

# KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

## 1. BÖLÜM: İMHA POLİTİKASININ NİTELİĞİ VE AMACI

### 1.1 Giriş

İşbu imha politikası **FLINT GROUP MATBAA MÜREKKEPLERİ SAN. VE TİC. A.Ş.** kısaca (“Flint Group”) olarak veri sorumlusu sıfatıyla elimizde bulduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin **Flint Group** tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve herhangi bir nedenle Flint Group nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

### 1.2. Tanımlar

Doğrudan tanımlayıcılar	Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,
Dolaylı tanımlayıcılar	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkarma imkanı veren, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,
İlgili kişi	Kişisel verisi işlenen gerçek kişiyi
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kanun	07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununu,
Yönetmelik	28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğini
Kurul	Kişisel Verileri Koruma Kurulunu
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 ortamı,
Kişisel Verilerin İşlenmesi ve Korunması Politikası	“ <a href="http://www.flintgrp.com">www.flintgrp.com</a> ” adresinden ulaşılabilecek, Flint Group elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı,
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

## 2. BÖLÜM: ORTAMLAR VE GÜVENLİK TEDBİRLERİ

### 2.1 Kişisel Verilerin Saklandığı Ortamlar

Flint Group nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Flint Group her halde veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri Kanun'a, Kişisel Verilerin İşlenmesi ve Korunması Politikası'na ve işbu Kişisel Veri Saklama ve İmha Politikası'na uygun olarak işlemek ve korumaktadır.

a.Matbu ortamlar	Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
b.Yerel dijital ortamlar	Flint Group bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır.
c.Bulut ortamlar	Flint Group bünyesinde yer almamakla birlikte, Flint Group kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

### 2.2 Ortamların Güvenliğinin Sağlanması

Flint Group, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düşüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

#### 2.2.1. Teknik Tedbirler

Flint Group, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.
- Flint Group bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.

### 2.2.2. İdari Tedbirler

Flint Group, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Flint Group çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.
- Şirket yerleşkelerinde güvenlik önlemleri alınmaktadır (örn. Bina ve odalara kontrollü giriş, veri depolama için kapalı dolaplar, sadece yetkili kişiler için erişim vb.)

### 2.2.3. Şirket İçi Denetim

Flint Group, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik derhal giderilir.

Üçüncü bir kişi tarafından kanuna aykırı olarak kişisel verilerin elde edilmesi halinde, Flint Group ilgili kişiye ve KVKK Kurulu'na en kısa sürede bilgi verecektir.

## 3. BÖLÜM: KİŞİSEL VERİLERİN İMHASI

### 3.1 Saklama ve İmha Nedenleri

#### 3.1.1. Saklama Nedenleri

Flint Group bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız (ilgili politikaya "<https://flintgrp.com/en/company/locations-contacts/emea/turkey/>") adresinden ulaşabilirsiniz) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

#### 3.1.2. İmha Nedenleri

Flint Group bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.

Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

1. Kanunlarda açıkça öngörülmesi.
2. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

5. İlgili kişinin kendisi tarafından alenileştirilmiş olması.
6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

### 3.2 İmha Yöntemleri

Flint Group, Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

Flint Group tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

#### 3.2.1 Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Bulandırma	Matbu ortamda bulunan kişisel veriler bulandırma yöntemi kullanılarak silinir. Bulandırma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünmez hale getirilmesi şeklinde yapılır.
Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Yazılımdan güvenli olarak silme	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

#### 3.2.2 Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel yok etme	Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel yok etme	Kişisel veri barındıran optik 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.

De-manyetize etme (degauss)	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
Üzerine yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
<b>Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
Yazılımdan güvenli olarak silme	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

### 3.2.3 Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır.  Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.
Bölgesel gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
Genelleştirme	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistikî veri haline getirilmesi işlemidir.
Alt ve üst sınır kodlama / Global kodlama	Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir.  Aynı kategori içinde kalan değerler birleştirilir.
Mikro birleştirme	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre

	dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
Veri karma ve bozma	Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

Flint Group, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır.

