TELESES MAĞAZACILIK TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

v.1

İçindekiler

1. AMAÇ

Kişisel Verileri Saklama ve İmha Politikası ("**Politika**"), Teleses Mağazacılık Ticaret Anonim Şirketi ("**Teleses**")'nin kişisel veri saklama ve imha faaliyetlerine yönelik Teleses tarafından benimsenen ve uygulanan yöntemler konusunda açıklamalarda bulunmak ve tüm ilgili tarafların bilgilendirilmesi amacı ile oluşturulmuştur.

Teleses'in gerçekleştirdiği tüm kişisel veri saklama ve imha faaliyetleri, işbu Politika"ya uygun olarak gerçekleştirilir.

2. KAPSAM

İşbu Politika, Teleses'in kişisel verilerini işlemekte olduğu tüm ilgili kişilere (çalışan adayları, çalışanlar, ziyaretçiler, gerçek kişi tedarikçi ve iş ortakları, tedarikçi ve iş ortaklarının çalışanları ve ilgili diğer üçüncü kişiler) ait kişisel verileri kapsamakta olup Teleses tarafından yönetilen tüm kişisel veri kayıt ortamları ile kişisel veri işleme süreçlerinde işbu Politika uygulanır.

3. GÖREV ve SORUMLULUK

İşbu Politika'nın hazırlanması ve güncel tutulması ile Teleses'deki faaliyetlerin Politika'ya uygun gerçekleştirildiğinin denetlenmesi işlerinden Teleses Kişisel Verileri Koruma Komitesi ("**KVK Komitesi/Komite**") sorumludur. Komite ve diğer sorumluların görev ve sorumluluklarına ilişkin tablo aşağıda yer almaktadır.

Unvan	**Görev ve Sorumluluk**
KVK Komitesi ("**Komite**")	KVK Komitesi, Teleses'deki kişisel veri işleme süreçlerinin Kanun'a, ikincil mevzuata, Kurul kararlarına ve rehberlerine uygun olarak işlenmesi, muhafaza edilmesi ve aktarılması, buna ilişkin belirlenen kriter ve kuralların çalışanlara ve Teleses adına veri işleyenlere duyurulması, çalışanlara eğitim verilmesi ve çalışanların farkındalığının artırılması, Özel Nitelikli Kişisel Veri işlenen, muhafaza edilen ve aktarılan tüm faaliyetlerde veri güvenliğini sağlamaya yönelik teknik ve idari tedbirleri alınması ile sorumludur.
KVK Komitesi Başkanı ("**KVK Komitesi Başkanı/Komite Başkanı**")	Komite Başkanı, KVK Komitesi'nin Politika'daki görevlerini yerine getirebilmesi için gerekli durumlarda Komite'yi toplantıya çağırmak ve Komite'nin gündemini belirlemek ile sorumludur.
KVK Komitesi Sekreteri ("**KVK Komitesi Sekreteri/ Komite Sekreteri**")	Komite Sekreteri, KVK Komitesi'nin Politika'daki görevlerini yerine getirebilmesi için gerekli işlemleri yapmakla sorumludur.

Birim Yöneticisi	Birim Yöneticisi, biriminde kişisel veri işleme süreçlerinin Politika'ya uygun olarak gerçekleştirilmesinden sorumludur.
Teleses Bilgi Teknolojileri Direktörü ("**Bilgi Teknolojileri Direktörü**")	Bilgi Teknolojileri Direktörü, biriminde kişisel veri işleme süreçlerinin Politika'ya uygun olarak gerçekleştirilmesinden sorumludur. Ayrıca diğer birimlerin kişisel veri işleme süreçlerinin Politika'ya uygun biçimde ve yöntemde gerçekleştirmesine destek verir.
Çalışanlar, Veri İşleyenler ve ilgili diğer kişiler	Kişisel veri işlerken Politika'daki kural ve talimatlara uygun olarak işlemek konusunda üzerine düşen faaliyetleri yerine getirirler, gerekli durumlarda çalışanlar Birim Yöneticilerine, veri işleyenler ve ilgili diğer kişiler de KVK Komite Başkanı'na bilgi verirler.

