

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. Giriş

1.1. Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası (“**Politika**”), 6698 Sayılı Kişisel Verilerin Korunması Kanunu (“**KVKK**” ya da “**Kanun**”) ve Kanun’un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“**Yönetmelik**”) uyarınca yükümlülüklerimizi yerine getirmek, kişisel verilere ilişkin mevzuat çerçevesinde kişisel veri işleme faaliyeti ve kişisel verilerin korunmasına yönelik benimsenen sistemler konusunda açıklamalarda bulunmak ve ilgili kişileri kişisel verilerinin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla **HeraBiyo Biyoteknoloji Araştırma ve Danışmanlık Limited Şirketi** (“**HeraBiyo**” veya “**Şirket**”) tarafından hazırlanmıştır.

1.2. Kapsam

- Bu Politika; gerçek kişi olmak kaydıyla şirket müşterilerinin, tüzel kişi müşterilerinde tüzel kişiliği temsile yetkili gerçek kişilerinin, potansiyel müşterilerinin, bunların çalışanlarının, çalışan, çalışan adayları, ürün/hizmet alan kişi yetkilisi/çalışanları, tedarikçi yetkilisi/çalışanları, fiziki ve sanal ziyaretçiler ve diğer üçüncü kişilere ilişkin kişisel verilerin saklanması ve imhasını kapsamakta olup Şirketin sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ile kişisel verilerin saklanmasına ve imhasına yönelik faaliyetlerde bu Politika uygulanır.
- Yukarıda belirtilen kategorilerde yer alan ilgili kişilere ilişkin işbu Politika’nın uygulama kapsamı Politika’nın tamamı olabileceği gibi (örn. Ziyaretçimiz de olan Aktif müşterilerimiz gibi); yalnızca bir kısım hükümleri de (örn. Yalnızca Ziyaretçilerimiz gibi) olabilecektir.
- İşbu Politikada kişisel verilerin işlenmesi, saklanması ve aktarılması gibi sair hususlarda hüküm bulunmayan hallerde bu hususlardaki detaylı bilgiye www.herabiyo.bio adresinde yer alan **HeraBiyo** Kişisel Veri Korunması ve İşlenmesi Politikası’ndan erişilebilmektedir.
- KVKK ve ilgili diğer mevzuat ile Politika arasında çelişki bulunması halinde, yürürlükte bulunan mevzuat uygulama alanı bulacaktır.

1.3. Tanımlar

Tanım	Açıklama
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Çalışan	Şirket çalışanı.

İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
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.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun ya da KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu.
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.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Veri İşleme Envanteri	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 envanter.
Kişisel Verilerin Korunması ve İşlenmesi Politikası	www.herabiyo.bio adresinde yer HeraBiyo Kişisel Verilerin Korunması ve İşlenmesi Politikası.
İlgili Kişi Başvuru Formu	Şirket bünyesinde kişisel verileri işlenen ilgili kişinin Kanun'un 11. maddesinde açıklanan haklarına ilişkin başvurularını kullanırken yararlanacakları başvuru formu.

Kişisel Verilerin İşlenmesi	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.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kurul	Kişisel Verileri Koruma Kurulu.
Kurum	Kişisel Verileri Koruma Kurumu.
Özel Nitelikli Kişisel Veri	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 verileri.
Periyodik İmha	Kanun’da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re’sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Kişisel Veri Saklama ve İmha Politikası.

Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Veri Sorumluları Sicili (VERBİS)	Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından tutulan veri sorumluları sicili.
Yönetmelik	28 Ekim 2017 tarihli Resmî Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

İşbu Politika’da kullanılan tanımlar aşağıda yer almaktadır:

2. İlkeler

Şirket tarafından kişisel verilerin işlenmesi, saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilmektedir:

