SNI TEKNOLOJİ HİZMETLERİ A.Ş.

KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI

I. Amaç

İşbu Kişisel Verilerin Saklanması ve İmhası Politikasının ("Politika") amacı; **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** ("SNI") tarafından işlenen kişisel verilerin işlenme sürelerinin belirlenmesi ve işleme süresi ve/veya işleme amacı ortadan kalkan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin kriter ve yöntemlerin ortaya konulmasıdır.

İşbu Politika'da 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkındaki Yönetmeliğin 6'ncı maddesinde yer alan veri güvenliğini sağlamak için alınmış teknik ve idari tedbirlere de yer verilmektedir. 30 Aralık 2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik hükümleri ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi de bu çerçevede dikkate alınmıştır.

II. Kapsam

İşbu Politika; 6698 Sayılı Kişisel Verilerin Korunması Kanununun 7'nci maddesi uyarınca "veri sorumlusu" sıfatıyla **SNI TEKNOLOJİ HİZMETLERİ A.Ş.**'nin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile işlediği, elektronik ve/veya kağıt ortamda yer alan ve işleme şartları sona ermiş tüm kişisel verileri silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini kapsamaktadır.

III. Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklama

SNI; bünyesindeki çeşitli departmanlar tarafından iş tanımları doğrultusunda yürütülen iş süreçleri ve bu süreçlere bağlı faaliyetleri gerçekleştirebilmek amacıyla çalışan, çalışan adayı, çalışan yakını, müşteri, müşteri iş ortağı, müşteri çalışanı, iş ortağı, tedarikçi, ziyaretçi, çevrimiçi ziyaretçilerine ait kişisel verileri işlemektedir. Bu kişisel verileri mevzuatta öngörülen veya ilgili departman tarafından kişisel veri işleme amacı çerçevesinde belirlenen süreler boyunca saklamaktadır. Tüm bu akış Kişisel Veri İşleme Envanterinde yer almaktadır. İlgili saklama süreleri sona erdiğinde ise, işbu Politika'da belirlenen silme, yok etme veya anonim hale getirme yöntemleri ile işleme amacı ortadan kalkan kişisel veriler imha edilmektedir.

IV. Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler

SNI, işlediği kişisel verilere hukuka aykırı erişimin engellenmesi, bu verilerin hukuka aykırı işlenmesinin önlenmesi ve kişisel verilerin muhafazasının sağlanmasına ilişkin olarak aşağıdaki teknik ve idari tedbirleri almaktadır:

Anti-Virüs

SNI'ın bilgi teknolojileri altyapısında bulunan tüm PC ve Sunucularda periyodik olarak güncellenen anti-virüs uygulaması yüklüdür.

Firewall

SNI sunucularını barındıran Data Center ve Felaket Kurtarma Merkezleri periyodik olarak güncellenen yazılım yüklü firewalllarca korunmakta olup, ilgili yeni nesil firewalllar tüm personellerin internet bağlantılarını kontrol etmekte ve bu kontrol sırasında virüs ve benzeri tehditlere karşı koruma sağlamaktadır.

VPN

İşyeri sunucu sistemlerine IP-SEC VPN ile bağlanmakta olup, 2 nokta arasındaki trafik şifreli bir şekilde iletilmektedir.

Tedarikçiler de **SNI** sunucu ya da sistemlerine Firewalllar üzerinde tanımlı bulunan SSL-VPN aracılığı ile erişim sağlayabilmektedirler. Her bir tedarikçi için ayrı SSL-VPN tanımı yapılmış olup, yapılan tanımlama ile tedarikçi sadece kullanması gereken ya da yetkilendirmesi yapılan sistemlere erişim sağlamaktadır.

Network Yapılandırması

SNI, işyerinde bulunan network ağını yapılandırmış ve bu sayede networke erişimi, sadece yetki verilen kişilerle sınırlamıştır.

Kullanıcı Tanımlamaları ve Need to Know

SNI ve işyeri çalışanlarının **SNI** sistemlerine olan yetkileri sadece iş tanımları ile gerekli olduğu ölçüde sınırlandırılmış olup, herhangi bir yetki ve görev değişikliği söz konusu olması durumunda sistemsel yetkileri de ivedi olarak güncellenmektedir.

Bilgi güvenliği Tehdit ve Olay Yönetimi

SNI sunucularında ve Firewallarında oluşan olaylar "Bilgi Güvenliği Tehdit ve Olay Yönetimi" sistemine aktarılmaktadır. Bu sistem güvenlik tehdidi oluştuğunda sorumlu personelleri uyarmakta ve ivedi bir şekilde tehdide cevap verilmesi imkanı sağlamaktadır.

Sızma Testi

Periyodik olarak **SNI** sistemindeki sunuculara, bilgisayarlarına ve örnek bir işyerine sızma testi manuel olarak tedarikçi bir firma tarafından yapılmaktadır. Bu test sonucunda oluşan güvenlik açıkları kapatılarak, ilgili güvenlik açıklarının kapatıldığına dair doğrulama testi yapılmaktadır. Ayrıca Bilgi Güvenliği Tehdit ve Olay Yönetimi sistemi tarafından da otomatik olarak sızma testi yapılmaktadır.

