

## DOPING BİLİŞİM TEKNOLOJİLERİ A.Ş.

### Kişisel Veri Saklama ve İmha Politikası

Doping Bilişim Teknolojileri A.Ş. ("Doping Bilişim") için ilişki içerisinde bulunduğu tüm gerçek kişilerin kişisel verilerinin korunması büyük önem arz etmektedir. Bu sebeple de yürürlükte bulunan mevzuata uyum gösterebilmek ve veri güvenliği ilkelerini uygulayabilmek adına azami gayret gösteren bir çalışma içerisindeyiz.

Bu kapsamda, 6698 sayılı Kanun ve ilgili mevzuat gereğince kişisel verilerin işlenmesi ve korunması için Doping Bilişim tarafından gereken idari ve teknik tedbirler alınmaktadır.

#### 1. AMAÇ

Kişisel Verileri Saklama ve İmha Politikası; Doping Bilişim Teknolojileri A.Ş. tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmış olup, kişisel verileriniz işbu politika kapsamında işlenmekte ve korunmaktadır.

Kişisel Verilerin saklanması ve imhasına ilişkin iş ve işlemler, Doping Bilişim tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

#### 2. KAPSAM

Bu politika; Çalışan, Ürün veya Hizmet Alan Kişi, Tedarikçi Yetkilisi, Tedarikçi Çalışanı, Potansiyel Ürün veya Hizmet Alıcısı, Ziyaretçi, Çalışan Adayı, Hissedar/Ortak, Veli/Vasi/Temsilci, Sınav Adayı, Diğer-Kullanıcı başta olmak üzere kişisel verileri Veri Sorumlusu tarafından işlenen gerçek kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verilerine ilişkindir.

##### 2.1 Kısaltmalar ve Tanımlar

<b>Açık Rıza</b>	İlgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanıdır.
<b>Alıcı Grubu</b>	Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.
<b>Anonim Hale Getirme</b>	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.
<b>Çalışan Adayı</b>	Veri sorumlusuna herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini incelenmesi amacıyla belirttiği kaynaklara iletmış olan gerçek kişilerdir.
<b>İlgili Kişi</b>	KVK Kanununda kişisel verisi işlenen gerçek kişiyi ifade etmek için "ilgili kişi" ifadesi kullanılmıştır.

<b>İmha</b>	Kişisel Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
<b>Kişisel Veri</b>	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir.
<b>Kişisel Veri İşleme Envanteri</b>	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanterdir.
<b>Kişisel Verilerin İşlenmesi</b>	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
<b>KVK Kanunu</b>	7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade etmektedir.
<b>Özel Nitelikte Kişisel Veriler</b>	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 verileridir. Özel nitelikli kişisel verilerin kıyas yoluyla genişletilmesi mümkün değildir.

<b>Potansiyel Müşteri</b>	Şirket'in ürün ve hizmetlerini kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişilerdir.
<b>Şirket Gerçek Kişi İş Ortağı</b>	Şirket'in her türlü iş ilişkisi içerisinde bulunduğu gerçek kişilerdir.
<b>Şirket Müşterisi</b>	Şirket ile herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirket'in sunmuş olduğu ürün ve hizmetleri kullanan veya kullanmış olan gerçek kişilerdir.
<b>Şirket Paydaşı</b>	Şirket'in Paydaşı gerçek kişilerdir.
<b>Şirket Yetkilisi</b>	Şirket'in yönetim kurulu üyesi ve diğer yetkili gerçek kişilerdir.
<b>Üçüncü Kişi</b>	Bu Politikada herhangi bir kişisel veri sahibi kategorisine girmeyen diğer gerçek kişilerdir.
<b>Üçüncü Kişi Şirket Yetkilisi, Çalışanı</b>	Şirket'in her türlü iş ilişkisi içerisinde bulunduğu gerçek ve tüzel kişilerin çalışanları ve yetkilileri dâhil olmak üzere, tüm gerçek kişilerdir.
<b>VERBİS</b>	Veri Sorumluları Sicil Bilgi Sistemi
<b>Veri İşleyen</b>	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi.
<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olanlardır.
<b>Ziyaretçi</b>	Şirket'in sahip olduğu veya şirketin yetkilendirdiği kişilere ait fiziksel yerleşkelere çeşitli amaçlarla giren veya internet sitelerini herhangi bir amaç ile ziyaret eden tüm gerçek kişilerdir.

