SECURITAS TÜRKİYE
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun (Kanun) ve 30224 sayılı Resmi Gazete'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ilgili hükümleri gereği Türkiye'de faaliyet gösteren *Securitas Güvenlik Hizmetleri A.Ş., Securitas İtfaiye Hizmetleri A.Ş., Securitas Uzaktan İzleme Alarm Hizmetleri A.Ş., Securitas Kontrol ve Destek Hizmetleri A.Ş., Securitas Risk Yönetimi ve Danışmanlık Hizmetleri A.Ş., Securitas Entegre Güvenlik Çözümleri ve Hizmetleri A.Ş., Securitas Tesis Yönetimi ve Danışmanlık Hizmet A.Ş.* Şirketlerimiz (bundan böyle "**Securitas**" veya "**Securitas Türkiye**" olarak anılacaktır**)** tarafından gerçekleştirilen kişisel verilerin saklanması ve imhası faaliyetlerine ilişkin usul ve esasları belirlemektir.

2. KAPSAM

Securitas Türkiye çalışanları, çalışan adayları, hizmet sağlayıcıları ve müşterilerin yetkilileri ile çalışanları, ziyaretçiler ve veri sorumlusu sıfatıyla kişisel verileri işlenen diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Securitas Türkiye'nin sahip olduğu ya da Securitas Türkiye tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik tüm faaliyetlerde bu politika uygulanır.

3. KISALTMALAR VE TANIMLAR

Politika: Kişisel Verileri Saklama ve İmha Politikasını,
Yönetmelik: 28 Ekim 2017 tarihli Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i
Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
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 verilerini,
İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,
Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişiyi,
Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
Periyodik imha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,
Kişisel Veri Saklama Tablosu: Kişisel verilerin Securitas Türkiye nezdinde saklanacağı süreleri gösteren tabloyu,
Kişisel Veri İşleme Envanteri: Securitas Türkiye'nin iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve

kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıkladığı envanteri,
Kişisel Verileri Koruma Komitesi: Securitas Türkiye'nin şirket içinde her departmandan bir temsilci olmak üzere oluşturduğu uyum süreci takibinden sorumlu komiteyi,
Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
VERBİS: Veri Sorumluları Sicil Bilgi Sistemi'ni
ifade eder.

4. KAYIT ORTAMLARI

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 kayıt ortamı kapsamına girer. Securitas Türkiye nezdinde saklanan kişisel veriler, ilgili verinin niteliğine, işlenme amaçlarına ve hukuki yükümlülüklerimize uygun kayıt ortamında tutulur. Kişisel veriler, Securitas Türkiye tarafından aşağıda listelenen ortamlarda kanunlara uygun olarak güvenli bir şekilde saklanır.

4.1. Elektronik Ortamlar

Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.),
Yazılımlar (ofis yazılımları, kurumsal & çalışan portal, Smart, Axapta, Securitas vakıf),
Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
Video Kaydı ve Ses Kaydı, Şirket bilgisayarları
Mobil cihazlar (telefon, tablet, pda vb.)
Optik diskler (CD, DVD vb.)
Çıkartılabilir bellekler (USB, Hafıza Kart vb.),
Yazıcı, tarayıcı, fotokopi makinesi

4.2. Fiziki Ortamlar

Kâğıt
Manuel veri kayıt sistemleri (ziyaretçi defteri, görev yeri defteri, matbu formlar, özlük dosyaları)
Yazılı, basılı, görsel ortamlar.

4.3. Bulut Ortamlar

Securitas Türkiye bünyesinde yer almamakla birlikte, Securitas Türkiye'nin kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır. Örn; Azure ortamları.

