri Müdürlüğü, Proje ve Yatırımlar Müdürlüğü, Kalite Güvence Müdürlüğü	Politikanın yürütülmesinden sorumludur

3. KAYIT ORTAMI

Kişisel veriler, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> Application, Database, File Server, Antivürüs Server (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Yazılımlar (.....) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) Kişisel bilgisayarlar (Masaüstü, dizüstü) Mobil cihazlar (telefon, tablet vb.) Optik diskler (CD, DVD vb.) Çıkartılabilir bellekler (USB, Hafıza Kart vb.) Yazıcı, tarayıcı, fotokopi makinesi 	<ul style="list-style-type: none"> Kâğıt Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHA HAKKINDA AÇIKLAMALAR

Kurum tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 SAKLAMAYA İLİŞKİN AÇIKLAMA

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta

öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.2 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.; faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir.

- 6698 sayılı Kişisel verilerin Korunması Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 4857 sayılı İş Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 213 Sayılı Vergi Usul Kanunu
- 1774 Sayılı Kimlik Bildirme Kanunu
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu
- 5651 sayılı İnternet ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Bu Kanunlar Uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri veya ilgili sürecin ihtilafa konu olması muhtemelse azami olarak ilgili kanundaki zaman aşımı süresi kadar saklanmaktadır. Herhangi bir ihtilafa konu olması mümkün görülmeyen süreçlerde ise YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından makul süre Veri Sorumluları Sicili Hakkında Yönetmelik, Kurul kararları ve rehberleri incelenerek belirlenir.

4.3 SAKLAMAYI GEREKTİREN İŞLEME ARAÇLARI

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklamaktadır.

- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- İlgili kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından ilgili kişilerin açık rızasının bulunması
- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Müşterilerle ve Potansiyel müşterilerle ilişkilerin yürütülmesi.
- Ticari faaliyetlerin sürdürülebilmesi
- Hukuki yükümlülüklerin yerine getirilebilmesi
- Çalışan haklarının ve yan haklarının planlanması ve ifası için Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Sözleşmeler ve protokollerin ifası.

- Satış sonrası hizmetlerin sunulması
- Sosyal sorumluluk projeleri faaliyet kayıtlarının arşivlenmesi.
- Kişisel Verilerin Korunması Kanunu kapsamında gerekli teknik önlemlerin alınmasını temin etmek (veri yedekleme, silme yok etme işlemlerinin kayıt altına alınması, erişim log kayıtlarının tutulması vb.),
- Kişisel Verilerin Korunması Kanunu kapsamında ilgili kişilerin talep ve şikayetlerin sonuçlandırılması.

4.4 İMHAYI GEREKTİREN DURUMLAR

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş., ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyetinde bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

durumlarda, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından ilgili kişinin talebi üzerine ya da re'sen silinir, yok edilir veya anonim hale getirilir.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından teknik ve idari tedbirler alınır.

5.1 TEKNİK TEDBİRLER

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Sızma testi uygulanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

5.1 İDARİ TEDBİRLER

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından, işlediği Kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır;

- Kişisel veri işleme envanteri hazırlanmıştır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- İlgili Kişileri Aydınlatma Yükümlülüğü Yerine Getirilmektedir.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Mevcut risk ve tehditler belirlenmiştir
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Çalışanlarla ve dış ilişkide olunan kişilerle gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır

- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1 KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verileri aşağıdaki yöntemler ile silinmektedir;

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre olan 10 Yılı sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.
Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365 gibi)	Bulut sisteminde verileri silme komutu vererek silinir. Anılan işlem gerçekleştirirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına özellikle dikkat edilecektir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını 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
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

6.2 KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel veriler, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından aşağıda verilen yöntemlerle yok edilir: Soft / Digital

Veri Kayıt Ortamı	Açıklama
Optik/Manyetik Medyada Yer Alan	Optik medya ve manyetik medyada hiçbir veri saklanmamaktadır.

Kişisel Veriler	
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kağıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kağıt kırma makinelerinde veya arşiv alanlarında yakılarak geri dönülemeyecek şekilde yok edilir.

6.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

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 veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

7.1 Genel Esaslar

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

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

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Kişisel Verileri Koruma Komitesi Başkanlığınca güncellemeler yapılır.

7.2 İLGİLİ KİŞİNİN KİŞİSEL VERİLERİNİN SİLİNMESİ VE YOK EDİLMESİ TALEBİ VE SİLME-YOK ETME SÜRELERİ

İlgili kişi, Kanunun uygulanmasıyla ilgili taleplerini tercihen YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. Yatırım A. Başvuru formunu kullanmak suretiyle yazılı olarak veya Kurul'un belirleyeceği diğer yöntemlerle YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. 'ya iletir.

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş., başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret esas alınabilir.

YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş., talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde YAVUZ BİNSAT KORUMA VE

ÖZEL GÜVENLİK A.Ş. tarafından gereği yerine getirilir. Başvurunun YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.'nin hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.

İlgili kişi, işbu Politika'da YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.'ya başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş. 'da her yıl Mayıs ve Kasım aylarında periyodik imha işlemi gerçekleştirilir. YAVUZ BİNSAT KORUMA VE ÖZEL GÜVENLİK A.Ş.; 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

9. SÜREÇ BAZINDA SAKLAMA VE İMHA SÜRELERİ TABLOSU

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Genel Kurul ve Yönetim Kurulu İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşme akdedilmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Teklif Süreci	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanların sistem ve yazılımlara tanımlanması/taahsis/erişim yetkisi verilmesi (e-mail adresi, kullanıcı adı, şifre, parola gibi)	İş akdi devam ettiği sürece kontrollü olarak gerçekleştirilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Etkinlik ve Toplantı Katılımcılarının Kaydı	Etkinliğinin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mahkeme/icra/idari merciler bilgi taleplerinin cevaplanması	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş akdinin sona ermesinden itibaren 5 yıl veya 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Lokasyon Kayıtları	Kayıttan itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan şirket GSM hattı kullanım ücret ve döküm	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha

kayıtları		süresinde
Çalışanlara Araç Kiralanması Sürecinde Edinilen Veriler	İlgili çalışana yönelik kiralama ilişkisi sona erdikten sonraki ilk periyodik imha sürecine kadar muhafaza edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Eğitimleri	İş Güvenliğine Yönelik Alınan Mesleki Eğitim Kayıtları 15 Yıl- Diğerleri 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Toplu İş Sözleşmesi- Sendikal İşlemler	İş Akdinin sona ermesinden itibaren ilk periyodik imha sürecine kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Veriler	Başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (sağlık raporları iş yeri hekimi tarafından teslim alınır ve muhafaza edilir)	Çalışanlar için iş ilişkisinin sona ermesine müteakip 15 yıl, Tedarikçi çalışanları için ilişkinin sona ermesinden itibaren 10 yıl.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Stajyer işlemleri	Stajın sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Burs Yardımı	Burs ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Seyahat İşlemleri	Seyahat tarihinden sonraki ilk periyodik imha süresine kadar.	Seyahat süresinden sonraki ilk periyodik imha süresinde
KVK Süreçleri (Aydınlatma, Açık Rıza, Başvuru ve Şikayetler)	İlgili sürecin tamamlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Silme Yok Etme Anonim Hale Getirme Kayıt Süreci	İşlem tarihinden itibaren 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Posta- Kargo İşlem Kayıtları	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi Kayıtları	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş yeri Kamera Kayıtları	3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha

		süresinde
Fihrist ve Rehber Kayıtları- İletişim faaliyetleri	Son iletişim tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sevkiyat Kayıtları (Kantar, Nakliye, Boşaltma, İrsaliye vb)	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Teknik Bilgi Talepleri, Müşteri Şikayetlerinin Yanıtlanması	İşlem tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Üye Olunan Derneklerle İlişkiler	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

10. POLİTİKA'NIN YAYINLANMASI ve SAKLANMASI

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, web sitesinde kamuya açıklanır. Basılı kağıt nüshası da Kişisel Verileri Koruması için görev atanan kişiler tarafından saklanır.

11. POLİTİKA'NIN GÜNCELLENME PERİYODU

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