### 3. SORUMLULUK VE GÖREV DAĞILIMI

Doping Bilişim Teknolojileri A.Ş.; tüm iş birimleri ve çalışanları işbu Politika ve Kişisel Verilerin Korunması ve İşlenmesi Yönetmeliği kapsamında belirtilmiş olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artması gibi sürekli denetimi ile kişisel verilerin hukuka uygun şekilde işlenmesini, tüm veri işleme ortamlarında veri güvenliğini sağlamaya dönük olarak teknik ve idari tedbirlerin uygulanmasına destek verir ve sorumlu birimlerle işbirliği içinde çalışır.

Doping Bilişim Teknolojileri A.Ş. bünyesinde oluşturduğu Kişisel Veri Komitesi; ilgili kişilerin verilerinin mevzuata, 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 insan kaynakları uzmanı, bir teknik uzman ve avukat olmak üzere dört kişiden oluşur. Kişisel Veri Komitesinde görevli çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

Unvan	Görev Tanımı
<b>Kişisel Verileri Koruma Komitesi</b>	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerden gelen talepleri karara bağlamak, kişisel verilerin korunması konusundaki gelişmeleri takip etmek; bu gelişmeler kapsamında yapılması gerekenler konusunda üst yönetime tavsiyelerde bulunmak ve Kurum ve Kurul ile olan ilişkileri yönetmek ile yükümlüdür.
<b>Kişisel Verileri Koruma Komitesi Yöneticisi</b>	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesinin raporlanmasından; Kişisel Veri Komitesi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

### 4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR

Doping Bilişim Teknolojileri A.Ş. tarafından ilişkide bulunulan gerçek kişilerin kişisel verileri KVK Kanunu'na uygun olarak saklanır ve imha edilir. Ayrıca, kişisel verilerin saklanması ve imhası sürecinde, bu verilerin 3. kişilerce hukuka aykırı olarak saklanmasını ve imhasını önlemek amacıyla her türlü teknik ve idari tedbirler alınmaktadır. Şirket olarak, kişisel verilerin saklanması ve imhası süreçlerinde özel hayatın gizliliğinin korunmasına önem verilmekte ve veri güvenliği en üst seviyede gözetilmektedir.

## Kayıt Ortamları

Kişisel veriler, Doping Bilişim tarafından aşağıda sunulan tabloda yer alan ortamlarda mevzuata uygun olarak tutulmakta ve güvenli bir şekilde saklanmaktadır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Yazılımlar, Güvenlik duvarı, Saldırı tespit ve engelleme sistemi, Antivirüs, Yazıcı, Tarayıcı, Fotokopi Makinesi, Bilgisayarlar, Kamera Kayıt Sistemleri, Optik Diskler ve Çıkarılabilir Bellekler, Mobil Cihazlar	Matbu Veri Kayıt Ortamları; Formlar ve Belgeler, Yazılı ve Görsel Diğer Ortamlar

## 5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

İş faaliyetleri sırasında çalışanlarımıza, çalışan adaylarımıza, ziyaretçilerimize, kullanıcılarımıza ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilere ait kişisel veriler özenli şekilde işbu protokolda ve Kanunda öngörölmüş usullerle toplamakta, işlemekte ve saklamakta ve imha etmektedir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

### 5.1 Saklamaya İlişkin Açıklamalar

Kanunun 3'üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4'üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörölen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirketimiz, kişisel verileri işlendikleri amaç için gerekli olan süre ve ilgili faaliyetin tabi olduğu yasal mevzuatta öngörölen minimum sürelerle uygun olarak muhafaza etmektedir. Bu kapsamda, Şirketimiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörölüp öngörölmediğini tespit etmekte, bir süre belirlenmişse mevcut duruma uygun en makul süreye uygun davranmaktadır. Kişisel veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

#### 5.1.1 Saklamayı Gerektiren Hukuki Sebepler

Doping Bilişim Teknolojileri A.Ş., faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörölen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,

- 5434 sayılı Emekli Saęlıęı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İřyeri Bina ve Eklentilerinde Alınacak Saęlık ve Gvenlik nlemlerine İliřkin Ynetmelik,
- Arřiv Hizmetleri Hakkında Ynetmelik
- Bu kanunlar uyarınca yrrlkte olan dięer ikincil dzenlemeler çerçevesinde ngrlen saklama sreleri kadar saklanmaktadır.

### 5.1.2 Saklamayı Gerektiren İřleme Amaçları

řirketimiz, faaliyetleri çerçevesinde işlemekte olduęu kiřisel verileri ařaęıdaki amaçlar doęrultusunda saklar.

1. Acil Durum Ynetimi Sreçlerinin Yrtlmesi
2. Bilgi Gvenlięi Sreçlerinin Yrtlmesi
3. Çalıřan Adayı / Stajyer / ęrenci Seçme ve Yerleřtirme Sreçlerinin Yrtlmesi
4. Çalıřan Adaylarının Bařvuru Sreçlerinin Yrtlmesi
5. Çalıřan Memnuniyeti ve Baęlılıęı Sreçlerinin Yrtlmesi
6. Çalıřanlar İin İř Akdi ve Mevzuattan Kaynaklı Ykmllklerin Yerine Getirilmesi
7. Çalıřanlar İin Yan Haklar ve Menfaatleri Sreçlerinin Yrtlmesi
8. Denetim / Etik Faaliyetlerinin Yrtlmesi
9. Eęitim Faaliyetlerinin Yrtlmesi
10. Eriřim Yetkilerinin Yrtlmesi
11. Faaliyetlerin Mevzuata Uygun Yrtlmesi
12. Finans ve Muhasebe İřlerinin Yrtlmesi
13. Firma / rn / Hizmetlere Baęlılık Sreçlerinin Yrtlmesi
14. Fiziksel Mekn Gvenlięinin Temini
15. Grevlendirme Sreçlerinin Yrtlmesi
16. Hukuk İřlerinin Takibi ve Yrtlmesi
17. İ Denetim/ Soruřturma / İstihbarat Faaliyetlerinin Yrtlmesi
18. İletifim Faaliyetlerinin Yrtlmesi

19. İnsan Kaynakları Süreçlerinin Planlanması
20. İş Faaliyetlerinin Yürütülmesi / Denetimi
21. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
22. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması ve Değerlendirilmesi
23. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
24. Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
25. Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
26. Mal / Hizmet Satış Süreçlerinin Yürütülmesi
27. Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
28. Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
29. Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
30. Organizasyon ve Etkinlik Yönetimi
31. Pazarlama Analiz Çalışmalarının Yürütülmesi
32. Performans Değerlendirme Süreçlerinin Yürütülmesi
33. Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
34. Risk Yönetimi Süreçlerinin Yürütülmesi
35. Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
36. Sosyal Sorumluluk ve Sivil Toplum Aktivitelerinin Yürütülmesi
37. Sözleşme Süreçlerinin Yürütülmesi
38. Sponsorluk Faaliyetlerinin Yürütülmesi
39. Stratejik Planlama Faaliyetlerinin Yürütülmesi
40. Talep / Şikayetlerin Takibi
41. Ücret Politikasının Yürütülmesi
42. Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
43. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
44. Yabancı Personel Çalışma ve Oturma İzni İşlemleri

45. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
46. Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
47. Yönetim Faaliyetlerinin Yürütülmesi
48. Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

## 5.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası sebebiyle gerekli olması hali,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- İlgili kişinin, Kanun'un 11. maddesindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun şirket tarafından kabul edilmesi,
- 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,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, durumlarında,

Şirketimiz tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir veya anonim hale getirilir.

## 6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK. 12. maddesindeki ilkeler çerçevesinde, Doping Bilişim tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır.

### 6.1 Teknik Tedbirler

Doping Bilişim tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Yeni teknolojik gelişmeler takip edilmekte ve özellikle siber güvenlik alanında sistemler üzerinde teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmekte ve yenilenmektedir.
- Virüs koruma sistemleri, veri açığı güvenlikleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.
- Sızma testleri ile şirketimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.



- Şirketimiz, bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal ve yazılımsal önlemler alınmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirketimiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Çalışanlar için yetki matrisi oluşturulmaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kişisel Verileri Koruma Komitesi kurulmuştur.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

#### **Teknik Tedbirler Listesi:**

1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
2. Anahtar yönetimi uygulanmaktadır.
3. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
4. Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
5. Çalışanlar için yetki matrisi oluşturulmuştur.
6. Erişim logları düzenli olarak tutulmaktadır.
7. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
8. Gerekğinde veri maskeleyme önlemi uygulanmaktadır.
9. Gizlilik taahhütnameleri yapılmaktadır.
10. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
11. Güncel anti-virüs sistemleri kullanılmaktadır.
12. Güvenlik duvarları kullanılmaktadır.
13. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
14. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
15. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
16. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
17. Kişisel veri güvenliğinin takibi yapılmaktadır.

18. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
19. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
20. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
19. Kişisel veriler mümkün olduğunca azaltılmaktadır.
20. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği sağlanmaktadır.
21. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
23. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
24. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
25. Mevcut riskler ve tehditler belirlenmiştir.
26. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
27. Saldırı tespit ve önleme sistemleri kullanılmaktadır.
28. Siber güvenlik önlemleri alınmış olup uygulaması sürekli takip edilmektedir.
29. Şifreleme yapılmaktadır.
30. Sızma testi uygulanmaktadır.
31. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

## 6.2. İdari Tedbirler

Şirketimiz tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- 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, 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.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- 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.

- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Şirket içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.

### 6.3 Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi

Doping Bilişim bünyesinde Kişisel Verileri Koruma Komitesi bulunmaktadır. Bu komite, veri sorumlusu olan Doping Bilişim adına, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri bizzat yapmakta ve ihtiyaç halinde yetkin kuruluşlardan destek almak suretiyle yaptırmaktadır. Bu denetim sonuçlarına göre, tespit edilen ihlaller, olumsuzluklar ve uygunsuzluklar Komite Yöneticisi 'ne bildirilmekte ve bu hususlar nezdinde gereken tedbirleri alınmaktadır.

## 7. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

KVK Kanunu'nun ilgili hükümleri ve Kurul tarafından çıkarılan "Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Hakkında Yönetmelik" uyarınca; ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde, Doping Bilişim 'in kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir. Doping Bilişim bu konuda yönetmelik hükümlerine göre bir politika oluşturmuş olup, bu politika uyarınca verinin niteliğine göre imha yapmaktadır. **7.1. Kişisel Verilerin Silinmesi**

<b>Kağıt Ortamında Bulunan Kişisel Verilerin Silinmesi</b>	
<b>Karartma</b>	Fiziki ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünmez hale getirilmesi şeklinde yapılır.
<b>Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri</b>	
<b>Yazılımdan güvenli olarak silme</b>	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

### 7.2. Kişisel Verilerin Yok Edilmesi:

<b>Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
<b>Fiziksel yok etme</b>	Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.
<b>Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri</b>	
<b>Fiziksel yok etme</b>	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.
<b>De-manyetize etme (degauss)</b>	Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
<b>Üzerine yazma</b>	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>	
<b>Yazılımdan güvenli olarak silme</b>	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

### **7.3. 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.

## **8. SAKLAMA VE İMHA SÜRELERİ**

Doping Bilişim tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Bilgi İşlem Departmanı tarafından yerine getirilir.

SÜREÇ/KAYNAK İŞLEM	SAKLAMA SÜRESİ	YASAL DAYANAK	İMHA SÜRESİ
Çağrı Merkezi Ses Kayıtları	3 Yıl	6563 Sayılı Kanun ve İlgili Mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Erişim Kısıtlamaları – Active Directory İşlemleri	İş ilişkisinin sona ermesinden itibaren 10 Yıl	4857 Sayılı İş Kanunu ve İlgili Mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlara Yönelik Kurumsal İletişim Faaliyetleri Uyarınca İşlenen Veriler (Örn: Katılımcı Listesi vb.)	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Sektörel teamüller geçerli. Buna İstinaden ancak açık rıza varlığı halinde işlenebilmektedir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Çalışanların Kişisel Verilerinin Yer Aldığı Ortamlara İlişkin Yaptığı Erişimlerin Log Kayıtları	En Az 2 Yıl Olmak Suretiyle İş Davalarına Konu Olabilmesi Sebebiyle 10 Yıl	5651 Sayılı Kanun Gereği, 4857 Sayılı İş Kanunu ve TİB (Telekomünikasyon İletişim Başkanlığı) Yönetmelikler	
Fatura/Gider Pusulası/Makbuz gibi Vergi Usul Kanunu Uyarınca Tutulması gereken Belgelerle İşlenen Kişisel Veriler	10 Yıl	213 Sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul İşlemleri Uyarınca İşlenen Veriler	10 Yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul Toplantı ve Yönetim Kurulu Toplantı İşlemleri	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

