

- Personel işe yeterlilik ve özlük haklarının tespitinin sağlanması amacıyla; 4857 sayılı İş Kanunu'nun "Çağrı üzerine çalışma ve uzaktan çalışma" başlıklı 14'üncü maddesinin altıncı fıkrasında belirtilen hukuki yükümlülüğün yerine getirilmesi,
- Personel özlük haklarının tespitinin sağlanması amacıyla; 4857 sayılı İş Kanunu'nun "İşçinin haklı nedenle fesih hakkı" başlıklı 24'üncü maddesinin birinci fıkrasında belirtilen hukuki yükümlülüğün yerine getirilmesi,
- Personel özlük haklarının tespitinin sağlanması amacıyla; 4857 sayılı İş Kanunu'nun "İşverenin haklı nedenle fesih hakkı" başlıklı 25'inci maddesinin birinci fıkrasında belirtilen hukuki yükümlülüğün yerine getirilmesi,
- Personel yan hak ve özlük haklarının tespitinin sağlanması amacıyla; 4857 sayılı İş Kanunu'nun "Fazla çalışma ücreti" başlıklı 41'inci maddesinde belirtilen hukuki yükümlülüğün yerine getirilmesi,
- Personel yan hak ve özlük haklarının tespitinin sağlanması amacıyla; 4857 sayılı İş Kanunu'nun "Analık halinde çalışma ve süt izni" başlıklı 74'üncü maddesinin birinci ve ikinci fıkrasında belirtilen hukuki yükümlülüğün yerine getirilmesi,
- Acil Durum Yönetimi Süreçlerinin Yürütülmesi,
- Faaliyetlerin Mevzuata Uygun Yürütülmesi,
- Hukuk İşlerinin Takibi ve Yürütülmesi,
- İnsan Kaynakları Süreçlerinin Planlanması,
- İş Faaliyetlerinin Yürütülmesi ve Denetimi,
- İzin Faaliyetlerinin Yürütülmesi,
- Personel Adaylarının Başvuru Süreçlerinin Yürütülmesi,
- Personel Görevlendirme Süreçlerinin Yürütülmesi,
- Personeller İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi,
- Personeller İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi,
- Saklama ve Arşiv Faaliyetlerinin Yürütülmesi,
- Sözleşme Süreçlerinin Yürütülmesi,
- Yetkili Kişi Kurum ve Kuruluşlara Bilgi Verilmesi,

Sağlık verileri kategorisinde belirlenen işleme amaçlarıdır.

4.2. KİŞİSEL VERİLERİN İMHASINI GEREKTİREN SEBEPLER

İlgili kişinin talebi ile veya Veri Sorumlusu tarafından re'sen aşağıdaki sebeplerin varlığının son bulması halinde söz konusu veriler silinir, yok edilir veya anonim hale getirilir. Buna göre kişisel veriler;

- İlgili kişinin, KVKK'nun 11'inci maddesindeki haklarını kullanmak suretiyle verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesine ilişkin talebinin Veri Sorumlusu tarafından kabulü,
- Veri Sorumlusu'nun, ilgili kişinin KVKK'nun 11'inci maddesindeki haklarını kullanarak başvurmasına karşın cevap vermemesi, başvuruyu reddetmesi ya da cevabın yetersiz olması sebepleriyle ilgili kişinin Kurul' a şikayette bulunması ve Kurul tarafından uygun bulunması,
- İlgili kişinin açık rızası ile işlenmiş kişisel verisi hakkındaki açık rızasını geri alması,

- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olmasına karşın, saklamayı haklı kılacak bir şartın mevcut olmaması,
- Kişisel verilerin işlenmesine veya saklanması öngören ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

Hallerinden birinin gerçekleşmesi ile işlenmeyi veya saklanmayı gerektiren amacın ortadan kalkması şeklinde yorumlanarak; silini, yok edilir veya anonim hale getirilir.

5. VERİ SORUMLUSUNUN UYGULADIĞI TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi amacıyla; KVKK'nun "*Veri güvenliğine ilişkin hükümler*" başlıklı 12'nci maddesi ile KVKK'nun "*Özel nitelikli kişisel verilerin işleme şartları*" başlıklı 6'ncı maddesinin dördüncü fıkrasında yer alan "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*" hüküm gereğince; veri sorumlusu sıfatı taşıyan Veri Sorumlusu'nun işlediği kişisel verilerin hukuka uygun olarak alınmış olduğu idari ve teknik tedbirler aşağıdaki gibidir.

5.1. TEKNİK TEDBİRLER

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Personeller için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Personeller için yetki matrisi oluşturulmuştur. (KOOPBİS, TOKBYS, Kurum İçi Kullanılan Programlar.)
- Kurum içi kullanılan programlarda Statik IP uygulaması kullanılmaktadır.
- Kurum içi kullanılan programlarda yetkili personel giriş yaparken SMS kodu ile giriş yapabilmektedir.
- Kurum içi kullanılan programlarda hareketsiz oturumlar belli bir dakikadan sonra yeniden giriş yapılması aşamasına yönlendirmektedir.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- 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 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 fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.

- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.

5.2. İDARİ TEDBİRLER

Veri Sorumlusu tarafından işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır;

- Veri Sorumlusu personelinin yürüttüğü iş ve işlemler sırasında kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri kazanmaları adına personelin tabi olduğu mevzuat ile ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Veri Sorumlusu tarafından yürütülen faaliyetlere ilişkin personellere gizlilik sözleşmeleri imzalatılmaktadır.
- Benimsenen “veri minimizasyonu” ilkesi kapsamında işlenen kişisel veriler yalnızca yetkili ve ilgili personelin erişimine açıktır.
- Kişisel veri içeren belge ve kayıtlar KVKK’da belirtilen usullere uygun şekilde muhafaza edilmektedir.
- Güvenlik politika ve prosedürlerine uymayan personellere yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- İlgili Kişi Başvuru Formu üzerinden Veri Sorumlusu’na yönlendirilen talep ve şikayetlerin kontrolü düzenli şekilde gerçekleştirilip; ilgili kişiye talebini yönelttiği tarihten başlayarak en geç 30 (otuz) gün içerisinde gerekçeli dönüş yapılmaktadır.
- Veri Sorumlusu herhangi bir veri ihlaliyle karşılaşması halinde durumun tespitinin ardından; veri güvenliği sorunları raporlanarak söz konusu ihlal durumu Kişisel Verileri Koruma Kurumu’nun resmi internet sitesinde yer alan Veri İhlal Formu’ nu usulüne uygun şekilde doldurmaya özen gösterecektir.
- Personelin kullanımına bırakılmış tüm cihaz, portal, uygulama ve yazılımlarda personele özgü atanmış kullanıcı adı ve parola bulunmaktadır.
- Personelin kullanımına bırakılmış tüm cihaz, portal, uygulama ve yazılımlarda personelin görev ve pozisyonuna uygun olarak tanımlanmış kısıtlı erişim uygulanmaktadır.

- Görev değişikliği veyahut personelin Veri Sorumlusu ile ilişkisinin kesilmesi halinde; kendisine tanımlanan erişim yetkisi derhal düzenlenmektedir.

5.3. ÖZEL NİTELİKLİ KİŞİSEL VERİLER HUSUSUNDA UYGULANAN İDARİ VE TEKNİK TEDBİRLER

KVKK'nun 22'nci maddesinin birinci fıkrasının (ç) ve (e) bentleri uyarınca Veri Sorumlusu tarafından aşağıda sayılan önlemler alınmaktadır;

Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan personellere yönelik;

- KVKK ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında gerekli teknik beceri ve farkındalığı kazanması adına konuyla ilgili eğitim sağlanmıştır.
- Personelle konuyla ilgili gizlilik sözleşmeleri yapılmıştır.
- Personellere yönelik tanımlana yetki kontrolleri periyodik olarak kontrolü gerçekleştirilmektedir.
- Görev değişikliği olan ya da Veri Sorumlusu ile ilişkisi kesilen personellerin bu alandaki yetkileri derhal kaldırılmaktadır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;

- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması,

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;

- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmıştır.
- Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmektedir.

6. SAKLAMA VE İMHA SÜRELERİ

Veri Sorumlusu, KVKK ve ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verileri saklama ve imha sürelerinin tespitinde belirtilen kriterlerden yararlanmaktadır.

Veri Sorumlusu 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 Envanteri'nde,
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında,

- Görev değişikliği veyahut personelin Veri Sorumlusu ile ilişkisinin kesilmesi halinde; kendisine tanımlanan erişim yetkisi derhal düzenlenmektedir.

5.3. ÖZEL NİTELİKLİ KİŞİSEL VERİLER HUSUSUNDA UYGULANAN İDARİ VE TEKNİK TEDBİRLER

KVKK'nun 22'nci maddesinin birinci fıkrasının (ç) ve (e) bentleri uyarınca Veri Sorumlusu tarafından aşağıda sayılan önlemler alınmaktadır;

Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan personellere yönelik;

- KVKK ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında gerekli teknik beceri ve farkındalığı kazanması adına konuyla ilgili eğitim sağlanmıştır.
- Personelle konuyla ilgili gizlilik sözleşmeleri yapılmıştır.
- Personellere yönelik tanımlana yetki kontrolleri periyodik olarak kontrolü gerçekleştirilmektedir.
- Görev değişikliği olan ya da Veri Sorumlusu ile ilişkisi kesilen personellerin bu alandaki yetkileri derhal kaldırılmaktadır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;

- Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması,

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;

- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınmıştır.
- Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmektedir.

6. SAKLAMA VE İMHA SÜRELERİ

Veri Sorumlusu, KVKK ve ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verileri saklama ve imha sürelerinin tespitinde belirtilen kriterlerden yararlanmaktadır.

Veri Sorumlusu 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 Envanteri'nde,
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında,

Yer verilmektedir.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde ilgili/yetkili birim tarafından güncellemeler yapılır.

