



**SİTEPLUS ÖZEL
GÜVENLİK HİZMETLERİ
A.Ş.**

2020

**KİŞİSEL VERİ SAKLAMA VE
İMHÂ POLİTİKASI**

AMAC:

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), SİTEPLUS Özel Güvenlik Hizmetleri A.Ş tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin, iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

SİTEPLUS; Kişisel Verilerin Korunması ve İşlenmesi Politikasında belirtilen temel ilkeler doğrultusunda şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin, T.C Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) , ikincil mevzuat ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, SİTEPLUS tarafından bu doğrultuda hazırlanmış olan bu Politikaya uygun olarak gerçekleştirilir.

Kişisel verilerin korunması ve kişisel verileri toplanan gerçek kişilerin temel hak ve hürriyetlerinin gözetilmesi kişisel verilerin işlenmesine ilişkin politikamızın temel prensibidir.

Şirketimiz, kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemleri sayılan ilkeler doğrultusunda hazırlanmış olan Politikaya uygun olarak gerçekleştirilmektedir.

KAPSAM:

Şirket çalışanları, çalışan adayları, tedarikçiler, müşteriler, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Şirketin uhdesinde bulunan ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika hükümleri uygulanacaktır.

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

Kısaltmalar ve tanımlar

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek ve ya tüzel kişi kategorisi
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Şirket Çalışanı	Bir iş akdi nedeniyle SİTEPLUS bünyesinde çalışmakta olan kimse
EBYS	Elektronik Belge Yönetim Sistemi

Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okuna-bildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
SİTEPLUS Hizmet Sağlayıcısı	SİTEPLUS ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenme-sinden sorumlu olan kişi ya da birim hariç olmak üzere; veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişi-sel verileri işleyen kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	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 verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süre-sini, 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
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 verileri.
Periyodik 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.
Politika	Kişisel Verileri Saklama ve İmha Politikası
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu 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 kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi
Veri Sorumluları Sicil Bilgi Sistemi	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

POLİTİKA İLE DÜZENLENEN KAYIT ORTAMLARI

SİTEPLUS, 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:

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> ✓ Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS.) ✓ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.) ✓ Kişisel bilgisayarlar (Masaüstü, dizüstü) 	<ul style="list-style-type: none"> ✓ Kâğıt ✓ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ✓ Yazılı, basılı, görsel ortamlar

<ul style="list-style-type: none">✓ Mobil cihazlar (telefon, tablet vb.)✓ Optik diskler (CD, DVD vb.)✓ Çıkarılabilir bellekler (USB, Hafıza Kart vb.)✓ Yazıcı, tarayıcı, fotokopi makinesi	
---	--

KİŞİSEL VERİLERİN İMHASINI GEREKTİREN SEBEPLER:

Şirketimiz, kişisel verileri, Kanunda belirtilen ilkelerle uyumlu şekilde SİTEPLUS Kişisel Verilerin Korunması ve İşlenmesi Politikasının ilgili maddelerinde yer alan kişisel veri işleme amaçlarıyla ve aşağıda belirtilen Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel verilerin işleme şartlarına istinaden, kişisel verileri saklamakta ve kullanmakta olup söz konusu şartların tamamının ortadan kalkması halinde, kişisel verileri, re 'sen veya kişisel veri sahibinin talebi üzerine imha etmektedir.

Kişisel Veri Sahibinin Açık Rızasının Bulunması: Kişisel verilerin işleme şartlarından biri, sahibinin açık rızasıdır. Kişisel veri sahibinin açık rızası, belirli bir konuya ilişkin bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklanmalıdır.

Kanunlarda Açıkça Öngörülmesi: Veri sahibinin kişisel verileri, kanunlarda açıkça öngörülmesi halinde açık rızası alınmadan hukuka uygun olarak işlenebilecektir.

Fiili İmkânsızlık Sebebiyle Kişisel Veri Sahibinin Açık Rızasının Alınmaması: Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınmayacak olan kişinin, kendisinin ya da 3. bir kişinin hayatı veya beden bütünlüğünü korumak için kişisel verisinin işlenmesinin zorunlu olması halinde, veri sahibinin kişisel verileri rızası alınmadan işlenebilecektir.

Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgili Olması: Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde, kişisel verilerin işlenmesi mümkündür.

Hukuki Yükümlülük: Şirketimizin hukuki yükümlülüklerini yerine getirmesi için veri işlemenin zorunlu olması halinde, kişisel veri sahibinin verileri işlenebilecektir.

Kişisel Veri Sahibinin Kişisel Verisini Alenileştirmesi: Veri sahibinin, kişisel verisinin kendisi tarafından alenileştirmiş olması halinde, ilgili kişisel veriler, alenileştirme amacıyla sınırlı olarak işlenebilecektir.

Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması: Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde, veri sahibinin kişisel verileri işlenebilecektir.

Şirketimizin Meşru Menfaati İçin Veri İşlemenin Zorunlu Olması: Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirketimizin meşru menfaatleri için veri işlenmesinin zorunlu olması halinde, veri sahibinin kişisel verileri işlenebilecektir.

Bu doğrultuda yukarıda belirtilen şartlardan bir ya da birden fazlası, kişisel veri işleme faaliyetinin dayanağı olabilmektedir.

→ **SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER**

Kurumda, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

- Arşiv Hizmetleri Hakkında Yönetmelik

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

→ **İMHA YI GEREKTİREN SEBEPLER**

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun, Kurum tarafından kabul edilmesi,
- Şirketin, 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 şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, durumlarında Şirket tarafından, ilgili kişinin talebi üzerine ya da re ‘sen silinir, yok edilir veya anonim hale getirilir.

→ **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. maddesiyle Kanunun 6. maddesinin dördüncü fıkrası gereği, özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde SİTEPLUS tarafından teknik ve idari tedbirler alınır.

Teknik Tedbirler

Kurumumuz tarafından işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Sızma (Penetrasyon) testleri ile Kurumumuzca bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Kurumumuzun 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 girişini 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.
- Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Kurumumuz, 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 bu durumu ilgili kişiye ve Kurula bildirmek için Kurumumuz 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 saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlarda tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçlarının kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler, e-posta yoluyla aktarılması gerektiğinde şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerektiğinde kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma yapılması gerektiğinde, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kâğıt ortamı yoluyla aktarımı gerektiğinde evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

İdari Tedbirler

Kurumumuz tarafından işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik olarak kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 6698 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Saklanan kişisel verilere şirket içi erişimi, iş tanımı gereği erişmesi gereken personel ile sınırlı tutulmaktadır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi dikkate alınır.
- Şirketimiz ile çalışanlar arasında yürütülen faaliyetlere ilişkin gizlilik sözleşmeleri imzalanmaktadır.
- Güvenlik politikası ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurumumuzca ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır. Denetimler sonucu ortaya çıkan gizlilik ve güvenlik zafiyetleri derhal giderilir.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİNE İLİŞKİN ESASLAR

SİTEPLUS, Kanununun 12 ve 13.maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması hallerinde, kişisel verilerin re'sen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi konusunda yükümlülüklerini yerine getirmektedir.

Şirket, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde şirkete ait kişisel verilerin korunması, işlenmesine ilişkin politikalarda düzenlenen genel ilkeler ile teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun olarak hareket etmektedir.

Şirket tarafından 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 iki yıl süreyle saklanır.

Şirket, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer.

Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almaktadır.

SİTEPLUS, verilerin kaydedildiği ortama bağlı olarak aşağıdaki yöntemlerden uygun olanı seçer:

- Silme komutu verme
- Karartma
- Dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakkını kaldırma
- Yazılım aracılığıyla silme
- Veri tabanı komutuyla silme

Kişisel Verilerin Yok Edilmesi

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

SİTEPLUS verilerin kaydedildiği ortama bağlı olarak aşağıdaki yöntemlerden uygun olanı seçer:

- Fiziksel yok etme
- Üzerine yazma
- Kâğıt imha makinesi ile yok etme
- Şifreleme anahtarlarının tüm kopyalarını yok etme

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 getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri

sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Şirket, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almaktadır.