4. TANIMLAMALAR VE KISALTMALAR

Bu doküman içinde geçen kısaltmalar ve tanımlar aşağıdaki gibidir:

Alıcı Grubu	**:**	Teleses'in kişisel verileri aktardığı gerçek veya tüzel kişiler
Açık Rıza	**:**	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme	**:**	Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Çalışan	**:**	Teleses çalışanları
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
Envanter	**:**	Teleses'in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verilerin işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu 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 detaylandırdığı envanter
Teleses	:	Teleses Mağazacılık Ticaret Anonim Şirketi
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
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/İşleme	:	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
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
Periyodik İmha	:	Kanun'da yer alan kişisel verilerin işlenme 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 Verileri Saklama ve İmha Politikası
Silme	:	Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Veri İşleyen	:	Teleses'in verdiği yetkiye dayanarak Teleses adına kişisel verileri işleyen gerçek veya tüzel kişi

Veri Kayıt Sistemi	**:**	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	**:**	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
VERBİS	**:**	Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemi, Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	**:**	28 Ekim 2017 tarihli Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
Yok Etme/Yok edilme	**:**	Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi

5. KAYIT ORTAMLARI

Kayıt Ortamı	Kayıt Ortamı Tipi	Sistem Sorumlusu	İlgili Departman	İmha Sorumlusu
Veri Tabanı				
E-Posta				
Sunucular				
Bulut Sunucuları				

Yazılımlar				
Bilgi Güvenliği Cihazları (Güvenlik duvarı, TPS vb.)				
Taşınabilir Bellek, CD vb.				
Kamera Kayıt Sistemleri				
Arşiv				
Fiziksel Ortamlar				

6. SAKLAMA ORTAMLARI

Teleses, tamamen otomatik veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlediği kişisel verileri hukuka uygun olarak aşağıda yer alan ortamlarda saklamaktadır:

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (File Server, Yedekleme, E-posta, Veri tabanı, Uygulama (Activtrak, Timedoctor vb.), Web, hosting hizmeti alınan üçüncü kişilere ait sunucular, masa telefonu sistemi sunucuları, Wi-fi sunucuları vb.) Yazılımlar (JIRA, Goverlan, SAP, vb.) Bilgi Güvenliği Cihazları (güvenlik duvarı, saldırı tespit ve engelleme, antivirüs vb.) Kişisel Bilgisayarlar (Masaüstü, dizüstü)	Kâğıt Dosyalar, Ofis Dolapları

Kamera Kayıt Sistemleri Optik Diskler (CD, DVD vb.) Çıkartılabilir Bellekler (USB, Harici Disk vb.)	

7. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

7.1. Saklamaya ilişkin Açıklamalar

Teleses, benimsemiş olduğu vizyon, misyon ve temel değerleri gereğince, bağlı olduğu mevzuatlar doğrultusunda, çalışanlarına, üyelerine ve iş ortaklarına ve ilgili diğer üçüncü kişilere en iyi hizmeti sağlamak için teknolojik kaynak ve altyapıları da kullanarak kişisel verileri işler.

Kişisel veriler, Kanun'un 4. maddesinde belirtilen başta *"kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi"* ilkesi ve diğer ilkeler göz önünde bulundurularak saklanır.

Kişisel veriler,

- Teleses tarafından ticari faaliyetlerinin sürdürülebilmesi,
- İnsan kaynakları süreçlerinin yürütülmesi, çalışan haklarının ve yan haklarının planlanması ve hizmet sözleşmelerinin ifası,
- Teleses iş ortakları ve her türlü mal veya hizmet alımı yaptığı tedarikçiler ile süreçlerin işletilebilmesi, gerekli durumlarda bu kişilerle veya iş ilişkisi içerisine girilebilecek diğer kişilerle iletişim kurulabilmesi,
- Teleses merkezinin ve çalışanlarının güvenliğinin sağlanabilmesi,
- Teleses'in taraf olduğu her türlü sözleşme veya ilgili mevzuatlardan doğan hak ve taleplerini kullanabilmesi,
- Hukuki yükümlülüklerin yerine getirilebilmesi,

amaçlarıyla, fiziki veya elektronik ortamlarda güvenli bir biçimde Kanun ve diğer ilgili yönetmelikte belirtilen sınırlar çerçevesinde saklanır.

