

**sHR.**

strategic  
human resources

**SHR İNSAN KAYNAKLARI YÖNETİM  
DANIŞMANLIĞI VE EĞİTİM HİZMETLERİ EBRU MERİÇ AKGÜL**

**KİŞİSEL VERİ  
SAKLAMA ve İMHA POLİTİKASI**

## 1. AMACI

SHR İnsan Kaynakları Yönetim Danışmanlığı ve Eğitim Hizmetleri Ebru Meriç Akgül şahıs şirketi (bundan sonra "sHR" olarak anılacaktır) bu Kişisel Veri Saklama ve İmha Politikası ("**Saklama ve İmha Politikası**") ile kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanununa ("**Kanun**") uygun olarak teknik ve idari korunması, kişisel verilerin işleme şartlarının ortadan kalkması halinde, 28/10/2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") hükümlerinin uygulamasını düzenlemek amacıyla çıkarılmaktadır.

## 2. KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI

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

### **Elektronik ortamlar:**

- E-Posta Kutusu
- Microsoft Office Programları
- Bulut teknolojileri

### **Fiziksel ortamlar:**

- Birim Dolapları
- Klasörler
- Arşiv

## 3. SAKLAMAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, sHR tarafından özellikle:

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

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

### **Saklamayı gerektiren sebepler:**

- a. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- b. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması,

- c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla, sHR'nin meşru menfaatinin olması,
- d. Kişisel verilerin sHR'nin herhangi bir hukuki yükümlülüğünü yerine getirmesi,
- e. Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

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

- a. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- b. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- c. Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
- d. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- e. İlgili kişinin, Kanun'un 11. Maddesinin 2 (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- f. Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- g. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

#### **4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN TEDBİRLER**

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

##### **4.1 Teknik Tedbirler**

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır,
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki

- güvenlik önlemleri alınmaktadır,
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır,
  - Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır,
  - Gizlilik taahhütnameleri yapılmaktadır,
  - Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır,
  - Güncel anti-virüs sistemleri kullanılmaktadır,
  - Güvenlik duvarları kullanılmaktadır,
  - İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir,
  - Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir,
  - Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır,
  - Kişisel veri güvenliğinin takibi yapılmaktadır,
  - Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır,
  - Kişisel veri içeren ortamların güvenliği sağlanmaktadır,
  - Kişisel veriler mümkün olduğunca azaltılmaktadır,
  - Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır,
  - Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır,
  - Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

#### **4.2 İdari Tedbirler**

- Çalışanlar, kişisel verilere hukuka aykırı erişimi engellemek için alınacak teknik tedbirler konusunda eğitilmektedir.
- İş birimi bazında kişisel veri işlenmesi hukuksal uyum gerekliliklerine uygun olarak sHR içinde kişisel verilere erişim ve yetkilendirme süreçleri tasarlanmakta ve uygulanmaktadır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- sHR personeli ile arasındaki ilişkiyi düzenleyen ve kişisel veri içeren her türlü belgeye kişisel verilerin hukuka uygun olarak işlenmesi için Kanun ile öngörülen yükümlülüklerle uygun hareket edilmesi gerektiği, kişisel verilerin ifşa edilmemesi gerektiği, kişisel verilerin hukuka aykırı olarak kullanılmaması gerektiği ve kişisel verilere ilişkin gizlilik yükümlülüğünün sHR ile olan iş akdinin sona ermesinden sonra dahi devam ettiği yönünde kayıtlar eklemiştir.
- Çalışanlar, öğrendikleri kişisel verileri kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonrada devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır.
- sHR tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi

kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.

- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- Gerekli hallerde kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında eğitimleri verir.

## **5. KİŞİSEL VERİLERİN İMHA EDİLMESİNE İLİŞKİN ALINAN TEDBİRLER**

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

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

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

#### **5.1.1 Kişisel Verilerin Silinmesi**

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

- ✓ Kağıt ortamında bulunan kişisel veriler karartma yöntemi ile çizilerek, boyanarak, kesilerek veya silinerek işlem uygulanacaktır.
- ✓ Merkezi dosyada yer alan ofis dosyaları için kullanıcıların erişim hakları ortadan kaldırılacaktır.
- ✓ Veri tabanlarında bulunan kişisel bilgilerin bulunduğu satırlar yahut sütunlar 'Delete' komutu ile silinecektir.

Gerekli olduğu zaman bir uzman tarafından yardım alınarak güvenli olarak silinecektir.

#### **5.1.2 Kişisel Verilerin Yok Edilmesi**

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

Fiziksel Yok Etme

Kağıt İmha Makinesi ile Yok Etme

### 5.1.3 Kişisel Verileri Anonim Hale Getirilmesi

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

**Maskleme (Masking):** Veri maskleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinde çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.

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

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

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

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

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

SHR kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin re'sen karar alabilecek ve seçmiş olduğu kategoriye göre kullanacağı yöntemi de serbestçe belirleyebilecektir. Ayrıca Yönetmelik'in 13. maddesi kapsamında ilgili kişinin başvuru esnasında kendisine ait kişisel verinin silinmesi, yok edilmesi yahut anonim hale getirilmesi kategorilerinden birini seçmesi halinde de ilgili kategoride kullanılacak

yöntemler konusunda sHR serbesti içinde olacaktır.

## **6. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ**

sHR, kişisel verileri işlendikleri amaç için kanunda ve mezuatta öngörülen süreler boyunca saklar. Talep halinde kişisel verisi işlenen kişiler bu süreler hakkında detaylıca bilgilendirilir. Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bu süreler; sHR'nin veri kategorileri ve veri sahibi kişi grupları değerlendirilerek; bu değerlendirme sonucu elde edilen verilerin kanunlarda yer alan yükümlülüklerin yerine getirilmesini sağlayacak ve azami Türk Borçlar Kanunu'nda yer alan zamanaşımı süresi (10 yıl) gözetilerek belirlenmiştir.

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

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

## **7. PERİYODİK İMHA SÜRELERİ**

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

## **8. PERSONEL**

Kanun kapsamında sHR veri sorumlusu sıfatıyla, Yönetmelik'in 11. maddesinin 1. fıkrasına dayanarak, Kanunun veri saklama ve imha süreci uygulanması bakımından yükümlülükleri yerine getirilecek personelin unvanları, birimleri ve görev tanımları Saklama ve İmha Politikasında yer alan tablo ile belirlenmiştir.

Sınırları belirlenmiş bu kişiler Türk Ticaret Kanunu, Borçlar Kanunu ve Türk Ceza Kanunu kapsamında kendi yetki sınırları içinde gerçekleşen işlem ve eylemlerden sorumludur. Özellikle Kollukta, Savcılıklarda, kamu kurumlarında ve mahkemelerde sHR'yi temsil etme ile ifade vermeye yetkili olarak Ebru MERİÇ AKGÜL Kişisel Verileri Koruma Komitesi Başkanı seçilmiştir. Her bir departman sorumlusu, departmanlardaki ilgili kullanıcıların Kanun ve Yönetmelik çerçevesinde hazırlanan Saklama ve İmha Politikası ve Kişisel Veri Politikası'na uygun davranıp davranmadığını denetlemekle yükümlü olacaktır.

## **9. REVİZYON VE YÜRÜRLÜKTEN KALDIRMA**

Saklama ve İmha Politikası'nın deęiřtirilmesi, yürürlükten kaldırılması halinde yeni düzenleme sHR internet sitesinden ilan edilecektir.

## **10. YÜRÜRLÜK**

Bu Saklama ve İmha Politikası yayınlandığı 23.03.2022 tarihinde yürürlüğe girer.