- Şirketimizce mevcut ya da edinilen kişisel veriler KVKK madde 4 uyarınca; (i) hukuka ve dürüstlük kurallarına uygun, (ii) doğru ve gerektiğinde güncel olacak şekilde, (iii) belirli, açık ve meşru amaçlar için işlenmekte, (iv) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak kullanılmakta ve (v) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan ve Şirketçe işbu Politikada belirlenen süre kadar muhafaza edilmektedir.
- Şirketimiz, ilgili kişinin açık rızasıyla veya KVKK’nın 5. ve 6. maddelerinde öngörülen hallerde ilgili kişinin açık rızası olmaksızın kişisel verileri ve **Özel Nitelikli Kişisel Verileri (Genetik ve Sağlık Verileri dahil)** işlemektedir. İlgili kişiler, kişisel veri işleme süreçlerine ilişkin olarak, Şirketimiz tarafından KVKK’nın 10. maddesine uygun olarak aydınlatılmakta ve ilgili kişinin bilgi talep etmeleri durumunda gerekli bilgilendirme yapılmaktadır.
- Şirketimiz, meşru ve hukuka uygun bir zeminde olan kişisel veri işleme amacını açık ve kesin bir biçimde belirlemektedir. Bu doğrultuda, kişisel veriler sunularak ya da sunulması planlanan **genetik analiz ve danışmanlık hizmetleri** kapsamında, yasal yükümlülükleri ile sınırlı olacak şekilde işlenmektedir. Kişisel verilerin ne amaçla işlendiği de kişisel veri işleme faaliyeti başlamaksızın ortaya konulur.
- **Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun’un 12. maddesi kapsamında alınması gereken ve işbu Politikanın 5. maddesinde belirtilen teknik ve idari tedbirlere (Özellikle biyoinformatik güvenliği),** ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.

- Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.
- Fiili imkânsızlık sebebiyle rızanın açıklanamayacağı durumda olan ya da rızaya geçerlilik tanınamayacak olan şahsın kendisine veya başka bir şahsın hayatını ya da beden bütünlüğünün tanınmadığı durumda olan kişinin kendisinin veya başka bir kişinin hayat ve beden bütünlüğünü korumak amacıyla kişisel verilerinin işlenmesinin gerekli olduğu durumlarda, veri sahibinin kişisel verilerini işlemek söz konusu olabilecektir.
- **HeraBiyo**, hukuki yükümlülüklerinin yerine getirilmesi amacıyla veri sahibinin kişisel verilerini işleyebilecektir. (Örneğin Sağlık Bakanlığı gibi kamu kurumlarının suallerine cevaben, belge gönderimi)
- Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilmektedir. Ancak, İlgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.
- Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Şirket tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından Şirket'e başvurulması halinde;
 - İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir,
 - Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.

3. Kayıt Ortamları

İlgili kişilere ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde aşağıdaki tabloda (**Tablo 1**) yer alan ortamlarda güvenli bir şekilde saklanmaktadır:

Tablo 1: Kişisel Veri Kayıt Ortamları Tablosu

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Verilerin bilgisayar, telefon gibi sair teknolojik cihazlar içerisinde tutulduğu ortamlardır:	Verilerin kâğıt ya da mikrofilm üzerine basılarak tutulduğu ortamlardır:
- Sunucular (Etki alanı, yedekleme, eposta, veri tabanı, web, dosya paylaşım vb.);	- Kâğıt;
- Biyoinformatik Analiz Sunucuları ve Bulut Depolama Alanları;	- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri, klinik kayıt formları);

- Yazılımlar;	- Yazılı, basılı, görsel ortamlar.
- Bilgi güvenliği cihazları;	
- Kişisel bilgisayarlar (Masaüstü, dizüstü);	
- Mobil Cihazlar (telefon, tablet vs.);	
- Optik diskler ve çıkartılabilir bellekler (CD, DVD, USB, Harici disk vs.).	

4. Saklama ve İmhayı Gerektiren Sebepler

Şirket tarafından, ilgili kişilere ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir. Bu kapsamda, saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir:

4.1. Saklamaya İlişkin Açıklamalar

İlgili kişiye ait kişisel veriler, Şirket tarafından Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları kapsamında özellikle; (i) ticari faaliyetlerin sürdürülebilmesi, (ii) hukuki yükümlülüklerin yerine getirilebilmesi ile (iii) müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan elektronik veya elektronik olmayan ortamlarda güvenli bir biçimde Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aşağıdaki gibidir:

- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi nedeniyle saklanması.
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması. **(Örn. Müşteriye analiz raporu sunulması amacıyla genetik verinin saklanması.)**
- Kişisel verilerin Şirket'in uymakla yükümlü olduğu herhangi bir hukuki yükümlülüğünü yerine getirmesine bağlı olarak saklanması.
- Kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması nedeniyle saklanması.
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunmasına bağlı olarak saklanması.
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanması zorunlu olması.
- İlgili kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından İlgili kişilerin açık rızasının bulunması nedeniyle saklanması.

