TELESES MAĞAZACILIK TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİ İŞLEME VE KORUMA POLİTİKASI

v.1

İçindekiler

1. AMAÇ

İşbu Kişisel Veri İşleme ve Koruma Politikası ("**Politika"**), Teleses Mağazacılık Ticaret Anonim Şirketi ("**Teleses**")'nin kişisel veri işleme faaliyetlerine yönelik olarak Teleses tarafından benimsenen ve uygulanan yöntemler ve kurallar konusunda açıklamalarda bulunmak amacı ile oluşturulmuştur.

2. KAPSAM

İşbu Politika, Teleses ve/veya Teleses adına Veri İşleyenler tarafından kişisel veri işlenen tüm kişisel veri işleme süreçlerini kapsamakta olup Teleses ve/veya Teleses adına Veri İşleyenler tarafından yönetilen tüm kişisel veri kayıt ortamları ile kişisel veri işleme süreçlerinde uygulanır.

Teleses ve/veya Teleses adına Veri İşleyenler tarafından işlenen kişisel veri işleme süreçlerinde, kişisel verilerle birlikte özel nitelikli kişisel veri de işleniyorsa veya yalnızca özel nitelikli kişisel veri işleniyorsa, bu durumda işbu Politika'ya ek olarak Teleses Özel Nitelikli Kişisel Veri İşleme Politikası'nda yer alan kurallar da 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**")	Komite, Teleses'deki kişisel veri işleme süreçlerinin Kanun'a, ikincil mevzuata, Kurul kararlarına ve rehberlerine uygun olarak işlemek, muhafaza etmek ve aktarmak, buna ilişkin belirlenen kriter ve kuralların çalışanlara ve Teleses adına veri işleyenlere duyurmak, çalışanların eğitimi ve farkındalığını artırmak, özel nitelikli kişisel veri işlenen, muhafaza edilen ve aktarılan tüm faaliyetlerde veri güvenliğini sağlamaya yönelik teknik ve idari tedbirleri almak 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 yapmak ile 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 vermek ile sorumludur.
Çalışanlar, Veri İşleyenler ve ilgili diğer kişiler	Kişisel veri işlerken Politika'daki kural ve talimatlara uygun olarak işlemek konusunda üzerine düşen faaliyetleri yerine getirmek, gerekli durumlarda çalışanlar Birim Yöneticilerine, Veri İşleyenler ve ilgili diğer kişiler de KVK Komite Başkanı'na bilgi vermek ile sorumludurlar.

4. TANIMLAR ve KISALTMALAR

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
Envanter	**:**	Teleses'in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri 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, (varsa) 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	:	Kişisel veriler'in 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
İrtibat Kişisi	:	Teleses'in Kanun ve ilgili mevzuattan doğan yükümlülüklerine ilişkin olarak Kurum ile iletişimi sağlamak amacıyla VERBİS'e kayıt esnasında bildirilen gerçek 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/İşleme	:	Kişisel veriler'in 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 Kişisel Veriler üzerinde gerçekleştirilen her türlü işlem
Kurum	:	Kişisel Verileri Koruma Kurumu
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 Veriler'in 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	:	Teleses Kişisel Veri İşleme ve Koruma Politikası

Silme	**:**	Kişisel verilerin silinmesi, kişisel verilerin İlgili Kullanıcı'lar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Veri İşleyen	**:**	Teleses'in verdiği yetkiye dayanarak Teleses adına Kişisel Veriler'i işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	**:**	Kişisel Veriler'in belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	**:**	Kişisel Veriler'in 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
Yok etme/Yok edilme	**:**	Kişisel Veriler'in yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi

5. KİŞİSEL VERİLERİN İŞLENMESİNE VE KORUNMASINA İLİŞKİN YÜKÜMLÜLÜKLER

Teleses veya Veri İşleyenler'i tarafından Kişisel Veriler'in işlenmesinde aşağıdaki kurallar uygulanır.

5.1. Kişisel Veri İşleme İlkelerine Uygunluk

Kişisel verilerin işlenmesinde aşağıdaki ilkelere uygun hareket edilir:

- Kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun hareket edilir. Kişisel veriler hiçbir şekilde İlgili Kişi'nin bilgisi olmaksızın toplanmaz ve işlenmez. Kişisel Veriler'in İlgili Kişi'den elde edilmemesi halinde Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ'in 6. maddesine uygun olarak hareket edilir.

