VHV ALLGEMEINE SİGORTA

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. Amaç ve Dayanak

Bu politika, 6698 sayılı Kişisel Verilerin Korunması Kanununa dayanılarak çıkarılmış bulunan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca; VHV Sigorta A.Ş. tarafından işlenmekte olan kişisel verilerin saklanması ve imha edilmesi süreçlerinin mevzuata uygun olarak yerine getirilmesine yönelik usul ve esasların belirlenmesi amacıyla uygulamaya alınmıştır.

2. Tanımlar

Kanun	: 6698 Sayılı Kişisel Verilerin Korunması Kanunu
Yönetmelik	: Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik
Politika	: Kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yapılan kişisel veri saklama ve imha politikası
Kurum	: Kişisel Verileri Koruma Kurumu
Kurul	: Kişisel Verileri Koruma Kurulu
Kişisel Veri	: Kanun kapsamında bulunduğu sürece, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Veri Sorumlusu	: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
İlgili Kişi	: Kişisel verisi işlenen gerçek kişi
Veri Koruma Görevlisi	: Veri sorumlusuna iletilen başvuruların ilgili birimler ile koordinasyon sağlanarak başvuru sahibine gerekli yanıtın iletilmesinden sorumlu kişi
KVK Komitesi	: Veri Koruma Görevlisi yönetiminde veri sorumlusu çalışanlarından oluşan KVK karar ve yönetim komitesi
Alıcı grubu	: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
İlgili kullanıcı	: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler
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
Veri kayıt sistemi	: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi

İmha	: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
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 işlemi
Kişisel verilerin silinmesi	: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Kişisel verilerin yok edilmesi	: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Kişisel verilerin anonim hale getirilmesi	: Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi

3. Kayıt Ortamları

İşlenmekte olan kişisel veriler aşağıda belirtilen kayıt ortamlarında hukuka uygun bir şekilde muhafaza edilmektedir.

3.1. Elektronik Ortamlar

Masaüstü ve dizüstü bilgisayarlar

Ağ cihazları ve sunucular

Şirket bünyesinde kullanılan yazılımlar

Mobil cihazlar

Optik ve çıkarılabilir diskler

Yazıcı, tarayıcı, fotokopi makinesi gibi ofis araçları

3.2. Elektronik Olmayan Ortamlar

Kağıt, bloknot, ajanda ve formlar, fiziksel dosyalar

4. Saklama Ve İmha Sebepleri

4.1. Saklama Sebepleri

a) Kanunun 3. maddesinde kişisel verilerin depolanması ve muhafaza edilmesinin de kişisel veri işleme faaliyetine dahil olduğu, 4/1. maddesinde kişisel verilerin ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve 4/2-d maddesinde ise ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekliliği düzenlenmiş olup işlenmekte olan kişisel veriler öncelikle kanunun bu maddeleri gereğince saklanmaktadır.
b) İlgili mevzuatta muhafaza edilmesi öngörülen kişisel verilerin saklanması bakımından

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 4857 sayılı İş Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 213 sayılı Vergi Usul Kanunu,
- 6102 sayılı Türk Ticaret Kanunu
- 5684 sayılı Sigortacılık Kanunu
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun
- 2918 sayılı Karayolları Trafik Kanunu

başta olmak üzere bu kanunlara dayanılarak yürürlüğe alınmış bulunan tüm alt mevzuat ile sektörel mevzuat hükümleri dikkate alınmaktadır.

c) İşlendikleri amaç doğrultusunda muhafaza edilmesi öngörülen kişisel verilerin saklanması bakımından ise kanunun 5/2-f maddesinde yer alan "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" ile açık rıza dışındaki diğer veri işleme şartlarının bulunmadığı durumlar için kanunun 5/1 maddesinde yer alan "açık rıza" veri işleme şartına dayanılmaktadır.

4.2. İmha Sebepleri

Kişisel veriler;

a) Kanunun geçici 1/3 maddesinde düzenlenmiş bulunan bu kanunun yayımı tarihinden önce işlenmiş olan kişisel verilerin yayımı tarihinden itibaren iki yıl içinde bu kanun hükümlerine uygun hâle getirilmesi gerektiği, bu kanun hükümlerine aykırı olduğu tespit edilen kişisel verilerin derhâl silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekliliği,

b) Kanunun 7. maddesinde düzenlenmiş bulunan bu kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekliliği,