5. SAKLAMA VE İMHAYA İLİŞKİN GENEL İLKELER

Securitas Türkiye tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilir:

- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'a ve ilgili mevzuat hükümlerine, Yönetmelik'e, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilir.
- Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Securitas Türkiye tarafından kayıt altına alınır ve söz konusu kayıtlar 3 (üç) yıl süreyle saklanır.
- Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Securitas Türkiye tarafından belirlenir.
- Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Securitas Türkiye tarafından resen veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta İlgili Kişi tarafından Securitas Türkiye'ye başvurulması halinde;
  - İletilen talepler en geç 30 (otuz) gün içerisinde cevaplandırılır,

- Kişisel verileri işleme şartları ortadan kalkmışsa, talebe konu kişisel veriler imha edilir ve ayrıca imhası gereken talebe konu verilerin Securitas Türkiye tarafından üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye Kişisel Veri Yönetim Müdürlüğü tarafından bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir.

5.1. Saklamayı Gerektiren Amaçlar ve Hukuki Sebepler

Kanunun 3üncü 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, Securitas Türkiye faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre zarfında saklanır.
Securitas Türkiye, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek.
- Çalışan adaylarının başvuru, seçme ve yerleştirme süreçlerini yürütmek.
- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülükleri yerine getirmek.
- Çalışanlar için eğitim, etkinlik ve organizasyon faaliyetlerini yürütmek.
- Kurumsal iletişim vasıtalarını oluşturmak ve iletişim süreçlerini yürütmek.
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş faaliyetlerini ve işlemleri ifa edebilmek.
- Hizmet sözleşmeleri kapsamında; müşteri yetkilisi ve müşteri çalışanlarının tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Acil durum süreçlerini yürütmek.
- Bilgi güvenliği süreçlerini yürütmek.
- Finans, muhasebe, bütçe ve raporlama süreçlerini yürütmek.
- İşyeri sıfatıyla konuşlandığı fiziksel mekânların güvenliğini temin etmek.
- İş sağlığı ve güvenliği faaliyetlerini yürütmek.
- Mal ve veya hizmet alımı süreçlerini yönetmek.
- Pazarlama analiz çalışmalarını yürütmek.
- Hizmet alan ve hizmet sunan sıfatıyla sözleşme süreçlerini yürütmek.
- Securitas Türkiye'nin fiziksel mekanlarını veya internet sitesini ziyaret eden kişilerin kaydını oluşturulmak ve takibini yapmak.
- Securitas Türkiye'ye iletilen her türlü talep, istek ve şikâyetin değerlendirme ve takibini yapmak.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Securitas Türkiye ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Taşınır mal ve kaynaklarının güvenliğini temin etmek.
- Denetim faaliyetlerinin yürütülmesi kapsamında yetkili kurum ve kuruluşlar ile bilgi paylaşmak.

Saklamayı gerektiren hukuki sebepler aşağıdaki gibidir:

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Securitas Türkiye'nin meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin Securitas Türkiye'nin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

Securitas Türkiye, faaliyetleri çerçevesinde işlediği kişisel verileri, ilgili mevzuatta öngörülen süre kadar muhafaza eder. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5237 sayılı Türk Ceza Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

5.2. İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

Aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Securitas Türkiye tarafından resen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya yürürlükten kaldırılması sebebiyle gerekli olması hali,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların (hukuki sebeplerin) ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- İlgili kişinin, Kanun'un 11. maddesindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun Securitas Türkiye tarafından kabul edilmesi,
- Securitas Türkiye'nin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması 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 sebebin olmaması.

5.3. Saklamayı Gerektiren Amaç ve Hukuki Sebeplerin Ortadan Kalkması Durumunda Yapılacaklar

Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme şartları ortadan kalkan kişisel veriler, Securitas Türkiye tarafından, iş ihtiyaçları göz önüne alınarak uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir.
Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde Securitas Türkiye kişisel verinin kendi bünyesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verilir. Tereddüt duyulan durumlarda Kişisel Veri Yönetim Müdürlüğü'nden görüş alınarak gerekli işlem yapılır.
Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

5.4. Kişisel Verileri Saklama ve İmha Süreleri

- Kişisel veri işleme faaliyetleri kapsamındaki tüm kişisel verilerle ilgili Kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta (*yalnızca VERBİS' kayıt yükümlüsü olan Securitas Türkiye Şirketleri için*) ;
- Süreç / faaliyet bazında saklama süreleri ise işbu Kişisel Veri Saklama ve İmha Politikasında

yer alır.