Teleses'in bünyesinde kişisel veriler, Kanun'un 5. ve 6. maddesinde sayılan aşağıdaki hukuki sebepler çerçevesinde işlenir:

- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- Kişisel verilerin; Teleses'in taraf olduğu sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Bir hakkın tesisi, kullanılması veya korunması için Teleses tarafından veri İşlemenin zorunlu olması,
- Kişisel verilerin Teleses'in bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,

- İlgili Kişi'nin kendisi tarafından alenileştirilmiş olması,
- İlgili Kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Teleses'in meşru menfaatleri için veri İşlenmesinin zorunlu olması,
- İşleme için ilgili kişinin açık rızasının olması gereken saklama faaliyetleri açısından ilgili kişinin açık rızası,
- Özel Nitelikli Kişisel Veriler için ise, ilgili kişinin açık rızası veya Kanun'un 6. maddesinde sayılan diğer istisnalardan birinin var olması.

7.2. İmhaya İlişkin Açıklamalar

Yönetmelik uyarınca, aşağıda sayılan hallerde kişisel veriler ya da Özel Nitelikli Kişisel Veriler, Teleses tarafından re'sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Açık rıza şartına istinaden kişisel veri işlenen hallerde, İlgili Kişi'nin açık rızasını geri alması,
- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- İlgili Kişinin, Kanun'un 11.maddesinden doğan hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun Teleses tarafından kabul edilmesi ya da Teleses tarafından talebin kabul edilmemesi üzerine İlgili Kişi tarafından Kurul'a yapılan başvuru üzerine Kurul'un İlgili Kişi'nin talebini kabul etmesi ve bu durumu Teleses'e bildirmesi,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması,
- Kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması halinde.

8. UYGULANAN TEKNİK VE İDARİ TEDBİRLER

Teleses, kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12. ve 6/4 maddesi uyarınca Kurul'un kararlarında ve rehberlerinde belirlediği teknik ve idari tedbirleri alır.

8.1. İdari Tedbirler

- 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.
- 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 veriler mümkün olduğunca azaltılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.

- İş süreçleri üzerinde risk analizleri gerçekleştirilmektedir.
- Envanterler oluşturulmuş, periyodik aralıklarla gözden geçirilmektedir.
- Kişisel verilerin korunması mevzuatı ve veri güvenliği hakkında eğitimlerin düzenlenmektedir.
- Kişisel verilerin korunması hakkında farkındalık çalışmaları yürütülmektedir.

8.2. Teknik Tedbirler

- Çalışanlar için yetki matrisi oluşturulmuştur.
- Ağ ve uygulama hizmetlerine kimlik doğrulama ile erişim gerçekleştirilmektedir.
- Ağ ve uygulama hizmetlerine erişimde şifreleme kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- 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.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurul'a bildirmek için Kurum 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 güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Bilişim sistemleri, kötü niyetli yazılımlara karşı uygulamalar aracılığı ile korunmaktadır.

9. KİŞİSEL VERİLERİ İMHA YÖNTEMLERİ

Bu Politika'da yukarıda 6. maddede belirtilen şartların ortadan kalkması halinde, kişisel veriler Teleses tarafından kendiliğinden veya İlgili Kişi'nin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta İlgili Kişi tarafından Teleses'e başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlanır ve İlgili Kişi'ye bilgi verilir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir,
- Kişisel verileri İşleme şartlarının tamamı ortadan kalkmamışsa, bu talep Veri Sorumlusu tarafından Kanun'un 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri kendiliğinden silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Teleses tarafından seçilir. Ancak, İlgili Kişi'nin belirli bir İmha yöntemini talep etmesi halinde, Teleses tarafından belirlenecek uygun yöntem, gerekçesi açıklanarak seçilir.

9.1. Silme

Basılı Doküman Üzerinde: Kâğıt ortamında bulunan kişisel veriler Şirket tarafından karartma yöntemi kullanılarak silinmelidir. 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 yapılır.

Bulut Çözümlerinde: Bulut sisteminde veriler silme komutu verilerek silinir ve veriye erişme yetkisi olan İlgili Kullanıcılar'ın varsa geri getirme yetkileri kaldırılır.

Dosya Sunucusunda (File Server): Dosya sunucusunda bulunan veriler silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde veriye erişme yetkisi olan İlgili Kullanıcılar'ın erişim haklarının kaldırılır. İşlem gerçekleştirilirken, İlgili Kullanıcılar'ın aynı zamanda sistem yöneticisi olmadığına dikkat edilir.

