OSKA ÇELİK EV İNŞAAT SANAYİ VE TİCARET LİMİTED ŞİRKETİ

KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

İÇİNDEKİLER

1. AMACI

OSKA ÇELİK EV **İNŞAAT** Sanayi ve Ticaret Limited Şirketi **("Şirket")** bu Kişisel Veri Saklama ve İmha Politikası **("Saklama ve İmha Politikası")** ile kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanununa **("Kanun")** uygun olarak teknik ve idari korunması, kişisel verilerin işlenme şartlarının ortadan kalkması halinde, 28/10/2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik **("Yönetmelik")** hükümlerinin uygulamasını düzenlemek amacıyla çıkarılmaktadır.

2. KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki listelenen ortamlarda başta Kanun hükümleri olmak üzere ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:

- E-Posta Kutusu
- Microsoft Office Programları
- Görüntü Kayıt Cihazları
- Yazılımlar (ofis yazılımları, portal)
- Bilgisayarlar (Masaüstü, dizüstü)

Fiziksel ortamlar:

- Birim Dolapları
- Klasörler
- Arşiv

3. SAKLAMAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, Şirket tarafından özellikle:

a. Faaliyetlerin sürdürülebilmesi,
b. Hukuki yükümlülüklerin yerine getirilebilmesi,
c. Çalışan haklarının ve yan haklarının planlanması ve ifası,
d. İş ilişkilerinin yönetilebilmesi,

Amacıyla yukarıda sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler:

1- DAYANAK KANUNLAR:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 1219 sayılı Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanun
- 6098 sayılı Türk Borçlar Kanunu,
- 5237 sayılı Türk Ceza Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 213 sayılı Vergi Usul Kanununun

2-) HUKUKİ SEBEPLER:

a. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
b. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması,
c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirket'in meşru menfaatinin olması,
d. Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi,
e. Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.
g. İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.
h. VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Şirket tarafından re'sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

a. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
b. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
c. Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
d. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
e. İlgili kişinin, Kanun'un 11. Maddesinin 2 (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
f. Veri sorumlusunun, 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,
g. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER

Şirket, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmak veya yaptırmaktadır. İşlenen kişisel verilerin teknik ve idari tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi durumunda, Şirket bu durumu mümkün olan en kısa süre içerisinde ilgili birimlere haber verir.

4.1 Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
  - Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

4.2 İdari Tedbirler

- Çalışanlar, kişisel verilere hukuka aykırı erişimi engellemek için alınacak teknik tedbirler konusunda eğitilmektedir.
- İş birimi bazında kişisel veri işlenmesi hukuksal uyum gerekliliklerine uygun olarak Şirket içinde kişisel verilere erişim ve yetkilendirme süreçleri tasarlanmakta ve uygulanmaktadır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- Şirket personeli ile arasındaki ilişkiyi düzenleyen ve kişisel veri içeren her türlü belgeye kişisel verilerin hukuka uygun olarak işlenmesi için Kanun ile öngörülen yükümlülüklere uygun hareket edilmesi gerektiği, kişisel verilerin ifşa edilmemesi gerektiği, kişisel verilerin hukuka aykırı olarak kullanılmaması gerektiği ve kişisel verilere ilişkin gizlilik yükümlülüğünün Şirket ile olan iş akdinin sona ermesinden sonra dahi devam ettiği yönünde kayıtlar eklemiştir.

- Çalışanlar, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonrada devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır.
- Şirket tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- Gerekli hallerde kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında eğitimleri verir.
- Şirket, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

5. KİŞİSEL VERİLERİN İMHA EDİLMESİNE İLİŞKİN ALINAN TEDBİRLER

Şirket ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir veya yok edebilir. Kişisel verilerin silinmesi akabinde ilgili kişiler hiçbir şekilde silinen verilere tekrardan erişilemeyecek ve kullanılmayacaktır. Şirket tarafından kişisel verilerin imha süreçlerinin tanımlanması ve takip edilmesine ilişkin etkin bir veri takip süreci yönetilecektir. Yürütülen süreç sırası ile silinecek verilerin tespit edilmesi, ilgili kişilerin tespiti, kişilerin erişim yöntemlerinin tespiti ve hemen akabinde verilerin silinmesi olacaktır.

Şirket kişisel verileri yok etmek, silmek veya anonim hale getirmek için verilerin kaydedildiği ortama bağlı olarak aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

5.1 Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesine İlişkin Yöntemler

5.1.1 Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin silinmesi yöntemi olarak Şirket aşağıdaki yöntemlerden bir veya birkaçını kullanabilir:

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
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.
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.
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.

Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır. Gerekli olduğu zaman bir uzman tarafından yardım alınarak güvenli olarak silinecektir.

5.1.2 Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin aşağıdaki yöntemlerle hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Fiziksel Yok Etme

Kağıt İmha Makinesi ile Yok Etme

De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir.

5.1.3 Kişisel Verileri Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Şirket kişisel verileri anonim hale getirmek için aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

Maskeleme (Masking): Veri maskeleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.

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

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

Şirket kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin re'sen karar alabilecek ve seçmiş olduğu kategoriye göre kullanacağı yöntemi de serbestçe belirleyebilecektir.