- İşlenen Kişisel Veriler'in doğru ve güncel olmasını sağlamak için Kişisel Veri işleme süreçlerinde gerekli tedbirler alınır. Kişisel Veriler'i işlenen İlgili Kişi'ye verilerini güncellemesi ve var ise işlenen verilerindeki hataları düzeltmesi için başvuruda bulunma imkânı tanınır.

- Kişisel Veriler belirli, açık ve meşru amaçlarla, kapsamı ve içeriği açıkça belirlenmiş, mevzuat ve iş süreçlerinin devamlılığını sağlamak için belirlenen meşru amaçlar dahilinde işlenir. Bu doğrultuda, Kişisel Veriler'in işlenmesi mevzuatı kapsamında için hazırlanan hukuki metinlerde belirlilik ve açıklık ilkesine uygun hareket edilmesine hassasiyet gösterilir.

- Kişisel Veriler belirlenen amaçlarla bağlantılı, sınırlı ve ölçülü olarak işlenir. Bu kapsamda veri minimizasyonu ilkesi uyarınca, Teleses, Kişisel Veri işlerken işleme amacı ile ilgili olmayan ve işleme süreci için işlenmesi gerekli/zorunlu olmayan hiçbir Kişisel Veri'yi işlemez.

- Kişisel Veriler ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir. Bu süreler sona erdiğinde Kişisel Veriler'in işlenmesine son verilir ve Kişisel Veriler silinerek, yok edilerek veya anonimleştirilerek İmha edilir. Kişisel Veriler'in İmhasına ilişkin hususlar Teleses Kişisel Verileri Saklama ve İmha Politikası'nda belirlenir.

5.2. Aydınlatma Yükümlülüğü

Kanun'un 10. maddesinde yer alan aydınlatma yükümlülüğü ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ hükümleri uyarınca Teleses veya Veri İşleyenler, Kişisel Veri işlemeden önce veya en geç işlenmesi sırasında aşağıdaki hususlarda İlgili Kişiler'i aydınlatmakla yükümlüdür;

- Veri sorumlusu olarak Teleses'in kimliği (Teleses Mağazacılık Ticaret Anonim Şirketi)
- Hangi kişisel verilerin işleneceği,
- Kişisel Veriler'in hangi amaçla işleneceği,
- İşlenen Kişisel Veriler'in kimlere ve hangi amaçla aktarılabileceği,
- Kişisel verileri toplamanın yöntemi ve hukuki sebebi,
- İlgili Kişiler'in Kanun'un 11. maddesinde yer alan hakları.

Aydınlatmanın yapılmasında bir şekil şartı olmamakla birlikte, aydınlatma yükümlülüğünün yerine getirildiğini ispat yükümlülüğü Veri Sorumlusu olarak Teleses'e ait olduğundan, Kişisel Veri işleme süreci kurgulanırken aydınlatma yükümlülüğünün yerine getirildiğini tevsik edici önlemler alınır.

Bu önlemler aydınlatmanın yapılma yöntemine göre değişiklik gösterebilir. (Örn. Basılı evrak ile aydınlatma yapıldığı durumlarda İlgili Kişiler'den aydınlatma metninin sonunda imzası alınabilir, sesli ortamda aydınlatma yapılması halinde ilgili ses kaydı saklanabilir veya dijital ortamlarda aydınlatma yapıldığı durumlarda aydınlatma yapıldığını kanıtlar dijital log kayıtları saklanabilir.)

Kişisel Veriler'in işlenme amaçlarının değişmesi durumunda, İlgili Kişiler'e yeni Kişisel Veri İşleme amacına ilişkin aydınlatma kişisel veri işleme faaliyetine başlanmadan önce yapılır.

Ayrıca, Kişisel Veriler'in doğrudan İlgili Kişiler'den elde edilmediği durumlarda (örn. üçüncü kişi bir veri sorumlusundan kişisel veri alınması) da Teleses tarafından aydınlatma yükümlülüğü;

- Kişisel Veriler'in elde edilmesinden itibaren makul bir süre içerisinde,

- Kişisel Veriler'in İlgili Kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında,

- Kişisel Veriler'in aktarılacak olması halinde, en geç Kişisel Veriler'in ilk kez aktarımının yapılacağı esnada

yerine getirilir.

Kanun'un 28. maddesi uyarınca ise, İlgili Kişi'nin kendisi tarafından alenileştirilmiş Kişisel Veriler'in işlenmesine ilişkin veri sorumlusu olarak Teleses'in İlgili Kişi'yi aydınlatma

yükümlülüğü bulunmadığından ayrıca bir aydınlatma yapılmaz. Ancak İlgili Kişi'nin Kişisel Veriler'ini alenileştirme amacı ile Kişisel Veri İşleme amacı uyumlu olmalıdır. Bu nedenle aydınlatma yapılmasına ilişkin istisnaya tabi olunup olunmadığı hususunda tereddüt yaşanması halinde Kişisel Veri İşleme Sürecine başlamadan önce Komite'ye veya Yasal Uyum Uzmanı'na danışılır.

5.3. Kişisel Verilerin İşlenme Şartları (Veri İşlemenin Hukuki Sebepleri)

Kişisel Veriler ancak veya (i) aşağıdaki İşleme sebeplerinden birinin varlığı halinde veya bu hallerden birisi yoksa (ii) İlgili Kişi'nin "açık rızası" alınarak işlenebilir:

- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin işlenmesinin zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili Kişi'nin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili Kişi'nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması,

Yukarıda yer alan işleme şartlarından herhangi birinin mevcut olmaması halinde Kişisel Veriler işlenemez, bu işleme şartlarından bir veya birkaçı başta mevcut olmasına rağmen sonradan ortadan kalkarsa ilgili Kişisel Veri işleme sürecine son verilir.

Kişisel Veri işleme sürecinin hukuki sebebinin tespitinde tereddüt yaşanması halinde Komite'ye veya Yasal Uyum Uzmanı'na danışılır.

Özel Nitelikli Kişisel Veriler'in işlenme şartlarına ilişkin olarak ise, Teleses Özel Nitelikli Kişisel Veri İşleme Politikası'nda yer alan kurallar uygulanır.

5.4. Kişisel Verilerin Aktarımı

Kişisel Veriler'in aktarımı, Teleses veya Veri İşleyenler tarafından Teleses adına işlenen Kişisel Veriler'in, Teleses dışındaki yurt içiveya yurt dışındaki gerçek veya tüzel kişilere aktarımı anlamına geklir.

Teleses'in bağlı olduğu şirketlere ve grup şirketlerine Kişisel Veri aktarımının da Kişisel Veri aktarımı sayıldığı ve Kişisel Veriler'in aktarımına ilişkin kurallara tabi olduğu göz önünde bulundurulur. Teleses içindeki departmanlar arası Kişisel Veri aktarımı veya paylaşımı ise Kişisel Veriler'in aktarımı sayılmadığından Kişisel Veriler'in aktarılmasına ilişkin kurallara tabi değildir.

Teleses, Kanun'un 5/2. ve 6/3. maddelerinde yer alan şartların sağlanması halinde, Kurul tarafından öngörülen yeterli önlemleri alarak Kişisel Veriler'i ve Özel Nitelikli Kişisel Veriler'i İlgili Kişi'nin açık rızası olmaksızın aktarabilir.

Kişisel Veriler her zaman gizlilik içinde işlenir ve verilerin paylaşılmasına yazılı ya da elektronik olarak rıza gösterilmediği veya Kanun'un 5/2. ve 6/3. maddeleri altında yer alan sebepler mevcut olmadığı ya da yasal olarak zorunluluk bulunmadığı sürece Teleses adına hareket etmeyen üçüncü taraflar ile paylaşılmaz.