<b>İş Başvurusu/Staj Başvurusu/ Başvuru Kabul Edilmediği Takdirde Aday Başvurularına İlişkin Veriler (Örn: CV, Özgeçmiş, Cover Letter, Başvuru Formu vb.)</b>	1 Yıl	Sektörel teamüller geçerli. Buna İstinaden ancak açık rıza varlığı halinde işlenebilmektedir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İş Kanunu Kapsamında Saklanan Özlük Dosyasına İlişkin Veriler</b>	İş İlişkisinin sona ermesinden itibaren 10 Yıl	4857 Sayılı İş Kanunu ve İlgili Mevzuat / 6098 Sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İş Kanunu Kapsamında Saklanan Veriler (Örn. Kıdem tazminatı, ihbar tazminatı, kötüniyet tazminatı, eşit davranma ilkesine aykırılık tazminatına konu olabilecek bilgiler, bordro kayıtları, yıllık izin gün sayısı vb.)</b>	İş İlişkisinin sona ermesinden itibaren 10 Yıl	4857 Sayılı İş Kanunu ve İlgili Mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İş Kanunu Kapsamında Saklanan Verilerden Sendikal Tazminata Konu Olabilecek Veriler (Örn: Performans kayıtları, disiplin cezaları, fesih evrakları vb.)</b>	İş İlişkisinin sona ermesinden itibaren 10 Yıl	6098 Sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>İş Kanunu Uyarınca: Çalışan ile ilgili Mahkeme/icra bilgi taleplerinin cevaplanması</b>	İş İlişkisinin sona ermesinden itibaren 10 Yıl	4857 Sayılı İş Kanunu ve İlgili Mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

<b>İş Sağlığı ve Güvenliği Mevzuatı Kapsamında Toplanan Veriler (Örn: İşe giriş sağlık testleri, sağlık raporları, İSG Eğitimleri, İş Sağlığı ve Güvenliği faaliyetlerine ilişkin kayıtlar vb.)</b>	İş İlişkisinin sona ermesinden itibaren 15 Yıl	6331 Sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Kamera Kayıtları</b>	7 gün	Veri Sorumlusunun Meşru menfaati	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

<b>Tanıtım Faaliyetleri Kaynaklı Görüntü Kayıtları</b>	Sözleşme ilişkisinin Sona Ermesinden İtibaren 10 Yıl	6098 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Muhasebe ve Finansal İşlemlere İlişkin tüm Kayıtlar</b>	10 Yıl	6102 Sayılı Kanun, 213 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Müşterilere İlişkin Kişisel Veriler</b>	Hukuki İlişki Son Erdikten Sonra 10 Yıl	6098 Sayılı Kanun, 213 Sayılı Kanun, 6502 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Sendikal Faaliyetler Uyarınca İşlenen ve Sendika ile Paylaşılan Kişisel Veriler</b>	10 Yıl	6356 Sayılı Sendikalar ve Toplu İş Sözleşmesi	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>SGK Mevzuatı kapsamında tutulan veriler (Örn: İşe giriş bildirgeleri, pirim/hizmet belgeleri vb.)</b>	İş İlişkisinin Sona Ermesinden İtibaren 10 Yıl	5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve İlgili Mevzuat	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Sözleşmeden Kaynaklı İlişkilerde İşlenen Kişisel Veriler (Örn: Ad soyad, görüntü ve ses kayıtları, mezuniyet bilgileri, yorum ve görüşler, imza sirküleri vb.)</b>	Hukuki ilişki süresince ve sona ermesinden itibaren 10 yıl	6098 Sayılı Türk Borçlar Kanunu md.146 ile 6102 Sayılı Türk Ticaret Kanunu md.82	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Şirket Faaliyetlerinin Yürütülmesi Kapsamında İşlenen ve Şirket' in Fikri Mülkiyeti ya da Ticari Mülkiyeti Konusunu Oluşturan Çalışanlara Ait Kişisel Veriler (Örn: dijital içeriklerdeki görsel ve işitsel veriler)</b>	Esere Konu Telif Hakkı Koruma Süresi Boyunca (70 yıl)	5846 Sayılı Fikir ve Sanat Eserleri Kanunu m. 27 ve Sözleşmeden Doğan Açık Rıza	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Kullanıcı Koşulları Kaynaklı İlişkilerde İşlenen Kişisel Veriler (Örn: Ad soyad, görüntü ve ses kayıtları, mezuniyet bilgileri, yorum ve görüşler, hukuki onay log kayıtları vb.)</b>	Sözleşmeden Kaynaklı Sözleşmenin Sona Ermesine Müteakip 10 Yıl	6098 Sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