c) Kanunun 4. maddesinde düzenlenen
   - Hukuka ve dürüstlük kurallarına uygun olma,
   - Doğru ve gerektiğinde güncel olma,
   - Belirli, açık ve meşru amaçlar için işlenme,
   - İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma kriterlerinin karşılanmaması,

d) Kanunun 4/2-d maddesinde düzenlenen ilgili mevzuatta öngörülen kişisel veri işleme süresinin dolması,

e) İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

f) Kanunun 4/2-d maddesinde düzenlenen saklanmasını gerektiren amacın ortadan kalkması,

g) Kanunun 4/2-d maddesinde düzenlenen saklanmasını gerektiren amaç için gerekli olan azami sürenin geçmiş olması ile birlikte kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
h) Kanunun 5/1 maddesinde düzenlenen açık rıza şartına dayanarak veri işlemenin söz konusu olduğu durumlarda ilgili kişinin açık rızasını geri alması,
i) Kanunun 5/2. maddesinde düzenlenen veri işleme şartlarının artık mevcut olmaması,
j) Kanunun 11. maddesinde düzenlenmiş bulunan haklar kapsamında ilgili kişi tarafından silme veya yok etme talebinin iletilmesi ile birlikte bu talebin gereğini yerine getirebilmeyi engelleyen bir mevzuat hükmü bulunmaması ve talebin kabul edilmesi,
k) Kanunun 15. maddesinde düzenlenmiş bulunan kurul tarafından kişisel verilerin imhasına karar verilmesi,

durumlarında silinir, yok edilir veya anonim hale getirilir. İlaveten bu konuyu düzenleyen 5237 sayılı Türk Ceza Kanunun 138/1 maddesinde kanunların belirlediği sürelerin geçmiş olması durumunda verilerin sistem içinde yok edilmemesi bir suç tipi olarak tanımlanmıştır.

5. Teknik Ve İdari Tedbirler

İşlenmekte olan kişisel verileri güvenli bir şekilde muhafaza etmek, hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, imha süreçlerini hukuka uygun bir şekilde gerçekleştirmek için her türlü teknik ve idari tedbirleri alınmaktadır.

5.1. Teknik Tedbirler

a) Sızma (Penetrasyon) testleri ile şirketimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
b) Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
c) Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
d) Şirketimiz bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
e) 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.
f) Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
g) Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.

h) Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
i) Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirler alınmaktadır.
j) Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için buna uygun bir sistem, prosedür ve altyapı oluşturulmuştur.
k) Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
l) Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
m) Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
n) Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
o) Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
p) Şirketimiz internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
q) Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
r) 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.
s) Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanmaktadır.
t) Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
u) Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2. İdari Tedbirler

a) Veri işleme ilkeleri, veri işleme şartları, verilerin güvenli bir şekilde muhafazası, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi, olası veri ihlal durumlarında kimler tarafından hangi adımlar

atılacağı, özel nitelikli verilerin işlenmesi başta olmak üzere kişisel verilerin korunması mevzuatının tamamı hakkında belirli periyotlarla bilinçlendirme ve farkındalık eğitimleri yapılmaktadır.

b) Kişisel veri paylaşımı yapılan üçüncü kişilere, olabilecek aktarım ihtimallerinin tamamı için (veri sorumlusundan veri sorumlusuna, veri sorumlusundan veri işleyene, veri işleyenden veri sorumlusuna, veri işleyenden veri işleyene) veri aktarım sözleşmeleri imzalatılmaktadır
c) Çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
d) Kişisel veri işlemeye başlamadan önce ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
e) Kişisel veri işleme envanteri hazırlanmış ve VERBİS sistemine bildirimler gerçekleştirilmiştir.
f) Şirket içi periyodik ve rastgele denetimler yapılmaktadır.

6. Kişisel Verilerin İmhası

Kişisel verilerin hukuka uygun olarak imha edilmesi için aşağıda belirtilen teknik ve idari tedbirler uygulanmaktadır.

6.1. Kişisel Verilerin Silinmesi

Bu politikanın 2 numaralı tanımlar bölümünde de yer aldığı üzere silme; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olup farklı ortam tiplerine göre silme işlemi aşağıdaki şekillerde gerçekleştirilmektedir.

a) Sunucularda yer alan kişisel veriler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır
b) Elektronik ortamda yer alan kişisel veriler veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir
c) Fiziksel ortamda tutulan kişisel veriler evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
d) Taşınabilir medyada bulunan kişisel veriler sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel Verilerin Yok Edilmesi

Bu politikanın 2 numaralı tanımlar bölümünde de yer aldığı üzere yok etme; kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi olup farklı ortam tiplerine göre yok etme işlemi aşağıdaki şekillerde gerçekleştirilmektedir.