5.4.1. Kişisel Verilerin Aktarım Şartları

Kişisel Veriler, ancak veya (i) aşağıdaki İşleme sebeplerinden birinin varlığı halinde yahut bu sebepler bulunmadığı takdirde (ii) İlgili Kişi'nin "açık rızasının" alınmış olması koşuluyla aktarılabilir:

- Kanunlarda açıkça Kişisel Veriler'in aktarılabileceğinin öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için Kişisel Veriler'in aktarımının zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin aktarılmasının gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için Kişisel Veriler'in aktarılmasının zorunlu olması,
- İlgili Kişi'nin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için Kişisel Veriler'in aktarılmasının zorunlu olması,
- İlgili Kişi'nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri aktarımının zorunlu olması,

Kişisel Veriler'in yurt dışındaki üçüncü kişilere aktarımı ise ayrıca düzenlenmiştir. Buna göre Kişisel Veriler;

a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi.

b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı.

c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı.

ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi.

Kişisel veriler arızi olmak kaydıyla sadece aşağıdaki hallerden birinin varlığı halinde yurt dışına kişisel veri aktarabilir:

a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.

b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.

ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.İlgili Kişi'nin açık rızası aranmaksızın yurt dışına aktarılabilir. Yeterli korumaya sahip ülkelere yapılacak aktarımlar için bu ülkenin Kurul tarafından ilan edilen (eğer ilan edilmişse) "yeterli korumaya sahip ülkeler" arasında yer alıp almadığı kontrol edilir.

Özel Nitelikli Kişisel Veriler'in aktarımına ilişkin olarak ise Teleses Özel Nitelikli Kişisel Veri İşleme Politikası'nda yer alan kurallar uygulanır.

5.5. Envanter'e ve VERBİS'e ilişkin Yükümlülükler

Teleses'in Kişisel Veri işleme süreçlerine ilişkin bilgilere Envanter'de yer verilir. Envanter güncel tutulur. Teleses'in mevcut kişisel veri işleme süreçlerinde bir değişiklik olması halinde Envanter'de ilgili Kişisel Veri işleme süreci uygun şekilde güncellenir. Teleses'in yeni bir Kişisel Veri işleme sürecine başlayacak olması halinde ise ilgili Kişisel Veri işleme süreci Envanter'e uygun şekilde işlenir. Bu değişiklik, Birim Yöneticisi, Veri İşleyen veya Çalışanlar'ın bildirimi üzerine KVK Komite Sekreteri tarafından yapılır. KVK Komite Sekreteri, bu değişikliğe ilişkin olarak ihtiyaç duyması halinde Komite'ye veya Yasal Uyum Uzmanı'na danışabilir.

Envanter'de yapılacak olası bir değişikliğin Teleses'in VERBİS'e beyan etmiş olduğu Kişisel Veri işleme süreçlerine ilişkin bilgilerde değişiklik yapılmasını gerektirip gerektirmediği ilgili Kişisel Veri İşleme Sürecini yürüten Birim Yöneticisi ve KVK Komite Sekreteri tarafından kontrol edilir. VERBİS'e beyan edilen bilgilerde güncelleme yapılması gerektiği sonucuna varılması halinde değişiklik, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde KVK Komite Sekreteri tarafından İrtibat Kişisi aracılığıyla VERBİS'e işlenir. KVK Komite Sekreteri, bu

değişikliğe ilişkin olarak ihtiyaç duyması halinde Komite'ye veya Yasal Uyum Uzmanı'na danışabilir.

5.6. Veri Güvenliği'ne ilişkin Yükümlülükler

Teleses, Kişisel Veriler'i işlerken:

- kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve
- kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbirleri alır.

Bu tedbirler aşağıdaki gibidir:

5.6.1. Kişisel Veriler'in Hukuka Uygun İşlenmesini Sağlamak için Alınan Teknik Tedbirler

- 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 kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin farklı bir ortamda saklanması, kullanılmadıkları zamanlarda kilit altında tutulması, giriş-çıkış kayıtlarının tutulması gibi ek tedbirler alınmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bulutta depolanan kişisel veriler kriptografik yöntemlerle şifrelenmekte ve her bir bulut çözümü için ayrı ayrı şifreleme yapılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs ve anti-spam sistemleri kullanılmaktadır.
- Yazılım ve donanımların yama yönetimi ve güncellemeleri düzenli olarak kontrol edilmektedir.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- 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.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

