Kişisel Veri Politikası ve Uygulama Prosedürleri

Tulipack Ambalaj A.Ş	**Kişisel Verilerin Korunması ve Yönetimine İlişkin Yönetmelik**	Rev. V2
Doküman No:		Tarih: 19.01.2021
İlgili Birimler	Tulipack Ambalaj A.Ş İnsan Kaynakları Departmanı Tulipack Ambalaj A.Ş Mali İşler Departmanı	
Revizyonlar	İlk Yayın	Tarih: 16.03.2020

Tulipack Ambalaj A.Ş ("**Şirket**" veya "**Tulipack**"), Kişisel Veri Politikası ve Uygulama Prosedürleri ("**Politika**") dokümanı ile kişisel verilerin işlenmesi, korunması, saklanması ve imha edilmesi konularında benimsenecek ilkeler ile uygulanacak prosedürleri düzenlemektedir.

Şirket buna uygun olarak, mevzuata uyum konusunda gerekli yapıyı, prosedür ve süreçleri oluşturacak; çalışanlarında ve iş ortaklarında farkındalığın yaratılması için gerekli mekanizmaları hayata geçirecektir.

Şirket internet sitesi üzerinden gizlilik politikası, şartlar ve koşullar, kişisel veri işlenmesi ve korunması aydınlatma metni, başvuru talep formu ve işbu Politika metnine ulaşılabilmektedir.

1. Amaç

Tulipack tarafından gerçekleştirilmekte olan veri toplama, kişisel verinin korunması, saklanması ve imhası faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Tulipack, Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, tedarikçiler, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**") ve diğer ilgili mevzuata uygun olarak işlenmesini, saklanmasını, imha edilmesini, paylaşılmasını ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını hedeflemiştir.

Kişisel verilerin toplanması, saklanması ve imhasına ilişkin iş ve işlemler, Tulipack tarafından bu doğrultuda hazırlanmış olan Politika'ya, Kişisel Verileri Koruma Kurulu uygulama ilkeleri, kararları ve Kanun'a uygun olarak, sınırlı ve ölçülü bir biçimde gerçekleştirilir.

2. Kapsam

Tulipack çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Tulipack'ın sahip olduğu ya da Tulipack tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

3. Tanımlar

Politika'da yer alan tanımlanmış terimler, aşağıda yer verilen tanımlandıkları anlamlarda kullanılmaktadır.

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

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.

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: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

Kişisel veri sahibi: Kişisel verisi işlenen gerçek kişi.

Kişisel verinin işlenmesi: 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.

Kurul: Kişisel Verileri Koruma Kurulu.

Kurum: Kişisel Verileri Koruma Kurumu.

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 veriler.

Periyodik imha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim

hale getirme işlemi.

Politika: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları işbu Politika.

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili.

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi.

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

Politika'da yer almayan tanımlar için Kanun'daki tanımlar geçerlidir.

4. Veri Sahibinin Haklarının Gözetilmesi

Tulipack, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gerekli bilgilendirmenin yapılması için Kanuna uygun olarak gerekli kanalları, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

Kişisel veri sahipleri, Kanun'un 11'inci maddesi gereği sahip olduğu haklarına ilişkin taleplerini yazılı olarak Şirket'e iletmeleri durumunda Şirket, talebin niteliğine göre talebi en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırır. İşlemin ayrıca bir maliyet gerektirmesi halinde, Şirket tarafından Kurulca belirlenen tarifedeki ücret alınacaktır. Kişisel veri sahipleri haklarını kullanırken taleplerini yazılı veya Kanun'un belirlediği yöntemler ile iletmelidirler. Kurul'un, henüz başkaca bir yöntem belirlememiş olması sebebiyle, bu aşamada veri sahiplerinin taleplerini yazılı olarak iletmeleri aranmaktadır.

5. Sorumluluk ve Görev Dağılımları

Şirket'in tüm birimleri ve çalışanları, Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi başta olmak üzere, kişisel verilerin hukuka uygun olarak işlenmesi, saklanması, imha edilmesi, paylaşılmasının sağlanması amaçlarıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir. Bell Grubu şirketleri ve Şirket, bu kapsamda, kişisel veri işleme süreçlerine ilişkin olarak veri envanterini ilgili birim ve çalışanlarının katılımıyla oluşturmuştur.

6. Saklamaya ve İmhaya İlişkin Açıklamalar

Şirket tarafından; çalışanlar, çalışan adayları, ziyaretçiler, tedarikçiler, hizmet sağlayıcıları ve ilişkide bulunulan diğer üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir. Bu

kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar ve her halükarda kişisel veri envanterinde, VERBİS kayıtlarında bildirilen kapsamdaki süreler kadar saklanır.

7. Saklamayı Gerektiren Hukuki Sebepler

Şirket faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatında, kişisel veri envanterinde, VERBİS kayıtlarında bildirilen kapsamda veya, uygulanabilir olduğu ölçüde bu Politika'da belirtilen süre kadar saklanır.

Bu kapsamda kişisel veriler:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik
- 213 sayılı Vergi Usul Kanunu

Başta olmak üzere, Şirket ve faaliyetleri hakkında uygulanan yasalar ve bu yasalar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde zorunlu saklama ve ispat süreleri varsa, bu süreler göz önünde bulundurularak saklanır. Kişisel veri envanteri doğrultusunda belirlenen süreçlere dair saklama süreleri ayrıca düzenlenmiştir.

8. Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- İnsan kaynakları süreçlerini yürütmek,
- Kurumsal iletişimi sağlamak,
- Şirket güvenliğini sağlamak,
- İş sağlığı ve güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü kapsamında delil niteliğindeki belgeleri ilgili kurum, kuruluş ve mahkeme ile icra dairelerine sağlayabilmek,
- Seçme-yerleştirme hizmetlerinin sunulması ve bu hizmetler için gerekli dokümantasyonun oluşturmak.

9. İmhayı Gerektiren Sebepler

Kişisel veriler:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; ilgili kişinin Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması hallerinde, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

10. Teknik ve İdari Tedbirler

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun ilgili maddeleri çerçevesinde Şirket tarafından aşağıda 11, 12, 13 ve 14. maddelerde yer verilen tedbirler alınır.

11. Teknik Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- 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.
- Şirket'in 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 ağını 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.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

- Kurum, 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 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.
- Şirket internet sayfasına erişimde güvenli protokol (*HTTPS*) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- 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 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 verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

12. İdari Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Bu alandaki eğitimler her yıl güncellenmektedir.
- Kanun'a ve kişisel verilerin korunması mevzuatına uyum için uzman danışmanlık hizmeti alınmaktadır.
- Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Her bir hizmet için iş akışı süreçleri tanımlanmış, çalışanlara aktarılmış; herkesin istediği zaman ulaşabilmesi için ortak arşiv alanına eklenmiştir.
- Müşterilerle yapılan sözleşme ve işlemlerde idari tedbir düzenlemelerine yer verilmektedir.

- Tedarikçilerle yapılan sözleşme ve işlemlerde idari tedbir düzenlemelerine yer verilmektedir.

13. İmha Teknikleri

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun tekniklerle imha edilir.

14. 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.

15. Periyodik İmha Süresi

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11.maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir.

16. Kişisel Verilerin Aktarılması

Şirket, mevzuat uyarınca kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak ve açık rıza gerektiren hallerde açık rıza temin etmek suretiyle veri sahibinin kişisel verilerini üçüncü kişilere aktarabilmektedir. Şirket, Kanun'un 8. maddesinde öngörülen düzenlemelere uygun hareket etmektedir. Bu madde uyarınca kural olarak kişisel veriler veri sahibinin açık rızası olmaksızın üçüncü kişilere aktarılamaz. Ancak Kanun'un 5. maddesinin ikinci fıkrasında belirtilen haller mevcut olduğunda, kişisel veriler veri sahibinin açık rızası olmaksızın yurt içinde üçüncü kişilere aktarılabilir.

17. Yurtdışına Aktarım

Kanun'un 9. Maddesi uyarınca kişisel veriler kural olarak, veri sahibinin açık rızası olmaksızın yurtdışına aktarılamaz. Ancak Kanun'un 5. maddesinin ikinci fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verilerin aktarılacağı yabancı ülkede;

- Yeterli korumanın bulunması,
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un

izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurtdışına aktarılabilir.

Şirket, hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin açık rızası var ise veya kişisel veri sahibinin açık rızası yok ise aşağıdaki hallerden birinin varlığı durumunda kişisel verileri yeterli korumaya sahip veya yeterli korumayı taahhüt eden veri sorumlusunun bulunduğu yabancı ülkelere aktarabilmektedir:

- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Şirket'in hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Kişisel veriler, kişisel veri sahibi tarafından alenileştirilmiş ise,
- Kişisel veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirket'in meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

Şirket, ana ilke olarak kişisel verilerin yurtdışına aktarımının gerekli olduğu hallerde, aktarımın sınırlılık ve ölçülülük prensibine uygun olması ve her halükarda uygulanabilir olduğu ölçüde, açık rıza temin edilmesi prensibini benimsemiştir. Şirket internet sitesinde yer alan aydınlatma metni ile mevzuatta öngörülen gerekli bilgilendirmenin yapılması sonrasında ayrı bir doküman ile açık rıza alınmasını sağlamaktadır.

18. Özel Nitelikli Kişisel Veriler

Şirket, mevzuatın öngördüğü şekilde özel nitelikli kişisel verileri sınırlılık ve ölçülülük ilkeleri ışığında işlemektedir. Bu doğrultuda bilumum idari ve teknik tedbirler alınmıştır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise:
a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

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

a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

Özel nitelikli kişisel veriler aktarılacaksa:
a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmıştır.

19. Aktarılan Üçüncü Kişiler

Şirket, Kanun'un 8 ve 9. maddelerine uygun olarak veri sahiplerinin kişisel verilerini aşağıda kategorik olarak sıralanan üçüncü kişilere aktarabilir:

- Bell Grubu şirketleri başta olmak üzere kişisel verilerin yasal olarak korunduğu ülkelerdeki şirketlere,
- İş ortaklarına,
- Banka ve sigorta şirketlerine,
- Hukuken yetkili kamu kurum ve kuruluşlarına

20. Güncelleme Periyodu

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

21. Yürürlük

Politika, Şirket internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.