<b>Şirket Faaliyetleri Uyarınca, Saklanması Gereken Ticari Defterler, Ticari Defterlerde Yer Alan Kayıtlara Dayanarak Oluşturulan Belgeler, Finansal Tablolar vb. İşlenen Kişisel Veriler</b>	10 Yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Şirket Ortakları ve Yönetim Kurulu Üyelerine ait Bilgiler (Örn: Huzur hakkı ve Kar payı ödemeleri vb.)</b>	10 Yıl	6102 Sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Şirket Ortakları ve Yönetim Kurulu Üyelerine ait Bilgiler (Pay defterinde yer alan kişisel veriler)</b>	Pay Defterinin Saklanması Zorunluluğu Sebebiyle Süresiz	6102 Sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Tedarikçilere İlişkin Kişisel Veriler</b>	Hukuki ilişki sona erdikten sonra 10 Yıl	6102 Sayılı Kanun, 6098 Sayılı Kanun ve 213 Sayılı Kanun	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Tüketicinin Korunması Hakkında Kanun(6502 Sayılı)Gereğince Satış Sonrası Hizmet Verilmesinin Zorunlu Olması Sebebiyle İşlenen Kişisel Veriler (Örn: Ürün kurulum tarihi, müşteri iletişim bilgileri)</b>	15 Yıl	6502 Sayılı Tüketicinin Korunması Hakkında Kanun, 13.06.2014 Tarih ve 29029 Sayılı Resmi Gazetede Yayınlanan Satış Sonrası Hizmetler Yönetmeliği	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Vergisel Kayıtlara İlişkin Kişisel Veriler</b>	10 Yıl	213 Sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Ziyaretçilerin Kişisel Verileri</b>	2 Yıl	5651 Sayılı Kanun (Şirketin Wi-Fi Ağına Erişim Sağlayan Ziyaretçiler İçin)	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
<b>Arşiv Belgeleri</b>	Son işlem tarihi üzerinden yirmi yıl geçmiş veya on beş yıl geçtikten sonra	DEVLET ARŞİV HİZMETLERİ	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
	kesin sonuca bağlanmış bulunan belgeler	HAKKINDA YÖNETMELİK	



## 9. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI; BU HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ METODOLOJİSİ

### 9.1 Veri Sahibinin Hakları ve Bu Haklarını Kullanması

#### 9.1.1 Kişisel Veri Sahibinin Hakları

Kişisel veri sahipleri aşağıda yer alan haklara sahiptirler:

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- KVK Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

#### 9.1.2 Kişisel Veri Sahibinin Haklarını İleri Süremeyeceği Haller

Kişisel veri sahipleri, KVK Kanunu'nun 28. maddesi gereğince aşağıdaki haller KVK Kanunu kapsamı dışında tutulduğundan, kişisel veri sahiplerinin bu konularda 9.1.1.'de sayılan haklarını ileri süremezler:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

KVK Kanunu'nun 28/2 maddesi gereğince; aşağıda sıralanan hallerde kişisel veri sahipleri zararın giderilmesini talep etme hakkı hariç, 9.1.1.'de sayılan diğer haklarını ileri süremezler:

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

### 9.1.3 Kişisel Veri Sahibinin Haklarını Kullanması

Kişisel Veri Sahipleri bu bölümün 9.1.1. Başlığı altında sıralanan haklarına ilişkin taleplerini kimliklerini tespit edecek bilgi ve belgelerle ve aşağıda belirtilen yöntemlerle veya Kişisel Verileri Koruma Kurulu'nun belirlediği diğer yöntemlerle Başvuru Formu'nu doldurup imzalayarak Şirkete ücretsiz olarak iletebileceklerdir:

- <https://www.dopinghafiza.com/> adresinde bulunan formun doldurulduktan sonra ıslak imzalı bir nüshasının bizzat elden veya noter aracılığı ile Yıldız Teknopark, Yıldız Teknik Üniversitesi, Çifte Havuzlar Mahallesi, Eski Londra Asfaltı Caddesi, Kuluçka Merkezi B2 Blok No:151/1G Kapı No:205 ESENLER / İSTANBUL adresine iletilmesi
- <https://www.dopinghafiza.com/> adresinde bulunan formun doldurulup 5070 Sayılı Elektronik İmza Kanunu kapsamındaki "güvenli elektronik imza"nızla imzalandıktan sonra güvenli elektronik imzalı formun info@dopinghafiza.com adresine kayıtlı elektronik posta ile gönderilmesi

Kişisel veri sahipleri adına üçüncü kişilerin başvuru talebinde bulunabilmesi için veri sahibi tarafından başvuruda bulunacak kişi adına noter kanalıyla düzenlenmiş özel vekâletname bulunmalıdır.

### 9.1.4 Kişisel Veri Sahibinin KVK Kurulu'na Şikâyetle Bulunma Hakkı

Kişisel veri sahibi KVK Kanunu'nun 14. maddesi gereğince başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; Şirketin cevabını öğrendiği tarihten itibaren otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde KVK Kurulu'na şikâyetle bulunabilir.

## 9.2 Şirketin Başvurulara Cevap Vermesi

### 9.2.1. Şirketin Başvurulara Cevap Verme Usulü ve Süresi

Kişisel veri sahibinin, bu bölümün 9.1.3. başlıklı kısmında yer alan usule uygun olarak talebini Şirkete iletmesi durumunda Şirket talebin niteliğine göre en geç otuz gün içinde ilgili talebi ücretsiz olarak sonuçlandıracaktır. Ancak, KVK Kurulunca bir ücret öngörülmesi hâlinde, Şirket tarafından başvuru sahibinden KVK Kurulunca belirlenen tarifedeki ücret alınacaktır.

### 9.2.2. Şirketin Başvuruda Bulunan Kişisel Veri Sahibinden Talep Edebileceği Bilgiler

Şirket, başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir. Şirket, kişisel veri sahibinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

### 9.2.3. Şirketin Kişisel Veri Sahibinin Başvurusunu Reddetme Hakkı

Şirket aşağıda yer alan hallerde başvuruda bulunan kişinin başvurusunu, gerekçesini açıklayarak reddedebilir:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.
- Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması
- Orantısız çaba gerektiren taleplerde bulunmuş olması.
- Talep edilen bilginin kamuya açık bir bilgi olması.

hakkında şeffaflık ve hesap verilebilirliğin sağlanması hedeflenmiştir.

## **10. ŞİRKET KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI'NIN DİĞER POLİTİKALARLA OLAN İLİŞKİSİ**

Şirket, işbu Politika ile ortaya koymuş olduğu esasların ilişkili olduğu kişisel verilerin korunması ve işlenmesi konusunda iç kullanıma yönelik alt politikalar da oluşturabileceği gibi çalışanlar başta olmak üzere belli kişi gruplarına yönelik olarak ayrıca başka politikalar da oluşturmaktadır.

Şirket içi politikalarının esasları, ilgili olduğu ölçüde kamuoyuna açık politikalara yansıtılarak, ilgililerinin bu çerçevede bilgilenmesi ve Şirketin yürütmekte olduğu kişisel veri işleme faaliyetleri

## **11. PERİYODİK İMHA SÜRESİ**

Yönetmeliğin 11 inci maddesi gereğince Doping Bilişim, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, şirkette her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir. **12.**

## **POLİTİKA'NIN YAYINLANMASI**

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır.

## **13. POLİTİKA'NIN GÜNCELLENME PERİYODU**

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

## **14. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI**

Doping Bilişim tarafından düzenlenen bu Politika yayınlandığı tarihte yürürlüğe konulmuştur. Bu Politika, Şirketimizin, internet sitesinde (<https://www.dopinghafiza.com/>) yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.