5.6.2. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan İdari Tedbirler

Teleses tarafından kişisel verilerin hukuka uygun işlenmesini sağlamak için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Envanter hazırlanmış ve periyodik olarak gözden geçirilmektedir.
- Envanter çerçevesinde hukuki yükümlülüklerin yerine getirilmesi için çalışmalar yapılmış, Şirket belgeleri KVK Mevzuatı açısından incelenerek bu belgeler üzerinde gerekli değişiklikler yapılmış ve eksik olan belgeler hazırlanmıştır.
- VERBİS kayıt yükümlülüğü tamamlanmış ve periyodik olarak gözden geçirilmektedir.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Gizlilik taahhütnameleri yapılmaktadır.
- Çalışanlar için Kanun ve bilgi güvenliği kapsamında farkındalık çalışmaları ve farkındalık eğitimleri düzenlenmektedir.
- Teleses ile Çalışanlar arasındaki hukuki ilişkiyi yöneten sözleşme ve belgelere, kişisel verileri işlememe, ifşa etmeme ve kullanmama yükümlülüğü getiren kayıtlar konulmakta ve denetimler yürütülerek Kanun'dan doğan yükümlülükler yerine getirilmektedir. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için Yetki Matrisi oluşturulmuştur ve düzenli olarak gözden geçirilmektedir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler kişisel 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 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.
- Veri İşleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri İşleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

5.6.3. Kişisel Verilerin Aktarılmasında Uyulacak Teknik ve İdari Tedbirler

Teleses, Kişisel Veriler'in aktarılmasına ilişkin gerekli teknik ve idari tedbirleri alır.

5.6.3.1. Kişisel Verilerin Aktarılmasında Alınan Teknik Tedbirler

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla Kişisel Veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

5.6.3.2. Kişisel Verilerin Aktarılmasında Alınan İdari Tedbirler

- Kişisel verilerin aktarılacağı Alıcı Grubu ile standart kişisel veri işleme sözleşmesi imzalanır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Veri İşleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri İşleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

5.6.4. Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik ve İdari Tedbirler

Teleses, kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin paylaşılması veya kişisel verilere başka şekillerdeki tüm hukuka aykırı erişimi önlemek için uygulama gerekliliği ve maliyetine göre gerekli teknik ve idari tedbirleri alır.

5.6.4.1. Kişisel Veriler'in Hukuka Aykırı Erişimini Engellemek için Alınan Teknik Tedbirler

Teleses tarafından Kişisel Veriler'in hukuka aykırı erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Kişisel Veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel Veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin farklı bir ortamda saklanması, kullanılmadıkları zamanlarda kilit altında tutulması, giriş-çıkış kayıtlarının tutulması gibi ek tedbirler alınmaktadır.
- Kişisel Veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.Erişim logları düzenli olarak ve log kayıtlarına kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Erişim yetkileri sınırlandırılmıştır ve yetkiler periyodik olarak gözden geçirilmektedir. Alınan teknik önlemler periyodik olarak iç denetim tetkiklerle kontrol edilerek ilgilisine raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek düzeltici faaliyet çerçevesinde gerekli çözüm üretilmektedir.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Bulutta depolanan kişisel veriler kriptografik yöntemlerle şifrelenmekte ve bu Kişisel Veriler'in güvenliği sağlanmaktadır.
- Şifreleme yapılmaktadır.

- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- Güncel anti-virüs ve anti-spam sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kötücül yazılım koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.
- Teknik konularda alanında eğitim görmüş ya da yetişmiş personel istihdam edilmektedir.
- Kişisel Veriler'in toplandığı uygulamalardaki güvenlik açıklarını saptamak için düzenli olarak güvenlik taramalarından geçirilmektedir. Tespit edilen açıkların kapatılması sağlanmaktadır.
- Sızma testi uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