BGYS

SNI bünyesinde oluşturulan BGYS toplantılarında kontrol formunda yer alan başlıklar aylık olarak Bilgi Teknolojileri Direktörü ve CFO tarafından denetlenmektedir. **2014** yılından bu yana Cobit standartlarında ve GV'nin denetim standartlarına uyumlu olarak oluşturulan denetim listesi periyodik olarak kontrol edilmektedir.

Farkındalık Eğitimi

SNI çalışanlarının çeşitli bilgi güvenliği ihlallerine karşı farkındalıklarını artırmak ve bilgi ihlali olaylarında insan faktörünün etkisini en aza indirmek için düzenli olarak eğitim verilmektedir. Tüm çalışanlar Siber Güvenlik ve Bilgi Güvenliği eğitimini almışlardır.

Clean Table & Clean Desk

SNI iç kuralları uyarınca SNI çalışanları "clean table & clean desk" prensibine uymakla yükümlüdür.

Diğer

Kişisel verilerin alındığı web sitesindeki tüm alanlar SSL ile korur.

Birincil işleme amacı dışında kalan tüm ikincil veri işlemeler bakımından, Pseudonymization (takma adlı veri) yöntemini kullanır (Örnek: Ahmet Yılmaz → "A… Y…").

Kağıt ortamdaki kişisel verilerin mutlaka kilitli dolaplarda muhafaza edilmesini ve sadece yetkili kişiler tarafından erişilmesini sağlar.

İşyerini üçüncü kişilerin izinsiz girişini engeller ve üçüncü kişilerin, bir refakatçi eşliğinde işyerini ziyaret etmesini sağlar.

İlgili verinin saklanması gerekliliği ortadan kalktıktan ya da çalışanın şirket ile ilişkisi bittikten sonra hem şirket tarafından sağlanan hem de şahsi cihaz ve ortamlardaki kişisel verilerin silinmesi sağlanmaktadır.

Hizmet alınan üçüncü taraflarca işlenen kişisel veriler, ilişki sona erdiği takdirde üçüncü taraflara ait sistemlerden silinmektedir.

SNI'ın gerekli bilgi güvenliği önlemlerini almasına karşın, **SNI** tarafından işletilen platformlara veya **SNI** sistemine yapılan saldırılar sonucunda kişisel verilerin zarar görmesi veya yetkisiz üçüncü kişilerin eline geçmesi durumunda, **SNI** bu durumu derhal sizlere ve Kişisel Verileri Koruma Kurulu'na bildirir ve gerekli önlemleri alır.

V. Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler

SNI; işlediği kişisel verilerin hukuka uygun olarak imha edilmesini sağlamak amacıyla **SNI** nezdinde bu işten sorumlu bir birim ("Teknik Birim") oluşturmuştur. Teknik Birim; kişisel verilerin silinmesini, sadece ilgili kullanıcılar tarafından kişisel verinin işlenebileceği, ilgisi olmayan diğer tüm bölümler için verinin işlenemeyeceği şekilde sağlar. Elektronik ortamdaki kişisel veriler için gerekli olduğu ölçüde maskeleme yöntemleri kullanılır. Kağıt ortamdaki kişisel veriler için silme işlemi, silinmesi gereken kişisel verilerin karartılması şeklinde gerçekleştirilir.

5.1. Kişisel Verilerin Silinmesi

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

5.1.1. Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi
- İlgili kullanıcıların kişisel veriler kapsamında erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması

- Silinen herhangi bir kişisel verinin tekrardan sisteme dahil olması durumunda, kişisel verilerin geri döndüğünün fark edildiği anda derhal silinmesi

5.1.2. Kişisel Verilerin Silinmesi Yöntemleri

a) Hizmet Olarak Uygulama Türü Bulut Çözümleri

Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

b) Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karatma işlemi ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

c) Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

d) Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

e) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

İşleme amacı tamamen ortadan kalkan kağıt ve elektronik ortamdaki kişisel veriler Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Rehberine uygun olarak yok edilir veya yine bu Rehber'de öngörülen yöntemlerle anonim hale getirilir. Teknik Birim tarafından gerçekleştirilen tüm silme, yok etme veya anonim hale getirme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Kağıt ortamdaki kişisel veriler bakımından ise bu işlemlerin gerçekleştirildiğine ilişkin tutanak düzenlenir ve Teknik Birim tarafından muhafaza edilir. Elektronik ve kağıt ortamdaki kişisel verilere ilişkin silme, yok etme veya anonim hale getirmeye ilişkin kayıtlar üç yıl süre ile saklanır. **SNI**; kişisel

verileri saklama süreleri boyunca sadece ilgili departmanların bu verilere erişimini sağlayacak şekilde "silme" yöntemini kullanır. Saklama sürelerinin bitmesi ve kişisel verinin saklanmasını gerektirecek herhangi bir başka amacın mevcut olmaması halinde ise anonim hale getirme yöntemini kullanır.