a) Fiziksel ortamda tutulan kişisel veriler kağıt öğütücü makinelerde geri döndürülemeyecek şekilde yok edilir, arşivde bulunan kişisel veriler ise yakılarak yok etme işlemi gerçekleştirilir.
b) Optik/manyetik medyada yer alan kişisel veriler yakılarak veya toz haline getirilerek fiziksel olarak yok etme işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Bu politikanın 2 numaralı tanımlar bölümünde de yer aldığı üzere anonim hale getirme; kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemi olup maskeleme, toplulaştırma ve veri üretme gibi yöntemlerle anonimleştirme işlemi gerçekleştirilmektedir.

7. Sorumluluk Ve Görev Dağılımı

Kişisel verilerin hukuka uygun olarak güvenli bir şekilde saklanması ve imha edilmesi süreçleri aşağıdaki birimler tarafından yerine getirilir.

a) Kişisel Verilerin Korunması Komite Başkan ve üyeleri:

Şirket nezdinde işlenen kişisel verilerin mevzuata uygun olarak işlenmesini temin etmek, yönetmek, kontrol etmek ve gerekli kararları almak için kişisel verilerin korunması komitesi oluşturulmuştur. Bu komitenin başkan ve üyeleri tarafından belirli periyotlarla değerlendirme toplantıları yapılarak KVK mevzuatına uyum noktasında güncel gelişmeler, veri koruma görevlisi yönetiminde alınan aksiyonlar ve sonraki adımlarda yerine getirilmesi planlanan yasal gereklilikler etraflıca değerlendirilir. Ayrıca üzerine karar alınmayı gerektirecek kritik önemdeki konular hakkında karar alarak uygulanmaya alınması sağlanır.

b) Veri Koruma Görevlisi:

Bu politikanın hazırlanması, güncellenmesi, geliştirilmesi, yürütülmesi ve ilgili ortamlarda yayınlanmasını temin eder. Kişisel verilerin korunması mevzuatına uyum için gerekli tüm adımları planlar, bu politikada belirtilen kişisel verilerin saklanması ve imha edilmesi işlemlerinin şirketin tüm departmanları tarafından yerine getirilmesini temin eder.

c) Bilgi Teknolojileri Yöneticisi:

Bu politika uyarınca kişisel verilerin saklanması ve imhası konusunda şirketin ilgili tüm departmanlarına ihtiyaç duyulan teknik çözümleri sunar. Politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

d) İnsan Kaynakları Yöneticisi:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

e) İşyeri Sağlık Birimi Yöneticisi (İşyeri Hekimi ve İSG Yöneticisi):

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

f) Mali İşler Yöneticisi:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

g) İdari İşler Yöneticisi:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

h) Pazarlama Yöneticisi:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

i) Hasar Departmanı Yöneticisi:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

j) Teknik Departmanlar Yöneticileri:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

k) Bölge Müdürlüğü Yöneticileri:

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

l) İstanbul Satış Yöneticisi

Bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

ve ilgili tüm departmanların yöneticileri de bu politikada belirtilen saklama ve imha gerekliliklerini mevzuata uygun şekilde yerine getirir.

8. Saklama Ve İmha Süreleri

NO	KİŞİSEL VERİ KATEGORİSİ	KİŞİSEL VERİ SAKLAMA SÜRESİ	İMHA SÜRESİ
1	Kimlik	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
2	İletişim	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
3	Lokasyon	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
4	Özlük	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
5	Hukuki İşlem	15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

6	Müşteri İşlem	Hizmet İlişkisinin Sonlanmasından İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
7	Fiziksel Mekan Güvenliği	Hizmet İlişkisinin Sonlanmasından İtibaren + 5 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
8	İşlem Güvenliği	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
9	Risk Yönetimi	Hizmet İlişkisinin Sonlanmasından İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
10	Finans	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
11	Mesleki Deneyim	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
10	Görsel ve İşitsel Kayıtlar	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
11	Sağlık Bilgileri	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
12	Diğer Bilgiler – İmza	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
13	Diğer Bilgiler- Araç Plakası	Hukuki İlişkinin (İş Akdinin) Sona Ermesinden İtibaren + 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

9. Periyodik İmha Süresi

Yönetmeliğin 11/2 maddesi gereğince kişisel verilerin imhası açısından şirketimiz periyodik imha süresi 6 ay olup haziran ve aralık aylarında periyodik imha işlemi gerçekleştirilmektedir.