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo; Securitas Türkiye kişisel veri işleme envanterinde yer alan saklama süreleri ve dayanakları esas alınarak oluşturulmuş olup gereklilik halinde Kişisel Veri Yönetim Müdürlüğü değerlendirmeleri de alınarak güncellenecektir. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi elektronik ve bulut ortamlarda bulunan kişisel veriler için Bilgi Teknolojileri Koordinatörlüğü, matbu ortamda bulunan kişisel veriler için ise veri işleyen departmanın KVK temsilcisi tarafından yerine getirilir. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır.

Tablo 1: Faaliyet bazında saklama ve imha süreleri tablosu

Faaliyet	Saklama Süresi
Bütçe ve Raporlama Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Finans ve Muhasebe İşleri	Hukuki ilişkinin sona ermesi + 10 yıl
Mali Denetim ve Kontrol Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Şirket Yönetim İşleri	Hukuki ilişkinin sona ermesi + 10 yıl
Mal ve Hizmet Sözleşmesi Süreçleri	Hukuki ilişkinin sona ermesi + 10 yıl
Personel İşlemleri	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Hukuki Süreçler (Dava ve İcra vs)	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Hasar Yönetim İşlemleri	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Satış & Pazarlama Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Müşteri Memnuniyeti Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Pazarlama Analiz Faaliyetleri	3 Ay
İş Geliştirme Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Reklam, Kampanya ve Promosyon Faaliyetleri	3 Ay
Talep, Şikâyet Yönetimi	Hukuki ilişkinin sona ermesi + 10 yıl
Eğitim, Etkinlik & Organizasyon Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl

Stratejik İstihdam Faaliyetleri	6 Ay
Bordro ve Özlük İşlemleri	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
İdari İşler	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Satınalma Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Bilgi Güvenliği İşlemleri	2 Yıl
İş Sağlığı ve Güvenliği Faaliyetleri	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Acil Durum Proje Süreçleri	Hukuki ilişkinin sona ermesi + 15 Gün
Acil Durum Yönetimi Süreçleri	iş kazası + 15 Yıl, hukuki ilişki/iş akdinin sona ermesi + 10 Yıl
Puantaj ve Hakediş İşlemleri	Hukuki ilişkinin sona ermesi + 10 yıl
Alarm Haber Alma İşlemleri	2 Yıl
Uzaktan İzleme Denetim Faaliyetleri	Hukuki ilişkinin sona ermesi + 10 yıl
Ziyaretçi Kayıtları	5 Yıl
Fiziksel Mekân Güvenliği İşlemleri	Hukuki ilişkinin sona ermesi + 10 yıl
Kamera Kayıtları	90 gün

5.4.1. Periyodik İmha Süreleri

Kişisel Verileri Periyodik İmha süresi Securitas Türkiye tarafından tespit ve tayin edilir; ancak her hâlükârda bu süre Yönetmeliğin 11 inci maddesi gereğince 6 (altı) ayı geçemez. Buna göre;

- Veri Sorumluları Siciline kaydolmakla yükümlü bulunan aşağıdaki Securitas Türkiye Şirketleri için her yıl Haziran ve Aralık aylarında periyodik imha işlemleri gerçekleştirilir.
    - *Securitas Güvenlik Hizmetleri A.Ş.*
    - *Securitas Entegre Güvenlik Çözümleri ve Hizmetleri A.Ş.*
    - *Securitas Tesis Yönetim ve Danışmanlık Hizmet A.Ş.*

- Veri Sorumluları Siciline kaydolmakla yükümlü olmayan yukarıda sayılan Şirketler dışında kalan Securitas Türkiye Şirketleri için ise imha yükümlülüğünün ortaya çıktığı tarihi izleyen 3 ay içerisinde imha işlemleri gerçekleştirilir.

6. KİŞİSEL VERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Securitas Türkiye tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Securitas Türkiye bünyesinde bulunan kişisel veriler Tablo1'de belirtilen şekilde silinir.