SİTEPLUS verilerin kaydedildiği ortama bağlı olarak aşağıdaki yöntemlerden uygun olanı seçer:

- Değişkenleri çıkartma
- Kayıtları çıkartma
- Alt ve üst sınır kodlama
- Bölgesel gizleme
- Örnekleme
- Mikro-birleştirme
- Veri değiş-tokuşu
- Görüntü ekleme
- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

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

Şirketimizce, kişisel verilerin saklanması ve imha edilmesi süreçlerinde yer alan kişiler, Kişisel Verilerin Korunması Hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi, konusunda bilgilendirilmekte ve eğitilmektedir. Bu kapsamda Şirketimiz çalışanları ve görevleri dolayısıyla kişisel verileri öğrenen kişiler, bahse konu bilgileri Kanun ve diğer ilgili mevzuat hükümlerine uygun olarak saklamakta ve imha etmektedir. Bu yükümlülük, ilgili kişilerin görevden ayrılmalarından sonra da devam etmektedir.

Bu kapsamda, Şirketimizin saklama ve imha süreçlerinde yer alan kişilere ilişkin detaylar aşağıda açıklanmaktadır:

UNVAN	BİRİM	GÖREV
Hukuk Direktörü	Hukuk	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İnsan Kaynakları Direktörü	İnsan kaynaklar	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kurumsal İletişim Müdürü	Kurumsal İletişim	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi

		uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	Bilgi İşlem	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İdari İşler Müdürü	İdari İşler	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Finans		Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Operasyon		Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

SITE+PLUS

SAKLAMA VE İMHA SÜRELERİ

Saklama süreleri sona eren kişisel veriler için re 'sen silme, yok etme veya anonim hale getirme işlemi Şirketimizce- ilgili birim yetkili kişi tarafından- yerine getirilir.

VERİ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Sözleşme Hazırlama	10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
İşe Alım	İş ilişkisinin kesilmesine müteakip 10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Personel Özlük	İş ilişkisinin kesilmesine müteakip 10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Personel ile ilgili mahkeme, icra bilgileri	İş ilişkisinin kesilmesine müteakip 10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
İSG uygulamaları	İş ilişkisinin kesilmesine müteakip 10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Şirket kurucuları ve yönetim kuruluna ait bilgiler	10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Kaza raporlama	10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde

Toplantı/eğitim katılım tutanakları	2 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Hizmet kayıtları: faaliyet esnasında tutulan kayıtlar (kontrol formları, görev yeri defterleri, ziyaretçi kayıt defteri, araç giriş kayıt defteri, ceride kayıt defteri, silah devir teslim defteri, kayıp/buluntu eşya formu vb.)	Hizmet sözleşmesinin bitmesine müteakip 1 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde
Muhasebesel kayıtlar	10 yıl	Saklama süresinin bitimini takip eden 6 aylık süre içerisinde

PERİYODİK İMHA SÜRELERİ

Şirketimiz, kişisel verileri imha etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri imha etmektedir. Bu kapsamda Şirketimizin kişisel verileri saklama süresi 10 (on) yıl olup yasal gereklilikler kapsamında belirli süreler ile tutulması zorunlu olan veriler, yasalarda belirtilen sürelerle sınırlı olarak işlenmektedir. Şirket, kişisel verileri imha etme yükümlülüğünün ortaya çıkması halinde kişisel verileri 6 (altı) aylık periyotlar halinde imha işlemine tabi tutmaktadır. Anılan süre, her hal ve koşulda Yönetmelik'in 11'inci maddesinde belirtilen azami periyodik imha süresini aşmamaktadır. Şirketimizde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

YÜRÜRLÜK

İşbu Politika yayın tarihinde yürürlüğe girmiştir. Politika, değişen şartlara ve mevzuata uyum sağlamak amacıyla zaman zaman güncellenebilecektir. Güncellenmiş Politika <http://siteplus.com.tr/> da yayımlandığı tarihte yürürlüğe girecektir.

İşbu Politika ile Kanun, Yönetmelik ve SİTEPLUS Kişisel Verilerin Korunması ve İşlenmesi Politikası hükümleri arasında herhangi bir çelişki olması halinde, Kanun, Yönetmelik ve SİTEPLUS Kişisel Verilerin Korunması ve İşlenmesi Politikasında yer alan hükümler geçerli olacaktır.