5.6.4.2. Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan İdari Tedbirler

Teleses tarafından Kişisel Veriler'in hukuka aykırı erişimini engellemek için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar için Kanun ve bilgi güvenliği kapsamında farkındalık çalışmaları ve farkındalık eğitimleri düzenlenmektedir.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- İş birimi ve süreç bazında yetki matrisleri hazırlanmış ve yetkilendirmeler yetki matrisine göre yapılmıştır. Verilen yetkiler düzenli olarak kontrol edilerek yetki matrisinin güncel tutulması konusunda gerekli hassasiyet gösterilmektedir.
- Çalışanlar, öğrendikleri Kişisel Veriler'i Kanun hükümlerine aykırı olarak başkasına açıklayamayacakları ve işleme amacı dışında kullanamayacakları ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Teleses tarafından Kişisel Veriler'in hukuka uygun olarak aktarıldığı Alıcı Grubu ile imzaladığı sözleşmelere Kanun'a uyumluluk için gerekli tedbirlerin alındığına ve Teleses'in belirlediği politikaların uygulandığına dair denetim uygulanacağına ilişkin hükümler eklenmektedir. Veri İşleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri İşleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.

5.6.5. Kişisel Verilerin Güvenli Ortamlarda Saklanması

Teleses, Kişisel Veriler'in güvenli ortamlarda saklanması ve veri bütünlüğünün bozulmaması, yetkisiz erişimlerin engellenmesi, hukuka aykırı amaçlarla yok edilmesini ve kaybolmasını önlemek için uygulama gerekliliği ve maliyetine göre teknik ve idari tedbirler almaktadır.

5.6.5.1. Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan Teknik Tedbirler

Teleses tarafından Kişisel Veriler'in güvenli ortamlarda saklanması için alınan başlıca teknik tedbirler aşağıdaki gibidir:

- Kişisel Veriler'in güvenli ortamlarda saklanması için teknolojik gelişmelere uygun sistemler kullanılmaktadır.
- Kişisel Veri'nin saklandığı alanlara göre fiziksel ya da yazılımsal güvenlik sistemleri kurulmakta, bilişim altyapısı üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri yapılmakta, yapılan test sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar düzeltici faaliyet kapsamında giderilmektedir. Alınan teknik ve idari tedbirlerin uygulandığı periyodik iç tetkiklerle kontrol edilir ve raporlanır.
- Kişisel Veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin farklı bir ortamda saklanması, kullanılmadıkları zamanlarda kilit altında tutulması, giriş-çıkış kayıtlarının tutulması gibi ek tedbirler alınmaktadır.
- Kişisel Veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Teknik konularda alanında eğitim görmüş ya da yetişmiş personel istihdam edilmektedir.
- Kişisel Veriler'in kontrolünün kaybedilmesi ya da bozulması riskine karşı hukuka uygun bir biçimde yedekleme sistemi kullanılmaktadır.
- Kişisel Veriler'in tutulduğu ortamlara yetki matrisine göre erişim verilerek ve veriye erişim kısıtlanarak yalnızca yetkili kişilerin bu verilere erişmesine izin verilmekte, Kişisel Veriler'in bulunduğu veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri ilgililere anlık olarak iletilmektedir.
- Kişisel Veriler veri kaybı önleme yazılımları ile korunmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Kişisel Veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan Kişisel Veriler'in güvenliği sağlanmaktadır.
- Erişim logları düzenli olarak ve kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Güncel anti-virüs ve anti-spam sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Sızma testi uygulanmaktadır.

5.6.5.2. Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan İdari Tedbirler

Teleses tarafından Kişisel Veriler'in güvenli ortamlarda saklanması için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar için Kanun ve Bilgi Güvenliği kapsamında farkındalık çalışmaları ve farkındalık eğitimleri düzenlenmektedir.
- Teleses tarafından Kişisel Veriler'in hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere Kanun'a uyumluluk için gerekli tedbirlerin alındığına ve Teleses'in belirlediği

politikaların uygulandığına dair denetim yapılacağı eklenmektedir. Veri İşleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

- Mevcut risk ve tehditler belirlenmiştir.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Kişisel Veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel Veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel Veri güvenliğinin takibi yapılmaktadır.

5.6.6. Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi

Teleses, Kanun'un 12. maddesine uygun olarak periyodik iç tetkikler gerçekleştirmekte ve raporlamaktadır. İç tetkik ile tespit edilen uygunsuzluklar ve riskler düzeltici faaliyet kapsamında değerlendirilerek önleyici faaliyetler uygulanmaktadır.