### 3.3. Saklama ve İmha Süresi

#### 3.3.1 Saklama Süresi

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ	İMHA SÜRESİ
<b>Çalışan</b>	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	Hizmet akdinin devamında ve hitamından itibaren de 10 (on) yıl müddetle muhafaza edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Çalışan</b>	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin devamında ve hitamından itibaren 10 (on) yıl müddetle muhafaza edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>İş Ortağı/Çözüm Ortağı/Danışman</b>	İş Ortağı/Çözüm Ortağı/Danışman ile Flint Group arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları,	İş Ortağı/Çözüm Ortağı/Danışmanın, Flint Group ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.

	İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	uyarınca 10 yıl süre ile saklanır.	
<b>Ziyaretçi</b>	Flint Group'a ait fiziki mekana girişte alınan Ziyaretçi'ye ait ad, soyad, T.C.K.N., araç plakası ile kamera kayıtları, telefon aramalarında alınan ses kayıtları	2 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>İnternet Sitesi Ziyaretçisi</b>	İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	2 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Çalışan Adayı</b>	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Stajyer(öğrenci)</b>	Stajyer'e ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10 (on) yıl müddetle muhafaza edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Müşteri</b>	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri	Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.

<b>Müşteri</b>	Kamera görüntüleri, araç plaka bilgisi	2 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Potansiyel Müşteri</b>	Potansiyel Müşteri ile Flint Group arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları	2 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.
<b>Flint Group'un İş birliği İçinde Kurum/Firmalar Olduğu</b>	Flint Group'un İşbirliği İçinde Olduğu Kurum/Firmalar ile Flint Group arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, Flint Group'un İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri	Flint Group'un İşbirliği İçinde Olduğu Kurum/Firmaların, Flint Group ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde.

\* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

### 3.3.2. İmha Süreleri

Flint Group, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanunun 13'ncü maddesine istinaden Flint Group'a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;



1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Flint Group talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Flint Group'un talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Flint Group, her halde yapılan işleme ilgili ilgili kişiye bilgi verir.
2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Flint Group tarafından Kanununun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

### **3.4 Periyodik İmha**

Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; Flint Group işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işleme siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri ilk kez 01.02.2021 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

### **3.5 İmha İşleminin Hukuka Uygunluğunun Denetimi**

Flint Group, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Flint Group, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

#### **3.5.1. Teknik Tedbirler**

- Flint Group, işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
- Flint Group, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- Flint Group, imha işlemi yapan kişilerin erişim kayıtlarını tutar.
- Flint Group, imha işlemi yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.
- Flint Group, imha işleminin Şirket dışından bir kişi tarafından yapılması halinde, bu alanda yetkin ve tecrübeli kişiler ile sözleşme imzalar.

#### **3.5.2. İdari Tedbirler**

- Flint Group, imha işlemi yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- Flint Group, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- Flint Group, teknik ya da hukuki gereklilikler nedeniyle imha işlemi üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.

- Flint Group, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklerle uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- Flint Group, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

#### 4. BÖLÜM: KİŞİSEL VERİ KOMİTESİ

Flint Group bünyesinde bir Kişisel Veri Komitesi kurar. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi bir yönetici, bir idari uzman ve bir teknik uzman olmak üzere üç kişiden oluşur. Kişisel Veri Komitesinde görevli Flint Group çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

Unvan	Görev Tanımı
<b>Kişisel Veri Komitesi Yöneticisi</b>	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
<b>KVK Uzmanı (Teknik ve İdari)</b>	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

#### 5. BÖLÜM: GÜNCELLEME VE UYUM

Flint Group, Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda Kişisel Verilerin İşlenmesi ve Korunması Politikasında ya da işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.

İşbu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.