Taşınabilir Ortamlarda: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve veri silineceği zaman tekrar geri getirilemeyecek şekilde biçimlendirilir.

Veri Tabanında: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinir. İşlem gerçekleştirilirken İlgili Kullanıcılar'ın aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

İşyeri Bilgisayarında: Kişisel verilere kimlik doğrulama ile erişim sağlanır ve işletim sistemi komutları kullanılarak silinir.

9.2. Yok Etme

Basılı Dokümanlar: Kişisel verilerin bulunduğu kâğıt ortamlar, kâğıt kırpma makinelerinde imha edilir.

Yerel Sistemler: Aşağıdaki yöntemlerden bir ya da birkaçı Teleses tarafından belirlenerek kullanılabilir.

- **De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
- **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir.
- **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir.

Çevresel Sistemler: Aşağıdaki yöntemlerden bir ya da birkaçı Teleses tarafından belirlenerek kullanılabilir.

- **Ağ cihazları (switch, router vb.):** Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yerel sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da yerel sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- **Manyetik bant:** Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

- **Manyetik disk gibi üniteler**: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

- **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. a'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

- **Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre yerel sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

- **Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme

komutu bulunmamaktadır. Yerel sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

9.3. Anonim Hale Getirme

Teleses, anonimleştirme için verinin bulunduğu ortam ve İşleme türüne göre aşağıdaki yöntemlerinden birini kullanır:

- **Değer düzensizliği sağlamayan anonim hale getirme yöntemleri**
    - Değişkenleri Çıkartma
    - Kayıtları Çıkartma
    - Genelleştirme
    - Bölgesel Gizleme
    - Alt ve Üst Sınır Kodlama
    - Global Kodlama
    - Örnekleme
- **Değer düzensizliği sağlamayan anonim hale getirme yöntemleri**
    - Mikro Birleştirme
    - Veri Değiş Tokuşu
    - Gürültü Ekleme

10. VERİ SAKLAMA VE İMHA SÜRELERİ

Veri saklama ve imha süreleri Envanterde detaylı olarak tutulur. Verilerin saklama ve imha süreleri aşağıda belirtildiği gibidir.

Süreç	Saklama Süresi	Periyodik İmha Süresi
Çalışan Adaylarına ilişkin İnsan Kaynakları Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanlara İlişkin İnsan Kaynakları Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Sağlığı ve İş Güvenliği Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk

		periyodik imha süresinde
Tedarikçiler, İş Ortakları ve Üye İşyerleri Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşme Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	90 gün	Saklama süresinin bitiminde
İnternet ve Ağ Erişim Kayıtları	2 yıl	Saklama süresinin bitiminde
Hukuki Uyuşmazlık süreçleri	Hukuki sürecin tamamlanmasını takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Süreçleri	Kişisel veriler herhangi bir hukuki sürece konu olmaması halinde şikâyet konusu sonuçlandıktan sonra, derhal imha edilir.	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Aydınlatma, bilgilendirme, izin ve açık rıza süreçleri	Hukuki ilişki sona erdikten sonra 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Açık rızaya dayalı olarak işlenen kişisel veriler	Açık rızayla işlenen veriler için açık rıza geri alınıncaya kadar	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde veya İlgili Kişi'nin talebinin Teleses'e ulaşmasından itibaren en kısa süre içinde

11. PERİYODİK İMHA SÜRESİ VE İMHA KAYITLARININ TUTULMAS

Teleses, Yönetmeliğin 11. maddesine de uygun olarak periyodik imha süresini 6 (altı) ay olarak belirlemiştir. Buna göre, Teleses, her yıl Ocak ve Temmuz aylarında periyodik imha işlemi gerçekleştirir.

Teleses, Komite aracılığıyla kişisel verilerin tamamının, planlanan zaman aralığında ve tespit edilen kayıtlarla imha edilip edildiğini kontrol eder ya da ettirir. Kişisel verilerin imhasının gerçekleştirilmesinin ardından İmhayı gerçekleştirenler, Ek-1'de yer alan Veri İmha Formu'nu doldurur ve Komite'ye iletir. Bu form Teleses tarafından diğer hukuki yükümlülükler saklı kalmak üzere en az üç yıl süreyle saklanır.