Veri İşleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

6. KİŞİSEL VERİ İHLALİ HALİNDE ALINACAK TEDBİRLER

Teleses tarafından, Kanun'un 12. maddesine uygun olarak işlenen Kişisel Veriler'in kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, "Teleses Kişisel Veri İhlal Tespit ve Müdahale Prosedürü"nde yer alan kurallar ve talimatlar uygulanır.

7. TELESES'E YAPILACAK İLGİLİ KİŞİ BAŞVURULARI

İlgili Kişiler, Teleses'e başvurarak Kanun'un 11. maddesinde sayılan aşağıdaki haklarını ileri sürebilir:

a) Kişisel Veri işlenip işlenmediğini öğrenme,

b) Kişisel Veriler'i işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel Veriler'in işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında Kişisel Veriler'in aktarıldığı üçüncü kişileri bilme,

d) Kişisel Veriler'in eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) Kişisel Veriler'in silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, Kişisel Veriler'in aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen Kişisel Veriler'in münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel Veriler'in kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

İlgili Kişi başvurularının yöntemi, başvuruların hangi kanallardan kabul edileceği, başvurunun Kanun'a uygun olup olmadığının denetlenmesinde esas alınacak kriterler, başvurulara cevap verme usulü ve süresi, başvurunun sonuçlandırılması, başvurunun reddi halinde İlgili Kişi'nin Kurul'a şikâyette bulunma hakkına ilişkin detay ve kurallar "Teleses İlgili Kişi Başvuru ve Şikâyet Prosedürü" adlı dokümanda yer almaktadır.

Olası bir İlgili Kişi başvurusu veya Kurul'a yapılacak şikayetlerde Teleses İlgili Kişi Başvuru ve Şikâyet Prosedürü'nde yer alan kurallar uygulanır.

8. KİŞİSEL VERİLERİN SAKLAMA SÜRESİ VE İMHASI

Kanun'unun 7. maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5. maddesi uyarınca Teleses Kişisel Veri Saklama ve İmha Politikası oluşturulmuştur.

Teleses'in her bir Kişisel Veri işleme süreci ile ilgili olarak:

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm Kişisel Veriler'le ilgili Kişisel Veri bazında saklama süreleri Teleses Envanter'inde,
- Veri kategorileri bazında saklama süreleri VERBİS'e girilen kayıtlarda,
- Süreç bazında saklama süreleri ise Teleses Kişisel Veri Saklama ve İmha Politikası'nda

yer alır.

Kişisel Veriler ve Özel Nitelikli Kişisel Veriler KVK Mevzuatı ve ilgili diğer mevzuatta öngörülen sürelerle sınırlı olarak saklanır. Kişisel Veriler'in ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre belirtilmemişse Kişisel Veriler aşağıdaki kriterler göz önüne alınarak belirlenen süre boyunca saklanır ve bu sürenin ardından imha edilir:

- İlgili veri kategorisinin işlenme amacı kapsamında Veri Sorumlusu'nun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,
- İlgili veri kategorisinde yer alan Kişisel Veri'nin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
- İlgili veri kategorisinin işlenme amacına bağlı olarak Veri Sorumlusu'nun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
- İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
- Veri Sorumlusu'nun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan Kişisel Veriler'i saklamak zorunda olduğu süre,
- Veri Sorumlusu tarafından, ilgili veri kategorisinde yer alan Kişisel Veri'ye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi

Kişisel Veriler'in işlenme amacı sona ermiş; ilgili mevzuat ve Teleses tarafından belirlenen saklama sürelerinin de sonuna gelinmişse; Kişisel Veriler, yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi veya Kişisel Veri'ye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis

edilmesi amacıyla saklanmaya devam edilir Bu süreler, ilgili hakkın ileri sürülebilmesine yönelik zaman aşımı süreleri ile zaman aşımı sürelerinin geçmesine rağmen daha önce aynı konularda Teleses'e yöneltilen taleplerdeki örnekler esas alınarak saklama süreleri belirlenir. Bu durumda, saklanan Kişisel Veriler'e herhangi bir başka amaçla erişilmez ve ancak ilgili hukuki uyuşmazlıkta kullanılması gerektiği zaman ilgili kişisel verilere erişim sağlanır. Burada da bahsi geçen süre sona erdikten sonra Kişisel Veriler silinir, yok edilir veya anonim hale getirilir. Kişisel Veriler imha edilirken Teleses Kişisel Verileri Saklama ve İmha Politikası'nda yer alan kural ve talimatlara uygun hareket edilir.