5.2. Kişisel Verilerin Yok Edilmesi

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

5.2.1. Kişisel Verilerin Yok Edilmesi Yöntemler,

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gerekir.

a) Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

- **Fiziksel Yok Etme:** Optik medya 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. Katı ha diskler bakımından üzerine yazma ya da de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
- **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en yaz yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

b) Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

- **Ağ cihazları (switch, router vb.):** Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünlerin, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da bir kaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, SSD, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu

kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Veri kayıt ortamı sabit olan yazıcı, gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c) Kağıt Ortamlar

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılığı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

d) Bulut Ortamı

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi gerekmektedir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemi ise aşağıdaki şekilde gerçekleştirilir.

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,
- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması, gerekir.

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

SNI, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbiri almıştır. **SNI**, Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi'nde belirtilen yöntemlerle kişisel verileri anonim hale getirecektir.

VI. Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanları, birimleri ve görev tanımları

SNI; Kişisel Verilerin Saklanması ve İmhası Politikası kapsamında saklama ve imha süreçlerine ilişkin olarak aşağıdaki unvan, birim ve görev tanımlarına sahip kişileri görevlendirir:

a) **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** bünyesinde kişisel veri işleyen tüm departmanların "veri sahipleri". Veri sahipleri gerek kendi departmanlarının kişisel veri işleme envanterinin güncelliğinin sağlanması gerek kişisel veri saklama ve imha süreçlerinin takibi için bölümünde çalışan bir başka kişiyi görevlendirebilir.

b) Teknik Birim.

VII. Saklama ve imha süreleri tablosu

Saklama ve imha süreleri tablosuna her bir departman bazında hazırlanmış Kişisel Veri İşleme Envanteri'nde yer verilmekte olup, yaşayan bir doküman olan ve ilgili departmanlarca zaman zaman güncellenecek Envanter'in takibi Teknik Birim tarafından yapılarak aynı Birim tarafından muhafaza edilmektedir.

VIII. Periyodik imha süresi

SNI; saklama süresi sona eren ve kişisel verinin saklanmasını gerektirecek başka herhangi bir veri işleme amacı mevcut olmayan kişisel verileri, saklama süresinin sona ermesini takiben 6 ay içerisinde imha eder.

IX. İlgili Kişinin talep etmesi durumunda kişisel verilerin silme ve yok etme süreleri

İlgili kişi, **SNI**'a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; **SNI**, talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. **SNI**, ilgili kişilerin silme veya yok etme taleplerini en geç **"otuz gün"** içinde sonuçlandırır.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa; **SNI** bu durumu üçüncü kişiye bildirerek söz konusu kişisel verilerin silinmesi veya yok edilmesini talep eder.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep **SNI** tarafından Kişisel Verilerin Korunması Kanunu'nun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç "otuz gün" içinde yazılı olarak ya da elektronik ortamda bildirilir.

X. Kişisel Verilerin Saklanması ve İmhası Politikasında yapılacak Güncellemeler

SNI, işbu politikada yapılacak güncellemeleri Genel Müdür onayına sunduktan sonra revize edilen maddeler, revizyon ve onay tarihi ile birlikte yayımlar.

XI. İlgili Dokümanlar

Kurumsal Bilgi Güvenliği Politikası

SNI TEKNOLOJİ HİZMETLERİ A.Ş. Gizlilik ve Kişisel Verilerin Korunması Politikası

Kişisel Veri İşleme Envanteri

İşbu Politika'da yapılan değişiklikler aşağıdaki tabloda yer almaktadır.

DÖKÜMAN TARİHÇESİ		
Versiyon	**Yayım Tarihi**	**Değişikliğin Tanımı**
v1	13.06.2017	İlk Yayım
v2	08.01.2020	Optimizasyon

SAKLAMA VE İMHA SÜRELERİ TABLOSU

Süreç	Saklama Süresi	İmha Süresi
Müşterilere, Müşteri Çalışanlarına, Müşteri İş Ortaklarına İlişkin Kişisel Veriler	Hukuki ilişki sona erdikten itibaren 10 yıl; 6563 Kanun ve ilgili ikincil mevzuat uyarınca 3 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
İş Çözüm Ortağı / Tedarikçilere İlişkin Kişisel Veriler	Hukuki ilişki sona erdikten itibaren 10 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
İş Başvurusu Sırasında Alınan CV ve Özlük Bilgileri	2 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Çağrı Merkezi Ses Kayıtları	3 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Çalışanlara İlişkin E-posta Arşivleri	Hukuki ilişki sona erdikten sonra 1 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Çevrimiçi Müşterilere İlişkin Kişisel Veriler	10 yıl; 6563 Kanun ve ilgili ikincil mevzuat uyarınca 3 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Potansiyel Müşterilere İlişkin Kişisel Veriler	1 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Ziyaretçilere İlişkin Kişisel Veriler (Kamera Kayıtları)	3 ay	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Ziyaretçi / Çevrimiçi Ziyaretçilere İlişkin Kişisel Veriler	2 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha
Muhasebe ve Finansal İşlemlere İlişkin Tüm Kayıtlar	10 yıl	Saklama Süresi Sona Erdikten Sonra İlk Periyodik İmha