Tablo 2: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	İşlem
Sunucularda/Elektronik ortamda Yer Alan Kişisel Veriler	Süresi dolmuş verilerin bulunduğu tablolar gözden geçirilir. Verilerin silinmesi veri tabanları üzerinde gerçekleştirilir.
Bulut Ortamda Yer Alan Kişisel Veriler	Bulut sisteminde veriler silme komutu verilerek silinir. Silme işlemini yapan kullanıcı bulut sistemi üzerinde silinmiş verileri geri getirme yetkisi yoktur.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilir, mümkün olmayan durumlar söz konusu olduğunda geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilir.
Taşınabilir Medyada Bulunan Kişisel Veriler	Taşınabilir medyada bulunan kişisel veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinir.

6.2. Kişisel Verilerin Yok Edilmesi

Securitas Türkiye bünyesinde bulunan kişisel veriler Tablo 2'de belirtilen şekilde yok edilir.

Tablo 3: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	İşlem
Sunucularda/Elektronik Ortamda Yer Alan Kişisel Veriler	Kişisel Veriler saklandığı sunucu diskleri üzerinden truncate işlemi ile silinerek üzerine yazma işlemi uygulanır. Mobil cihazlar fabrika ayarlarına getirilir.
Bulut Ortamda Yer Alan Kişisel Veriler	Kişisel verilerin saklanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Hizmet ilişkisi sona erdiğinde şifreler yok edilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler ve ve ya talep üzerine yok edilmesi uygun görülenler kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

Taşınabilir Medyada Bulunan Kişisel Veriler	Taşınabilir medyada bulunan kişisel veriler; destekleniyorsa <block erase> komutu kullanılarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemi kullanılarak yok edilir. Çalışanların taşınabilir medyaya aktardığı verilerin loglaması yapılarak kayıt tutulur.

6.3. 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 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.

Securitas Türkiye bünyesinde bulunan kişisel veriler Tablo 4'de belirtilen şekilde anonim hale getirilir.

Tablo 4: Kişisel Verilerin Anonim Hale Getirilmesi

Veri Kayıt Ortamı	**İşlem**
Sunucularda/Elektronik Ortamda Yer Alan Kişisel Veriler	Değişkenleri çıkartma yöntemi ve genelleştirme kullanılır. İlgili kişisel veriler özel bir değerden daha genel bir değere çevrilir. Raporlar kişi bazlı olarak değil, bölge/iş süreci/eğitim bazlı olarak tablolaştırılır.
Bulut Ortamda Yer Alan Kişisel Veriler	Değişkenleri çıkartma yöntemi ve genelleştirme kullanılır. İlgili kişisel veriler özel bir değerden daha genel bir değere çevrilir. Raporlar kişi bazlı olarak değil, bölge/iş süreci/eğitim bazlı olarak tablolaştırılır.
Fiziksel Ortamda Yer Alan Kişisel Veriler	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçı geri getirilemez şekilde kesilerek ya da mürekkep karalanarak anonimleştirme sağlanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Değişkenleri çıkartma yöntemi ve genelleştirme kullanılır. İlgili kişisel veriler özel bir değerden daha genel bir değere çevrilir. Raporlar kişi bazlı olarak değil, bölge/iş süreci/eğitim vb bazlı olarak tablolaştırılır. Çalışanların taşınabilir medyaya aktardığı verilerin loglaması yapılarak kayıt tutulur.

7. GÜVENLİK TEDBİRLERİ

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla Kanun'un 12. maddesindeki ilkeler çerçevesinde, Securitas Türkiye tarafından idari ve teknik tedbirler alınır.

7.1. İdari Tedbirler

Securitas Türkiye idari tedbirler kapsamında;

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri uygular.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları düzenler.
- Çalışanlara iş sözleşmesi yanında gizlilik sözleşmesi / taahhüdü imzalatır.
- Şirket içi kişisel veri işleme faaliyetlerini kayıt altında tutup güncelleyeceği bir envanter hazırlar.
- Saklanan kişisel verilere şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi dikkate alınır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin protokol imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar. İmzalanan sözleşme ve veya protokol veri güvenliği hükümleri içerir.
- Kişisel veri güvenliği adına politika ve prosedürler oluşturarak veri yönetiminde ilgili prosedürleri takip eder.
- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- Kişisel veri güvenliği sorunlarını hızlı bir şekilde KVK Uzman Yardımcısı ile Bilgi Teknolojileri Koordinatörlüğüne raporlar.
- Mümkün olduğunca az kişisel veri elde eder.