9. KİŞİSEL VERİ KATEGORİLERİ

Kişisel Veri Kategorisi	Açıklama
Kimlik Bilgisi	İlgili Kişi'nin kimliğine dair bilgilerin bulunduğu verilerdir; ad-soyadı, T.C. kimlik numarası, uyruk bilgisi, anne adı-baba adı, doğum yeri, doğum tarihi, cinsiyet gibi bilgileri içeren ehliyet, nüfus cüzdanı ve pasaport gibi belgeler ile vergi numarası, SGK numarası, imza bilgisi vb. bilgiler
İletişim Bilgisi	İlgili Kişi hakkındaki telefon numarası, adres, e-posta adresi, faks numarası gibi iletişim bilgileri
Fiziksel Mekân Güvenlik Bilgisi	İlgili Kişi hakkındaki fiziksel mekâna girişte, fiziksel mekânın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler; kamera kayıtları ve güvenlik noktasında alınan kayıtlar vb.
Finansal Bilgi	İlgili Kişi hakkındaki her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler ile banka hesap numarası, IBAN numarası, kredi kartı bilgisi, finansal profil, malvarlığı verisi, gelir bilgisi gibi veriler
Görsel/İşitsel Bilgi	İlgili Kişi hakkındaki fotoğraf ve kamera kayıtları (Fiziksel Mekân Güvenlik Bilgisi kapsamında giren kayıtlar hariç), ses kayıtları ile kişisel veri içeren belgelerin kopyası niteliğindeki belgelerde yer alan veriler
Özlük Bilgisi	İlgili Kişi hakkındaki özlük haklarının oluşmasına temel olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veri
Özel Nitelikli Kişisel Veri	İlgili Kişi'nin 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

Mesleki Deneyim Bilgisi	İlgili Kişi hakkındaki diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, transkript bilgileri gibi veriler
Müşteri İşlem Bilgisi	İlgili Kişi hakkındaki çağrı merkezi kayıtları, fatura, senet, çek bilgileri, gişe dekontlarındaki bilgiler, sipariş bilgisi, talep bilgisi gibi veriler
İşlem Güvenliği Bilgisi	İlgili Kişi hakkındaki IP adresi bilgileri, internet sitesi giriş çıkış bilgileri, şifre ve parola bilgileri gibi veriler
Hukuki İşlem	İlgili Kişi hakkındaki adli makamlarla yazışmalardaki bilgiler, dava dosyasındaki bilgiler, icra dosyasındaki bilgiler gibi veriler
Pazarlama	İlgili Kişi hakkındaki alışveriş geçmişi bilgileri, anket, çerez kayıtları, kampanya çalışmasıyla elde edilen bilgiler gibi veriler

10. İLGİLİ KİŞİ KATEGORİLERİ

- Çalışan Adayı
- Referans Kişisi
- Stajyer
- Çalışan
- Topluluk Şirketi Çalışanı
- (Çalışan) Aile Üyeleri
- Potansiyel Ürün veya Hizmet Alıcısı (Potansiyel Müşteri)
- Ürün veya Hizmet Alan Kişi (Müşteri)
- Gerçek Kişi Tedarikçi
- Tedarikçi Çalışanı
- Tedarikçi Yetkilisi
- İş Ortağı Çalışanı veya Yetkilisi
- Veli / Vasi / Temsilci
- Ziyaretçi (Web Sitesi Ziyaretçisi)
- Ziyaretçi (Mobil Uygulama Ziyaretçisi)
- Ziyaretçi (Merkez Ziyaretçisi)
- Ziyaretçi (Fabrika Ziyaretçisi)
- Ziyaretçi (Depo Ziyaretçisi)
- Hukuki İşlem İlgilisi
- Hissedar/Ortak

11. 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 İşleme ve Koruma Politikası yayımlandı.
v.2		