TÜRK TELEKOM

BİLGİ GÜVENLİĞİ POLİTİKASI

Türk Telekom, Bilgi Güvenliği Yönetim Sistemi ile iş ihtiyaçları, kanunlar ve yasal düzenlemelere ilişkin beklentileri karşılamak için tespit edilen bilgi güvenliği gereksinimlerini değerlendirir ve adresler. Bilgi Güvenliği Yönetim Sistemi'nin işletilmesi ile bilgi güvenliği riskleri belirlenmekte, değerlendirilmekte ve kontrol edilmektedir. Türk Telekom Yönetimi, Bilgi Güvenliği Yönetim Sisteminin etkin şekilde işletilmesi için uygun görevlendirmeleri yapar ve gerekli desteği sağlar. Bu kapsamda, Türk Telekom çalışmalarına katkıda bulunan tüm tarafların benimsemesi gereken Bilgi Güvenliği gereksinimlerinin çerçevesini çizmek için Bilgi Güvenliği Politikaları oluşturulmuştur. Bilgi Güvenliği Politikaları, Türk Telekom çalışanlarını ve birlikte iş yapılan üçüncü tarafları kapsamaktadır.
Türk Telekom Yönetimi, Bilgi Güvenliği Yönetim Sistemi'nin etkin olarak çalıştığının kontrolü amacıyla yılda en az bir kez bağımsız gözden geçirmelerin gerçekleştirilmiş olmasını ve sonuçların raporlanmasını sağlar.

Türk Telekom Bilgi Güvenliği Politikası Yönetim Kurulu tarafından onaylanmıştır. Şirketin Bilgi Güvenliği komitesi yılda en az bir kez toplanarak Bilgi Güvenliği Yönetim Sistemi ile ilgili yürütülen tüm faaliyetlerin ve hazırlanan raporların değerlendirilmesi, bilgi güvenliği kaynaklarının atanması, ihtiyaçların bütçelendirilmesi ve bilgi güvenliği risk raporlarının değerlendirilmesi faaliyetlerini yürütür.

Ayrıca Kişisel Verilerin Korunması Kanunu kapsamında Türk Telekom bünyesinde tüm kişisel veri süreçlerinin kontrolünün sağlanması ve kanuni gereksinimlerinin yerine getirilebilmesi amacıyla Kişisel Veri Koruma Komitesi kurulmuştur.

Kişisel Verilerin Korunması ve Veri Sorumlusu

Kişisel veriler; 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 5809 Sayılı Elektronik Haberleşme Kanunu, Bilgi Teknolojileri ve İletişim Kurumu, Kişisel Verileri Koruma Kurumu düzenlemeleri ve sair mevzuat hükümleri çerçevesinde işlenebilecek olup, ilgili mevzuat gereğince Türk Telekom kişisel verilerin hukuka aykırı olarak işlenmesini önleme, hukuka aykırı olarak erişilmesini önleme ve muhafazasını sağlama amacıyla, uygun güvenlik düzeyini temin etmeye yönelik tüm teknik ve idari tedbirleri almaktadır.

Kişisel Verilerin İşlenmesine Dair İlgili Kişinin Hakları

KVKK 11. Maddesi uyarınca ilgili kişilerin Türk Telekom'a başvurarak;

a) Kişisel verinin işlenip işlenmediğini öğrenme,
b) Kişisel veriler işlenmişse buna ilişkin bilgi talep etme,
c) Kişisel verilerin işlenme amacı ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d) Kişisel veriler eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e) Kanun'un ilgili maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranması halinde zararın giderilmesini talep etme,

hakları bulunmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel veriler ile ilgili tüm soru ve talepler Türk Telekom Turgut Özal Bulvarı 06103 Aydınlıkevler / Ankara adresine yazılı olarak (Noter kanalı vb. yollarla) iletilebilir.

Bilgi Güvenliği Olay Yönetimi

Türk Telekom'da Bilgi Güvenliği Olay Yönetimi SOME (Siber Olaylara Müdahale Ekibi) tarafından Bilgi Güvenliği Olay Takip Prosedürü gereğince gerçekleştirilir. SOME, Bilgi güvenliği olaylarının takibini Olay Müdahale Formu üzerinden gerçekleştirir.