7.2. Teknik Tedbirler:

Securitas Türkiye teknik tedbirler kapsamında;

- Ağ güvenliği ve uygulama güvenliğini sağlar.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemlerini alır.
- Çalışanlar için yetki matrisi oluşturur.
- Erişim loglarını düzenli olarak tutar.
- Gerektiğinde veri maskeleme önlemi uygular.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerini kaldırır.
- Güncel anti-virüs sistemlerini aktif tutar.
- Güvenlik duvarları kullanır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliğini sağlar.
- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerini sürekli takip ederek gerekli güvenlik testlerinin düzenli olarak yaptırılmasını sağlar.
- Kişisel veriler yedeklenir ve yedeklenen kişisel verilerin güvenliğini sağlar.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygular ve bunların takibini yapar.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutar.
- Mevcut risk ve tehditleri belirler.
- Saldırı tespit ve önleme sistemleri kullanır.
- Siber güvenlik önlemleri alır ve uygulanmasını sürekli takip eder.

8. GÖREV VE SORUMLULUKLAR

8.1. Kişisel Verileri Koruma Komitesinin Görev ve Yetkileri

Kişisel Verileri Koruma Komitesi, işbu Politika'nın ilgili iş birimlerine duyurulmasından ve gereklerinin yerine getirilmesinin takibinden sorumludur. Kişisel Verileri Koruma Komitesi kişisel verilerin korunmasına ilişkin mevzuat değişiklikleri, Kurulun düzenleyici işlemleri ile kararları, mahkeme kararları veya süreç, uygulama ve sistemlerdeki değişiklikler gibi durumları ilgili iş birimlerinin takip etmesi ve gerekiyorsa iş süreçlerini güncellemeleri için gerekli

duyuruları ve bildirimleri yapar ve Kanun ve ikincil düzenlemeleri ile Kurulun kararları ve düzenlemeleri, mahkeme kararları ve sair yetkili makamların kararlarının ve/veya taleplerinin incelenmesi, değerlendirilmesi, takibi ve sonuçlandırılmasına yönelik süreçleri belirler ve ilgili birimlere duyurur.

8.2. Kişisel Veri Saklama ve İmha Süreçlerinde Yer Alacak Kişiler ve Sorumlulukları

Securitas Türkiye içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette Securitas Türkiye nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur. Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerinde bulunması durumunda, söz konusu veri Bilgi Teknolojileri Koordinatörlüğü tarafından saklanır. İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak Bilgi Teknolojileri Koordinatörlüğü tarafından yapılır.

8.3. Kişisel Veri Saklama ve İmha Süreçleri İhlal Durumları ve Yaptırımlar

Çalışanların politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğundadır. Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın amiri tarafından bağlı bulunan bir üst amire bildirilir. Aykırılığın önemli boyutta olması halinde ise üst amir tarafından vakit kaybetmeksizin Kişisel Veri Yönetim Müdürlüğü'ne bilgi verilir. Kişisel Veri Yönetim Müdürlüğü gerekli ise Kişisel Verileri Koruma Komitesi'nin de görüşünü alarak KVK mevzuatı çerçevesinde gerekli işlemleri koordine eder. Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları disiplin süreci işlemlerini koordine eder.

9. YÜRÜRLÜK

İşbu Politika tüm çalışanlara duyurularak yürürlüğe girer ve yürürlüğü itibariyle Securitas Türkiye bünyesinde kişisel veri işleyen herkes için bağlayıcı kabul edilir. Politika her yıl Ocak ayında ve veya gerekli hallerde Kişisel Veri Yönetimi Müdürlüğü tarafından gözden geçirilerek düzenlenir.