

[AÇIK]

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

1.4.2019

KVKK.POL.02/S-01/

TURKTRUST

[AÇIK]

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

İÇİNDEKİLER

1. AMAÇ.....	2
2. KAPSAM.....	2
3. TANIMLAR.....	3
4. REFERANSLAR	4
5. ÖZEL NİTELİKLİ KİŞİSEL VERİ	4
5.1 ÖZEL NİTELİKLİ KİŞİSEL VERİ İŞLENMESİNE İLİŞKİN GENEL İLKELER	4
5.2 ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI	5
5.3 ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME AMAÇLARI	5
5.4 ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI	5
5.5 VERİ İŞLEME ŞARTLARININ ORTADAN KALKMASI	6
5.6 ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNDE GÜVENLİK ÖNLEMLERİ	7
6. POLİTİKA YÜRÜRLÜK VE GÜNCELLEMELER	8

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bu politikanın amacı, 6698 sayılı Kişisel Verilerin Korunması Kanununa uygun olarak özel nitelikli kişisel verilerin işlenmesi ve korunmasına yönelik sistemler konusunda açıklamalarda bulunmaktır. Bu kapsamda aktif ve potansiyel müşterilerimiz, çalışanlarımız, ziyaretçilerimiz ve şirketimiz ile ilişki içinde bulunan diğer gerçek ve tüzel kişiler başta olmak üzere özel nitelikli kişisel verileri Şirketimiz tarafından işlenen ilgili kişileri bilgilendirmektir.

Şirketimiz tarafından özel nitelikli kişisel verilerin işlenmesi ve korunması faaliyetlerinde mevzuata tam uyumun sağlanması ve ilgili kişilerin özel nitelikli kişisel verilerine dair tüm haklarının korunması hedeflenmektedir.

2. KAPSAM

İşbu Özel Nitelikli Kişisel Veri Güvenliği Politikası (Bundan sonra "Politika" olarak anılacaktır) TÜRKTRUST (Bundan sonra "Şirket" olarak anılacaktır) bünyesinde kişisel verileri işleyen herhangi bir sürece dâhil olan tüm departmanları, çalışanları ve üçüncü tarafları kapsamaktadır.

İşbu Politika; Şirket'in özel nitelikli kişisel verilerin güvenliğine yönelik kuralları tanımlayacak ve bu alandaki yönetimi sağlayacak tüm faaliyetleri kapsayacak olup, bunu sürdürmek adına her adımda uygulanacaktır.

İşbu Politika özel nitelikli kişisel veri olmayan veriler hakkında uygulanmayacaktır.

Konuyla alakalı yeni mevzuatın belirlenmesi veya ilgili mevzuatın güncellenmesi durumunda, Şirket politikasını ilgili mevzuata uyumlu olacak şekilde güncelleyerek mevzuat gerekliliklerine uyacaktır.

İşbu Politikanın Şirket tarafından uygulanmasında hukuki bir engel olduğuna kanaat getirdiği durumlarda, Şirket uygulayacağı adımları, gerek görmesi durumunda Hukuk Danışmanına ve Üst Yönetime danışarak, Politikayı yeniden belirleyebilecektir.

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

3. TANIMLAR

Kısaltma	Tanım
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.
İlgili Karar	“Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler” ile ilgili Kişisel Verileri Koruma Kurulu’nun 31.01.2018 tarihli, 2018/10 sayılı kararıdır.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu’dur.
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 ortama verilen addır.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir ve kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hallerini kapsar.
Kişisel verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi
Kişisel veri işleme envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçlarını, veri kategorisini, aktarılan alıcı grubunu ve veri konusunu kişi grubuyla ilişkilendirerek oluşturan ve detaylandıran envanterdir.
Kurul	Kişisel Verileri Koruma Kurulu’dur.

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

Kısaltma	Tanım
Özel Nitelikli Kişisel Veri	6698 sayılı Kişisel Verilerin Korunması Kanunu'nda belirtilen özel nitelikli kişisel veriler, işlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına neden olma riski taşıyan verilerdir.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir.

4. REFERANSLAR

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu,
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,
- Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı.

5. ÖZEL NİTELİKLİ KİŞİSEL VERİ

5.1 Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Kanunun 4.maddesinde kişisel verilerin işlenmesine ilişkin usul ve esaslar düzenlenmiştir.

Buna göre; Kanunda kişisel verilerin işlenmesinde sayılan genel (temel) ilkeler şunlardır:

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

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunur ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilir.

Kişisel veriler Şirket bünyesinde veri sahiplerinden alınan açık rıza aracılığıyla işlenmekte olup, bu veriler ancak işbu Politika'nın yukarıdaki ilkeler doğrultusunda belirtilen kontroller çerçevesinde işlem görmektedir. Şirket ile veri sahibi arasındaki ilişkinin türüne ve niteliğine, kullanılan iletişim kanallarına ve bahsi geçen amaç bilgisine bağlı olarak çeşitlenmekte ve farklılaşmaktadır. Bu veriler Kişisel Veri İşleme Envanteri içinde belirtilmiştir.

5.2 Özel Nitelikli Kişisel Verilerin İşlenme Şartları

- 1- Özel nitelikli kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.
- 2- Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verileri olan ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir.
- 3- Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

5.3 Özel Nitelikli Kişisel Verilerin İşlenme Amaçları

Kişisel veriler, Kişisel Veri İşleme Envanteri içinde belirtilen amaçlar kapsamında işlenebilmekte olup, bu amaçların ve ilgili yasal sürelerin öngördüğü müddetçe saklanabilmektedir.