Veri ihlal olaylarının önüne geçmek ve tespitini sağlamak için gerekli teknolojiler kullanılarak tedbirler alınmaktadır. Şirketçe tespit edilen ihlal olaylarını Türk Telekom Bilgi Güvenliği Politika ve Prosedürleri gereğince değerlendirip gerektiği durumlarda Etik Kurul ve "Ulusal Siber Olaylara Müdahale Merkezi" (USOM) ile paylaşılmaktadır.

Politikalar ve Sistemlerin Denetimi

Bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesinin, işletilmesinin, güncelliğinin sağlanması ve gerekli yönetsel sorumlulukların belirlenmesi için Türk Telekom'un bilgi sistemleri yönetimine ilişkin 22 adet politika bulunmaktadır. Söz konusu politikalar yıllık olarak gözden geçirilmektedir.

Türk Telekom'un uluslararası akreditasyona sahip kuruluş Türk Standartları Enstitüsü (TSE) tarafından ISO/IEC 27001 sertifikasyon denetimleri yılda bir defa gerçekleştirilmektedir. Ayrıca, Türk Telekom yasalarla görevlendirilen Telekomünikasyon sektörü düzenleyici kuruluşu Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından denetlenmektedir. Şirket içinde de Bilgi Güvenliği Politika ve Süreçleri'nin ilgili birimler tarafından uygulanması Bilgi Güvenliği denetçileri ve İç denetim ekiplerince periyodik olarak denetlenmektedir.

Türk Telekom, yetkilendirilmiş olduğu hizmetlerin müşterilerine sunulabilmesi için gerekli olan verinin kullanımı için müşterilerinden gerekli izinleri alarak sadece bu verilere işlem yapmaktadır. Ayrıca Telekomünikasyon sektörünü ilgilendiren kapsamlarda Kanuni yükümlülükler gereği ihtiyaç duyulan veriler tutulmaktadır. Bu kapsamda tüm verilere erişimler "ihtiyaç duyulan kadar bil" ("Need to Know") prensibine göre yapılandırılmakta ve bu verilere erişime yalnızca görevi gereği ihtiyaç duyan kişiler yetkilidir. Şüpheli veya amacı dışında kullanımları tespit edebilmek amacıyla bu verilere erişim sürekli kayıt altına alınmakta ve denetlenmektedir.

Türk Telekom'da sistemler arası erişimler, sistemlere uzaktan erişimler, veri tabanlarına erişimler, kullanıcı tanımlama süreçleri, raporlama talepleri süreçleri talep yönetim sistemleri üzerinden tasarlanan güvenli ve kontrollü süreçler ile işletilmektedir. Sistemler üzerinde belirli periyotlarda ve projelerin canlıya alımlarından önce güvenlik testleri yapılarak tespit edilen güvenlik bulgularının ilgili ekiplerce giderilmesi sağlanmaktadır. Network katmanında planlanan katmanlı yapı ile uygulama katmanı, veri tabanı katmanı, web katmanları ayrıştırılarak güvenlik riskleri minimize edilmektedir. Network seviyesindeki güvenlik cihazları ile erişimlerin belirlenen kurallara göre kontrollü erişim sağlanması garanti altına alınmaktadır. Şebeke ve Bilgi Güvenliği Yönetmeliği kapsamında "Görevlerin ve ortamların ayrılması" maddesi uyarınca kritik sistemlerde yapılacak işlemlerin başlatılması ve onaylanması süreçleri ayrıştırılmıştır. Tüm sistemlerin erişim kontrolü kapsamında Türk Telekom Grubu Bilgi Güvenliği Politika ve Prosedürleri uyarınca en az yılda bir kez gözden geçirilmesi yapılmaktadır.

Son kullanıcıların hareketlerini gözlemleyerek kritik verilerin işlendiği ve geçtiği her türlü kanaldan kasten ya da yanlışlıkla dışarıya veri sızmasını önlemeye yönelik sistemler Türk Telekom şebekelerinde kullanılmaktadır. KVKK gereksinimlerini karşılamak ve gizli verilere yetkisiz erişimleri engellemek için veri tabanlarında kritik/kişisel/gizli verilerin anonimleştirmesi, maskelenmesi ve kullanıcı yetkilendirmeleri yapılmaktadır.