4.2. İmhaya İlişkin Açıklamalar

Kanun ve ilgili diğer kanun hükümlerine uygun olarak saklanıyor olmasına rağmen, saklanmasını gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

Bu kapsamda, Kanun ve Yönetmelik uyarınca, aşağıda sayılan hallerde ilgili kişilere ait kişisel veriler, Şirket tarafından re'sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası.
- 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 rızasını geri alması.
- İlgili kişinin, Kanun'un 11. Maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu 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 şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması.
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

Şirketimiz, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini ve kişisel verilere hukuka aykırı erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktadır. Bu kapsamda, Şirket tarafından alınmış olan idari ve teknik tedbirler aşağıda sayılmıştır:

5.1. İdari Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar için veri güvenliği konusunda belli aralıklarla **eğitim ve farkındalık çalışmaları** yapılmaktadır. **(Özellikle biyoteknoloji ve genetik veri güvenliği etiği vurgulanarak.)**
- İlgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- 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 **anonimleştirme ve takma ad verme teknikleri** ile mümkün olduğunca azaltılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- **Özel nitelikli kişisel veri (Genetik Veriler) güvenliğine yönelik protokol ve prosedürler** belirlenmiş ve uygulanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

5.2. Teknik Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan teknik tedbirler aşağıda sıralanmaktadır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır. **(Genetik veri transferi için güvenli tüneller tercih edilmektedir.)**
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

6. SAKLAMA VE İMHA SÜRELERİ

Şirketimiz öncelikle, kişisel verilerin saklanması için ilgili mevzuatta bir süre öngörülüp öngörülmediğini tespit eder. İlgili mevzuatta bir süre öngörülümüşse bu süreye riayet eder; bir sürenin öngörülmemiş olması hâlinde kişisel verileri işlendikleri amaç için gerekli olan süre kadar muhafaza eder. Kişisel verilerin işlenme amacı sona ermiş ve ilgili mevzuat ve/veya Şirketimizin belirlediği saklama sürelerinin sonuna gelinmişse yalnızca olası hukuki uyumsuzluklarda delil teşkil etmesi, kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla kanunlarda öngörülen zamanaşımı süreleri boyunca saklanabilecektir. İleride kullanılabilme ihtimaline dayanılarak Şirketimiz tarafından kişisel veriler saklanmamaktadır.

Şirket tarafından tespit edilen süreç bazında saklama ve imha süreleri aşağıda listelenmektedir. Ayrıca; süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde yer almaktadır.

Süreç Bazında Saklama ve İmha Süreçleri:

- **Müşterilere/İlgili Kişilere İlişkin Kişisel Veriler (Genetik ve Sağlık Verileri dahil):**

- **Saklama Süresi:** Sözleşmenin bitiminden itibaren 10 yıl
- **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **Tedarikçilere veya Tüzel Kişi Tedarikçi Yetkilisi/Çalışanlarına İlişkin Kişisel Veriler:**
 - **Saklama Süresi:** Sözleşmenin bitiminden itibaren 10 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **Sözleşme İşlemleri Dolayısıyla Elde Edilen Kişisel Veriler:**
 - **Saklama Süresi:** Sözleşmenin bitiminden itibaren 10 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **Muhasebe ve Finansal İşlemlere İlişkin Tüm Kişisel Veriler:**
 - **Saklama Süresi:** Alındığı yılı takip eden yıldan itibaren 5 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **İş Akdinin İfası, AGİ Ödemeleri, Yan Hak ve İmkanların Temini ile SGK Nezdinde Yürütülecek Süreçler Gibi Sair Süreçler İçerisinde Şirket Çalışanları ve Stajyerlerinden Alınan Tüm Kişisel Veriler (İş Sağlığı ve Güvenliği dolayısıyla alınan veriler hariç):**
 - **Saklama Süresi:** Sözleşmenin bitiminden itibaren 10 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **Güvenlik Kamera Görüntüleri:**
 - **Saklama Süresi:** Kayıt Tarihinden İtibaren 30 Gün
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **IP Adreslerine İlişkin Kişisel Veriler:**
 - **Saklama Süresi:** Alındığı Tarihten İtibaren 6 ay
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **İş Ortağı/Çözüm Ortağı/Danışmanlara İlişkin Kişisel Veriler:**
 - **Saklama Süresi:** İş İlişkisinin bitiminden itibaren 10 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.
- **Potansiyel Müşteri ve Tedarikçilerden İş Geliştirme İçin Alınan Kişisel Veriler:**
 - **Saklama Süresi:** Alındığı tarihten itibaren 1 yıl
 - **İmha Süresi:** Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde.