5.4 Özel Nitelikli Kişisel Verilerin Aktarılması

Kişisel Verilerin Aktarılması

- Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz
- Kişisel veriler; Kanunun 5 inci maddesinin ikinci fıkrasında, yeterli önlemler alınmak kaydıyla, 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.
- Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

Kişisel Verilerin Yurt Dışına Aktarılması

- Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.
- Kişisel veriler, Kanunun 5 inci maddesinin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;
 - a) Yeterli korumanın bulunması,
 - b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.
- Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

Şirket, işbu Politikanın “Özel Nitelikli Kişisel Verilerin İşlenme Amaçları” bölümünde örneklendirilen amaçlar çerçevesinde ve Kişisel Verileri Koruma Kanununun 8 ve 9’uncu maddeleri uyarınca yurt içi ve yurt dışı veri aktarımı yapmaktadır ve kişisel veriler bu kapsamda kullanılan sunucu ve elektronik ortamlarda işlenerek saklanabilmektedir. Şirket tarafından hazırlanmış Kişisel Veri İşleme Envanterinde veri aktarımı gerçekleştiren taraflar ve veri aktarım amaçları detaylı bir şekilde belirtilmiştir. Yapılan bu aktarımların niteliği ve paylaşım yapılan taraflar, Veri sahibi ile Şirket arasındaki ilişki türüne ve niteliğine, aktarımın amacına ve ilgili yasal dayanağa bağlı olarak değişmekte olup, bu kapsamda Şirket tarafından Kişisel Verileri Saklama ve İmha Politikası içinde tanımlanmış olan tedbirler, uygulama esas usulleri ve bu çerçevede alınacak olan aksiyonlar geçerlidir.

5.5 Veri İşleme Şartlarının Ortadan Kalkması

Şirket, özel nitelikli kişisel veri işleme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu tüm çalışanları ile paylaşır.

Çalışanlar, veri işleme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez. Şirket, şartların ortadan kalktığı ortamları ilgili iş birimlerinin ya da İcra Kurulunun talebi üzerine işbu Politikaya uygun bir şekilde ortadan kaldırmakla yükümlüdür.

Şirket aşağıda örnek olarak listelenen ve “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*” içinde de belirtilen ilgili durumlarda özel nitelikli kişisel veri işleme şartlarının ortadan kalktığını kabul eder:

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

- a) Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- b) Kişisel verileri işlemenin hukuka ve dürüstlük kuralına aykırı olması,
- c) Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması.

Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.

Bu kapsamda Şirket tarafından “*Kişisel Veri Saklama ve İmha Politikası*” içinde tanımlı olan tedbirler, uygulama esas usulleri ve bu çerçevede alınacak olan aksiyonlar geçerlidir.

5.6 Özel Nitelikli Kişisel Verilerin İşlenmesinde Güvenlik Önlemleri

6698 sayılı Kişisel Verilerin Korunması Kanununun 6 ıncı maddesinin (4) numaralı fıkrasında, “*Özel nitelikli kişisel verilerin işlenmesinde ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır*” hükmü yer almaktadır.

Bu çerçevede, Kanunun 22 inci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler, Kişisel Verileri Koruma Kurulu’nun 07.03.2018 tarihli Resmi Gazetede yayımlanan, 31.01.2018 tarihli kararı uyarınca aşağıdaki şekilde belirlenmiştir:

- 1- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,
 - Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
 - Gizlilik sözleşmelerinin yapılması,
 - Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
 - Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
- 2- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması, Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;
 - Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
 - Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

- Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
 - Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - Verilere bir yazılım aracılığıyla erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- 3- 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;
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
 - Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- 4- Özel nitelikli kişisel verileri aktaracak ise;
- Verilerin e-posta yoluyla aktarılması gerekiyorsa, şifreli olarak kurumsal e-posta adresi ile veya kayıtlı elektronik posta (KEP) hesabı kullanılarak aktarılması,
 - Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtar farklı ortamda tutulması,
 - Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemi ile veri aktarımının gerçekleştirilmesi,
 - Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.
- 5- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmaktadır.

6. Politika Yürürlük ve Güncellemeler

İşbu Politika, Şirket Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girecektir. Politikada yapılacak değişiklikler ve bu değişikliklerin yürürlüğe konulması konusunda gereken çalışmalar Kalite Sistemleri Müdürlüğü, İcra Kurulu Üyeleri tarafından yapılacak ve Şirket Yönetim Kurulu onayından sonra yürürlüğe girecektir.

ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI

Ancak, mevzuat değişiklikleri, atıf yapılan bir teknik standarttaki değişme, Kişisel Verileri Koruma Kurulu'nun işlemleri ve/veya vereceği kararlar ile mahkeme kararları doğrultusunda Şirket bu Politikayı gözden geçirme ve gerekli durumlarda Politikayı güncelleme, değiştirme veya ortadan kaldırıp yeni bir Politika oluşturma hakkını saklı tutar.

Politika, olağan olarak yılda bir defa gözden geçirilir ve gerekirse güncellenir. Politikanın yürürlükten kaldırılmasına ilişkin olarak karar verme yetkisi Şirket Yönetim Kurulu'na aittir.

DEĞİŞİKLİK NOTLARI

01.04.2019	Kişisel Veri Saklama ve İmha Politikası yayımlanmıştır.
------------	---

* Daha eski tarihli bir değişiklik bulunmamaktadır.