12. GÜNCELLENME PERİYODU

Teleses, Kanun'da yapılan değişiklikler nedeniyle, Kurul kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda veya herhangi bir nedenle ihtiyaç duyması halinde işbu Politika'yı değiştirebilir, güncelleyebilir.

İşbu Politika'da yapılan değişiklikler derhal metne işlenir, değişikliklere ilişkin açıklamalar aşağıdaki tabloya işlenir ve Politika'nın güncel versiyonu Komite'nin belirlediği yetkili tarafından Teleses bünyesinde kişisel verilerin tutulduğu, işlendiği veya aktarıldığı sistemleri kullanan / yöneten birimler, çalışanlar ve ilgili diğer kişilere duyurulur.

No	Tarih	Açıklama ve Yapılan Değişiklikler
v.1	__/__/28/09/2024	Kişisel Veri Saklama ve İmha Politikası yayımlandı.
v.2		

EK-1

KİŞİSEL VERİ İMHA TUTANAĞI

İşbu tutanak Veri Sorumlusu olan **Teleses Mağazacılık Ticaret Anonim Şirketi** tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu Md. 7 (1) **"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir."** Hükmü kapsamındaki hukuki yükümlülüğün yerine getirildiğini kayıt altına almak için düzenlenmiştir. İmha Edilen dokümanların / dosyaların içerik detayı aşağıda belirtilmiştir.

İLGİLİ KİŞİNİN İMHA TALEBİ İSTEĞİ /İMHA SEBEBİ			
İLGİLİ KİŞİ		**(VARSA) İLGİLİ KİŞİNİN TALEP TARİHİ**	
İMHA TARİHİ		**DİĞER (Lütfen Belirtiniz)**	

İMHA EDİLEN	**İÇERDİĞİ KİŞİSEL VERİLER**	**İMHA YÖNTEMİ**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

İMHA İŞLEMİNİ GERÇEKLEŞTİREN
Adı Soyadı / Görevi / İmza

İMHAYA ŞAHİTLİK EDENLER

Adı Soyadı / Görevi / İmza **Adı Soyadı / Görevi / İmza**

KİŞİSEL VERİ İMHA TUTANAĞI TUTULMASI SÜRECİNE İLİŞKİN

İLGİLİ KİŞİ AYDINLATMA METNİ

İşbu veri imha tutanağında yer alan imha işlemini gerçekleştiren ile imha işlemine tanıklık eden veri ilgililerine ait adı, soyadı, görev ve imza verileri 6698 Sayılı KVK Kanunu uyarınca veri sorumlusu olan **Teleses Mağazacılık Ticaret Anonim Şirketi** tarafından İlgili mevzuat ve şirketimizin veri saklama ve imha politikasına uygun olarak verilerin silindiği, yok edildiği yahut anonimleştirildiğinin kayıt altına alınabilmesi ve ilgili kamu kurum ve kuruluşları tarafından talep edildiğinde sunulabilmesi için düzenlenmiş olup, bu amaçla sınırlı olarak formda yer alan kişisel verileriniz "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" ve "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması." hukuki sebeplerine dayalı olarak otomatik ve otomatik olmayan yöntemlerle işlenebilecek ve talep edilmesi halinde mevzuatta öngörülen sınırlamalar dahilinde ilgili kamu kurum ve kuruluşlarına yahut tutanak konusu kişisel verilerle ilgili olarak başvuruda bulunan ilgili kişiye aktarılabilecektir. Kanun'un 11. Maddesinde belirtilen haklarını ile ilgili olarak bize aşağıdaki yöntemlerle ulaşabilirsiniz.

Yazılı başvuru:
Lütfen başvurularınızı aşağıdaki ifadeyi zarfın üzerine/yazının başlığına aynen yazınız.
"Teleses Mağazacılık Ticaret Anonim Şirketi Hukuk Departmanı dikkatine"
Başvurularınızı aşağıdaki adrese gönderiniz:
Beytepe Mah. Ali Şir Nevai Cad. no: 9/C Çankaya/ANKARA

E-Posta yoluyla başvuru:
Lütfen başvurunuzun "Konu" kısmına aşağıdaki ibareyi aynen yazınız.
"Teleses Mağazacılık Ticaret Anonim Şirketi Hukuk Departmanı dikkatine"
Başvurularınızı aşağıdaki adrese gönderiniz:
magazacilik@teleses.com.tr & teleses.magazacilik@hs03.kep.tr