Ayrıca Yönetmelik'in 13. maddesi kapsamında ilgili kişinin başvuru esnasında kendisine ait kişisel verinin silinmesi, yok edilmesi yahut anonim hale getirilmesi kategorilerinden birini seçmesi halinde de ilgili kategoride kullanılacak yöntemler konusunda Şirket serbesti içinde olacaktır.

6. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Şirket, kişisel verileri işlendikleri amaç için Ek-1'de belirtilen süreler boyunca saklar. Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Mevzuatta öngörülmüş bir süre olmaması halinde kişisel veriler Ek-1'deki tabloda yer alan kişisel verilerin tutulması için azami süre boyunca saklanacaktır. Bu süreler; Şirket'in veri kategorileri ve veri sahibi kişi grupları değerlendirilerek; bu değerlendirme sonucu elde edilen verilerin kanunlarda yer alan yükümlülüklerin yerine getirilmesini sağlayacak ve azami Türk Borçlar Kanunu'nda yer alan zamanaşımı süresi (10 yıl) gözetilerek belirlenmiştir.

Bu sürelerin sona ermesi dolayısıyla silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı durumda Şirket bu tarihi takip eden ilk periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir.

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 üç yıl süreyle saklanır.

7. PERİYODİK İMHA SÜRELERİ

Yönetmeliğin 11 inci maddesi gereğince, periyodik imha süresini 6 ay olarak belirlenmiştir. Buna göre, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir. Söz konusu sistemlerde bilgilerin tekrar geri getirilmeyecek şekilde, verilerin kaydedildiği varsa evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülmeyecek şekilde silinecektir.

8. PERSONEL

Kanun kapsamında Şirket veri sorumlusu sıfatıyla, Yönetmelik'in 11. maddesinin 1. fıkrasına dayanarak, Kanunun veri saklama ve imha süreci uygulanması bakımından yükümlülükleri yerine getirilecek KVKK temsilci Saklama ve İmha Politikası belirlenmiştir.
Sınırları belirlenmiş bu kişiler Türk Ticaret Kanunu, Borçlar Kanunu ve Türk Ceza Kanunu kapsamında kendi yetki sınırları içinde gerçekleşen işlem ve eylemlerden sorumludur. Özellikle Kollukta, Savcılıklarda, kamu kurumlarında ve mahkemelerde Şirket'i temsil etme ile ifade vermeye yetkili olarak Şirket Kişisel Verileri Koruma temsilcisi seçilmiştir. Temsilci ilgili kullanıcıların Kanun ve Yönetmelik çerçevesinde hazırlanan Saklama ve İmha Politikası ve Kişisel Veri Politikası'na uygun davranıp davranmadığını denetlemekle yükümlü olacaktır. Temsilci belirtilen periyodik imha sürelerinde işbu Saklama ve İmha Politikası doğrultusunda gerçekleştirdiği işlemleri Şirket Yönetim kuruluna raporlayacaktır. Bu raporlar için yapılan çalışma sonuçlarında çıkan karar uygulamaya konulacaktır.

9. YAYINLAMA VE SAKLANMASI

POLİTİKA, ıslak imzalı olarak basılı kâğıtta düzenlenir ve İşyerinde ilgili dosyalarda saklanır. Şirketin bir internet sayfası olması halinde POLİTİKA aynı zamanda internet sayfasında da kamuya açıklanır.

10.REVİZYON VE YÜRÜRLÜKTEN KALDIRMA

Saklama ve İmha Politikası'nın değiştirilmesi, yürürlükten kaldırılması halinde yeni düzenleme "www.guneymasura.com" internet sitesinden ilan edilecektir

11.YÜRÜRLÜK

Bu Saklama ve İmha Politikası yayınlandığı tarihinde yürürlüğe girer.

EKLER

EK 1-Veri Saklama ve İmha Süreleri

EK 1- Veri Saklama ve İmha Süreleri

Veri Kategorisi	Saklama Süresi	İmha Süresi
Kimlik	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl+Aday başvuru tarihinden itibaren 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl+Aday başvuru tarihinden itibaren 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Lokasyon	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 12 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Özlük	İstihdamın sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlem	Yargı kararının kesinleşmesinden itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri İşlem	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekân Güvenliği	7 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem Güvenliği	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Risk Yönetimi	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans	İşlem tarihi veya hukuki ilişkinin sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mesleki Deneyim	İstihdamın sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Pazarlama	İstihdamın sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Görsel ve İşitsel Kayıtlar	Hukuki Süreç+10 yıl ,Kamera Kayıtları 7 gün,Organizasyon ve etkinlik fotoğrafları süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık Bilgileri	SGK HİZMETİ BİTİMİNDEN İTİBAREN 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	SGK HİZMETİ BİTİMİNDEN İTİBAREN 10 YIL	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışma Verisi	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Web Sitesi Kullanım Verileri	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Talep/Şikayet Yönetimi Bilgisi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İmzalar	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Araç Bilgileri	10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yabancı Oturma İzni Bilgileri	İstihdamın sonlanmasından itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde