

Do You Use Tüketim Ürünleri San. A.Ş.

<https://doyouuse.com>



ÖZEL NİTELİKLİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Adres : Alkent 2000 Mah. Hadımköy Yolu Cad. Demir La Vida
Evleri B Blok No:149/1 B Büyükçekmece/İSTANBUL
Telefon : +90 (212) 875 45 45
Fax : +90 (212) 875 45 47
Web : www.cokamaci.com.tr
E-mail : kvk@cokamaci.com.tr

İçindekiler

1. AMAÇ	2
2. TANIMLAR	3

3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ	4
4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI İÇİN ALINAN TEKNİK VE İDARİ TEDBİRLER	4
4.1 İDARİ TEDBİRLER	5
4.2 TEKNİK TEDBİRLER	5
a. Elektronik Ortamda Muhafaza Edilen ve/veya Erişilen Özel Nitelikli Kişisel Veriler Bakımından Alınan Teknik Tedbirler	5
b. Fiziksel Ortamda Muhafaza Edilen ve/veya Erişilen Özel Nitelikli Kişisel Veriler Bakımından Alınan Teknik Tedbirler	6
5. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI	6
6. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI	6
7. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	7
7.1. Özel Nitelikli Kişisel Verilerin Silinmesi	7
7.2. Özel Nitelikli Kişisel Verilerin Yok Edilmesi	8
7.3. Özel Nitelikli Kişisel Verilerin Anonim Hale Getirilmesi	9
7.3.1 Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	9
7.3.2 Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	9
7.3.3 Anonimlik Güvencesi	10
8.SAKLAMA VE İMHA SÜRELERİ	10

1. AMAÇ

Do You Use Tüketim Ürünleri San. A.Ş. tarafından hazırlanan İşbu Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Politikası' nın amacı, Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarihli ve

2018/10 sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler kararından doğan hukuki yükümlülüklerin yerine getirilmesi ile özel nitelikli kişisel verilerin işlenmesinde alınan teknik ve idari tedbirlerin ortaya konulmasıdır. Veri Sorumlusu konumunda olan Do You Use Tüketim Ürünleri San. A.Ş. bundan böyle “Şirket” olarak adlandırılacaktır.

2. TANIMLAR

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
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 kişilerdir.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi. (“Politika” da “veri sahibi” şeklinde ifade edilmektedir.)
Çalışan	Do You Use Tüketim Ürünleri San. A.Ş. ile bu şirketlerin iştirakleri olan grup şirketleri bünyesinde çalışan personel
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Hizmet Sağlayıcı	Do You Use Tüketim Ürünleri San. A.Ş. ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	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 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.
Özel Nitelikli 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.
Özel Nitelikli Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi
Özel Nitelikli Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Özel Nitelikli Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Politika	Özel Nitelikli Kişisel Verileri İşleme, Saklama ve İmha Politikası
Kurul	Kişisel Verileri Koruma Kurulu.
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.
Biyometrik	Kişilere ait parmak izi, avuç içi izi, yüz, iris, retina, kulak, ses, imza, yürüyüş biçimi, el damarı, vücut kokusu ve DNA bilgisi biyometrik veriler kapsamındadır. Kişilerin kimliğinin tespit edilebilmesini sağlayan benzersiz

	fiziksel veya davranışsal özellikleri içeren genel kavram.
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.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu 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.
Yönetmelik	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

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 özel nitelikli kişisel verilerdir.

Şirket, özel nitelikli kişisel verilerin işlenmesinde Kanun'a ve diğer mevzuat hükümlerine riayet eder. Bu doğrultuda özel nitelikli kişisel veriler aşağıdaki ilkelere uygun olarak işlenir:

- Hukuka ve dürüstlük kurallarına uygun olma
- Doğru ve gerektiğinde güncel olma
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
- Belirli, açık ve meşru amaçlar için işlenme
- Mevzuatta öngörülen ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Özel nitelikli kişisel verilerin işlenmesi yasaktır. Ancak bu verilerin işlenmesi;

- a. İlgili kişinin açık rızasının olması,
- b. Kanunlarda açıkça öngörülmesi,
- c. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- d. İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,
- e. Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
- f. Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,
- g. İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,
- h. Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması, halinde mümkündür."

4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI İÇİN ALINAN TEKNİK VE İDARİ TEDBİRLER

Şirket, özel nitelikli kişisel verilerin Kanun'a ve ilgili mevzuata uygun olarak işlenmesi ile özel nitelikli kişisel verilerin güvenliğinin sağlanması için Kişisel Verileri Koruma Kurumunun ilan ettiği alınması gereken yeterli önlemleri almaktadır. Bu kapsamda alınan tedbirler aşağıda sıralanmıştır:

4.1 İDARİ TEDBİRLER

- Şirket, özel nitelikli kişisel verilerin işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli Gizlilik konusunda düzenli eğitimler vermektedir.
- Şirket, çalışanları ile veri güvenliğinin sağlanması için gizlilik sözleşmeleri akdetmektedir.
- Verilere erişim yetkisine sahip kullanıcılar, yetki kapsamı ve süreleri net olarak tanımlanmakta ve periyodik yetki kontrolleri gerçekleştirilmektedir.
- Görev değişikliği olan ya da işten ayrılan çalışanların kişisel verilere erişim yetkileri derhal kaldırılmaktadır. Şirket, bu kapsamda çalışanlara tahsis etmiş olduğu envanterleri derhal iade almaktadır.

4.2 TEKNİK TEDBİRLER

a. Elektronik Ortamda Muhafaza Edilen ve/veya Erişilen Özel Nitelikli Kişisel Veriler Bakımından Alınan Teknik Tedbirler

- Sızma (Penetrasyon) testleri ile Şirketimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirketimizin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağı oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- 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.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresi kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı

ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

b. Fiziksel Ortamda Muhafaza Edilen ve/veya Erişilen Özel Nitelikli Kişisel Veriler Bakımından Alınan Teknik Tedbirler

- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri alınmaktadır.
- Bu ortamların fiziksel güvenliği sağlanmakta ve yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

5. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI

Şirket, özel nitelikli kişisel verileri Kanun'un 8. ve 9. maddelerinde yer alan veri işleme şartları çerçevesinde aktarmaktadır. Veri güvenliğini sağlama amacıyla Şirket tarafından veri aktarımında aşağıdaki kurallar uygulanmakta ve bu kapsamda periyodik denetimler gerçekleştirilmektedir.

✓ **E-Posta Yoluyla Aktarım**

Özel nitelikli kişisel verilerin e-posta yoluyla aktarıldığı hallerde şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarım yapılmaktadır.

✓ **Taşınabilir Bellek, CD, DVD Gibi Ortamlar Yoluyla Aktarım**

Özel nitelikli kişisel verilerin taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarıldığı hallerde kriptografik yöntemlerle şifreleme işlemi yapılmakta ve kriptografik anahtar farklı bir ortamda tutulmaktadır.

✓ **Farklı Fiziksel Ortamlardaki Sunucular Arasında Aktarım**

Farklı fiziksel ortamlardaki sunucular arasında özel nitelikli kişisel veri aktarımında, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.

✓ **Kâğıt Ortamı Yoluyla Aktarım**

Özel nitelikli kişisel verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınmakta ve evrak "gizlilik dereceli belgeler" formatında gönderilmektedir.

6. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

Özel nitelikli kişisel veriler, Şirket tarafından Kanun ile diğer mevzuata ve Kurul tarafından yayımlanan Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler kararına uygun olarak aşağıdaki hallerde saklanmaktadır:

- Veri sahibinin açık rızasının elde edilmiş olması
- Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin saklanması kanunlarda öngörülmüş olması
- Sağlık ve cinsel hayata ilişkin verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla saklanması
- Şirket tarafından Kanun ile diğer mevzuata uygun olarak saklanan özel nitelikli kişisel veriler aşağıdaki sebeplerin ortaya çıkması halinde re'sen ya da veri sahibinin talebi üzerine silinir, yok edilir ya da anonim hale getirilir:

- Özel nitelikli kişisel veri saklama faaliyetinin veri sahibinin açık rızasına dayandığı hallerde açık rızanın geri alınmış olması
- Özel nitelikli kişisel verilerin saklanma amacının gerçekleşmiş, imkansızlaşmış ya da diğer herhangi bir yolla ortadan kalkmış olması
- Özel nitelikli kişisel verilerin saklanmasına dayanak teşkil eden mevzuat hükümlerinin değişmesi ya da yürürlükten kalkması
- Kanun'un 6. maddesinde yer alan işleme şartlarının tamamının ortadan kalkmış olması
- Veri sahibinin Şirket'e usulüne uygun olarak ilettiği özel nitelikli kişisel verilerinin imhasına ilişkin talebinin Şirket tarafından haklı görülmesi ve olumlu sonuçlandırılması
- Şirket'in, veri sahibi tarafından özel nitelikli kişisel verilerinin imhası 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.

7. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Şirket tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde Şirket tarafından re'sen yahut İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen teknikler ile imha edilecektir.

7.1. Özel Nitelikli Kişisel Verilerin Silinmesi

Şirket tarafından kişisel verilerin silinmesi ve yok edilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır.

Sunucularda Yer Alan Kişisel Verilerin Yazılımdan Güvenli Olarak Silme: 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 kullanılarak silinecektir.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesinde ise; 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 yöntemleri kullanılarak işlem yapılacaktır.

Ancak, Şirket içerisinde, gerektiğinde 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 kişiyi erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

Uzman Tarafından Güvenli Olarak Silme: Şirket gerekli gördüğü durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

Kâğıt Ortamında Bulunan Kişisel Verilerin Karartılması: Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemi ile de kişisel veriler silinebilecektir.

Tablo -4 : Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim

	yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

7.2. Özel Nitelikli Kişisel Verilerin Yok Edilmesi

Şirketimiz tarafından kullanılacak olan yok etme yöntemleri aşağıda gösterilmiştir.

De-manyetize Etme: Manyetik medyanın yüksek değerinde manyetik alanda fiziksel değişime tabi tutularak üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir.

Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür verilerin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi işlemidir. Özellikle yazılı kâğıt ve defterler ve mikrofişler bu şekilde yok edilir.

Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az 8 kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilesini imkânsızlaştıran veri yok etme yöntemidir.

Bulut İmhası : Bulut sistemler üzerinde tutulan kişisel verilerin imha bildiriminin anlaşmalı servis sağlayıcıya yapılmasının ardından kişisel verilerin şifreleme anahtarlarının tüm kopyalarının imha edilmesi işlemidir.

Çevresel Sistemlerde Yer Alan Kişisel Verilerin İmhası: Yazıcı, parmak izi ünitesi, kapı giriş turnikesi gibi sistemler içerisinde yer alan kişisel verileri barındıran cihazlar, üzerine yazma, manyetize etme veya fiziksel yok etme uygulanarak imha edilir. Bu imha işlemleri, cihazların yedekleme, bakım ve benzeri işlemlere tabi tutulmasından önce yapılır.

Tablo -5 : Özel Nitelikli Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerinde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

7.3. Özel Nitelikli 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.

7.3.1 Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

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 anonimleştirmeye 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.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.

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. Örneğin, şirketin futbol takımının yedek listesinde olan ilgili veri sorumluları arasında yalnızca bir kişi 65 yaşında ise yaş, cinsiyet ve sağlık durumu yönünden futbol oynayabilecek olup olmadığı bilgisinin birlikte saklandığı bir veri kümesinde ‘Yaş:65’ yerine ‘Bilinmiyor’ yazılması veya bu kısmın boş bırakılması anonimleştirmeyi sağlayacaktır.

Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin; çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

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.

7.3.2 Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.

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.

Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (*büyükten küçüğe gibi*) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır.

(Örneğin, maaş bilgisi için; 50.000 TL altı ve üstü iki grup yapılır ise, 50.000 ve daha az maaş alan kişilerin maaşlarının toplamı kişi sayısına bölünür ve 50.000TL altında maaş alan herkesin maaş kümesine elde edilen bu değer yazılır.)

Veri Değiş Tokuşu: Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.

7.3.3 Anonimlik Güvencesi

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir.

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulmaması,
- Bir ya da birden fazla değer bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

8.SAKLAMA VE İMHA SÜRELERİ

Şirket 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, Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.
- Söz konusu saklama süreleri üzerinde, gerekmesi halinde Şirket yönetimi tarafından güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re 'sen silme, yok etme veya anonim hale getirme işlemi Şirket yönetiminin onayı ile KVK sürecinde görevlendirilen sorumlu personel tarafından yerine getirilir.

İşbu Politikada yapılan değişiklikler aşağıdaki tabloda gösterilmektedir.

Politika Güncelleme Tarihi	Değişiklikler
21/03/2024	Oluşturma
14/04/2025	Kanun Değişiklikleri