Kişisel verinin saklanması ve imhasına ilişkin olarak KVKK veya yönetmeliklerde öngörülmüş olan sürelerle uyulmaktadır.

Anılan sürenin sona ermesi halinde; saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi ilgili/yetkili birim tarafından tarafında yerine getirilir.

KVKK'da veya yönetmeliklerde söz konusu verinin saklanması ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda;

- KVKK'nun 6'ncı maddesine göre özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının Veri Sorumlusu açısından önem derecesine göre belirlenir.
- Verinin saklanmasının KVKK'nun 4'üncü maddesinde belirtilen ilkelere uygunluğu sorgulanır. Saklanmasının KVKK'nun 4'üncü maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
- Verinin saklanmasının KVKK'nun 5 ve 6'ncı maddelerinde öngörülmüş olan istisnalardan hangileri kapsamında değerlendirilebileceği tespit edilir. Bu istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde ise silme, yok etme veya anonim hale getirme işlemleri uygulanır.

7. KİŞİSEL VERİLERİN İMHA USULLERİ

7.1. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri Sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmektedir.

Kişisel veriler çeşitli kayıt ortamlarında saklanabilmeleri mümkün olduğundan, bu verilerin silinmesinde kullanılacak yöntemler kayıt ortamlarına uygun olmalıdır. Veri Sorumlusu tarafından uygulanan yöntemler aşağıda sayılmaktadır.

Kağıt Ortamında Bulunan Kişisel Veriler: 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 ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılmaktadır.

Merkezi Sunucuda Yer Alan Veriler: Veriler işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir.

Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olduğuna dikkat edilmektedir. Ancak anılan işlemi yalnızca sistem yöneticisi gerçekleştirebilir.

7.2. KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri Sorumlusu kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmiştir.

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilir ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmektedir.

Çevresel Sistemler

Ortam türüne bağlı olarak kullanılan yok etme yöntemleri aşağıda yer almaktadır:

Ağ Cihazları: Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırma makineleri ile anlaşılmaz boyutta, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre yerel sistemlerde belirtilen yöntemlerin bir ya da birkaçı kullanılarak yok edilmektedir.

Fiziksel Yok Etme: Optik medya 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.

Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medya da fiziksel olarak yok edilmektedir.

7.3. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

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

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ	KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI KANUNİ DAYANAK
Personel İşlemlerinin Süreçlerinin Yürütülmesi	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	4857 Sayılı İş Kanunu ve İlgili Mevzuat / 6098 Sayılı Türk Borçlar Kanunu
Kamera Kayıtları	3 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
Tedarikçilere İlişkin Kişisel Veriler	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	6098 Sayılı Türk Borçlar Kanunu
Sözleşmeler	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	6098 Sayılı Türk Borçlar Kanunu
İnsan Kaynakları Süreçleri	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	4857 Sayılı İş Kanunu ve İlgili Mevzuat / 6098 Sayılı Türk Borçlar Kanunu
SGK Mevzuatı kapsamında tutulan veriler (Örn: İşe giriş bildirgeleri, pirim/hizmet belgeleri vb.)	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	4857 Sayılı İş Kanunu ve İlgili Mevzuat / 6098 Sayılı Türk Borçlar Kanunu
Ortaklara Ait "Ortaklık/Kredi Çerçeve Sözleşmesi Dosyası" Verileri	Hukuki İlişki Süresince +10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde	6102 Sayılı Türk Ticaret Kanunu

9. GÜNCELLEMELER

KVKK'na ve Kurul kararlarına ilişkin yapılan değişiklikler ışığında işbu politikada yapılan güncelleme ve değişiklikler aşağıdaki tablodadır.

GÜNCELLEME TARİHİ	DAYANAK	DEĞİŞİKLİĞİN KAPSAMI

10. PERİYODİK İMHA SÜRESİ

Kurum, Yönetmelik' in 11'inci maddesinde periyodik imha süresini 6 ay olarak belirlemiştir. Bu sebeple Veri Sorumlusu her yıl Haziran ve Aralık aylarında periyodik imha işlemini gerçekleştirmektedir.

11. POLİTİKA'NIN YAYINLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda saklanır ve veri sorumlusunun resmi internet sitesinde yayımlanır. Ver Sorumlusu, ihtiyaç duyuldukça gerekli olan bölümleri güncelleme hakkını saklı tutmaktadır. Güncellemelere ilişkin tablo işbu Politika'nın 8'inci başlığında bulunmakta olup; gerekli bilgiye ilgililer buradan ulaşabilmektedir.

İşbu Politika imza tarihinden itibaren yürürlüğe girmiş kabul edilir.

12. REFERANSLAR

İşbu Politika hazırlanırken,

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu,
- 30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,
- Kişisel Verileri Koruma Kurumu Yayınları,
- Kişisel Verileri Koruma Kurulu İlke Kararları,

Referans alınmıştır.

İşbu Metnin tüm hakları saklıdır. Veri sorumlusunun yazılı onayı olmaksızın kopyalanamaz ve çoğaltılamaz.