7. PERİYODİK İMHA VE KİŞİSEL VERİ İMHA BAŞVURUSU

7.1. Periyodik İmha

- Şirket, Kanun, ilgili mevzuat, **HeraBiyo** Kişisel Verilerin Korunması ve İşlenmesi 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.
- **Yönetmeliğin 11. maddesi gereğince Şirket, periyodik imha süresini 1 yıl olarak belirlemiştir. Buna göre, Şirket tarafından yılda bir kez olmak üzere Aralık aylarında periyodik imha işlemi gerçekleştirilir.**

7.2. Kişisel Veri İmha Başvurusu

İlgili kişi, Kanunun 13. maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin imhasını talep ettiğinde:

1. **Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa;** Şirket 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. Şirket'in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.

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

8. KİŞİSEL VERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir. Bu kapsamda, 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. Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

8.1. Kişisel Verilerin Silinmesi Yöntemleri

- **Yazılımdan Güvenli Olarak Silme (Dijital Ortamlar):**
 - Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.
 - Yazılım sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.
 - Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır:
 - Başka herhangi bir kurum, kuruluş veya şahıs kişinin erişimine kapalı olması.
 - Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.
- **Kâğıt Ortamında Bulunan Kişisel Verilerin Karartılması (Fiziksel Ortamlar):**
 - Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

8.2. Kişisel Verilerin Yok Edilmesi Yöntemleri

- **Fiziksel Yok Etme (Kağıt ve Optik/Manyetik Medya):**
 - Elektronik olmayan ortamda tutulan belgeler, evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.

- Elektronik ortamda 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 (Overwrite):**
 - 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.

8.3. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

Kişisel veriler, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi amacıyla aşağıda belirtilen tekniklerle anonim hale getirilir:

- **Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri:**
 - Bu yöntemler, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirme yöntemleridir.
 - **Değişken Çıkartma:** Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden “yüksek dereceli betimleyici” olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir. (Örn. İsim, soy isim, doğum tarihi gibi.)
 - **Kayıtları Çıkartma:** Veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.
 - **Bölgesel Gizleme:** Tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır. (Örn. Nadir rastlanan yaş/cinsiyet/hastalık kombinasyonu yerine 'Bilinmiyor' yazılması.)
 - **Alt ve Üst Sınır Kodlama:** Önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir. (Örn. '5 yıl', '7 yıl' kıdem yerine '5-10 yıl arası' kategorisinin kullanılması.)
 - **Genelleştirme/Veri Toplulaştırma:** Birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. (Örn. Çalışanların yaşlarının tek tek yerine, yaş aralıklarının veya ortalamasının verilmesi.)
 - **Global Kodlama/Veri Türetme:** Kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. (Örn. Açık adres yerine ikamet edilen bölgenin belirtilmesi.)
- **Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri:**

- Bu yöntemlerde kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratılmaktadır. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.
 - **Gürültü Ekleme:** Özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir.
 - **Mikro Birleştirme:** Tüm veriler ilk olarak anlamlı bir sıraya dizilerek gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır.
 - **Veri Değiş Tokuşu:** Saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Kategorize edilebilen veriler için kullanılan bu yöntemde amaç ilgili kişiye ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.