Ağırlıklı olarak teknoloji süreçlerini kapsayan ve her yılsonunda gerçekleştirilen risk değerlendirmelerine bağlı olarak oluşturulan bir yıllık denetim planı, Yönetim Kurulu bünyesinde oluşturulmuş olan Denetim Komitesi tarafından onaylanır ve denetim planının gerçekleştirilmesi için Türk Telekom İç Denetim Başkanlığı yetkilendirilir. Bu çerçevede gerçekleştirilen risk değerlendirmelerinde ele alınan tüm konular içinde Bilgi Güvenliğinin son yıllarda en kritik alanlar arasında yer aldığı görülmektedir. Bu nedenle Türk Telekom İç Denetim Başkanlığı'nın denetim planları her yıl Bilgi Güvenliği Politikaları ve Sistemlerini kapsamaktadır. Öte yandan, genel kabul görmüş denetim ilkelerine göre, kullanılan metodolojiler çerçevesinde İç Denetim Başkanlığı Türk Telekom Grup bünyesindeki Bilgi Güvenliği ile ilgili alanlara yönelik denetimlerde makul güvence sağlamaktadır.

Üçüncü Taraflarda Bilgi Güvenliği

3. Taraf bilgi güvenliği politikamız üçüncü taraflarca imzalanarak uyumları denetlenmektedir. Ayrıca verinin güvenli aktarımı ve iş gereğinden fazla verinin aktarılmaması için onay süreçleri bulunmakta ve işletilmektedir. Sistemlerde bu verilerin korunması için uluslararası standartlarla belirlenmiş güvenlik tedbirleri sistemlerde/uygulamalarda alınmaktadır. Kişisel Verilerin Korunması Kanunu kapsamında Türk Telekom tarafından Aydınlatma Metinleri hazırlanmıştır.

Tüm sözleşmelerde Firmalarla 3. Taraf Bilgi Güvenliği Politikası ve ilgili işin kapsamında Türk Telekom'a hizmet verecek her bir Firma çalışanı ile Güvenlik Taahhütnamesi imzalanmaktadır. Söz konusu Politika ve Taahhütname ile Türk Telekom gizli/hassas verilerinin korunması amacıyla alınması gerekli önlemleri tanımlanmış ve yükümlülükleri belirtmiştir.

Türk Telekom 3. Taraf olarak müşteri verilerini işleyen yetkili bayilere sahiptir. Tüm bayilerde görünür alanlarda sergilenmek üzere Aydınlatma metinleri dağıtılmıştır. Tüm açık rıza gerektiren iş akışları için abone ve bayi çalışanlarına hitaben rıza metinleri hazırlanmış, bayilerin tüm gerekli hallerde bu onayları almaları zorunlu kılınmıştır. Ek olarak, iş ortağı ve tedarikçi sözleşmeleri KVKK ve ilgili mevzuata uygun şekilde incelenmekte ve revize edilmektedir. Ayrıca, iş ortaklarına ve bayilere kişisel verilerin korunması kapsamında gerekli eğitimler yapılmakta, duyurular gönderilmekte ve denetimler yapılmaktadır.

Veri Güvenliği ve Gizlilik ile İlgili Çalışan Eğitimleri

Bilgi Güvenliği ve İş Sürekliliği eğitimleri sınıf içi ve e-eğitim olarak personele verilmektedir. Personel tarafından bilgi güveliği taahhütnamesi imzalanır. Ayrıca, personele sürekli olarak bilgi güvenliği konularında bilgilendirme mailleri atılmaktadır.

Düzenli olarak verilen online eğitimler aşağıdaki konuları içermektedir:

- Kişisel veri işlemenin tarihi ve hukuksal zemini
- Türk Telekom'un bu konuda ana sorumlulukları
- Kişisel Veri İşleme Envanteri ve VERBİS
- İlgili kişinin hakları
- Veri depolama süreleri ve silme/imha
- İlgili kanun ve düzenlemelerde yer alan cezalar

- Türk Telekom iş süreçlerinde alınması gereken özel tedbirler
- Özel nitelikli kişisel veriler özelinde alınması gereken aksiyonlar
- Bilgi Güvenliği Farkındalığı
- İş Sürekliliği

Bilgi Güvenliği Sertifikasyonları

Türk Telekom'un sabit ve mobil şebekelerini kapsayan ISO 27001 sertifikası bulunmaktadır. Bu kapsamda yıllık periyotlarda Bilgi Güvenliği İç Denetim çalışmaları yürütülmektedir ve denetim sonuçlarına göre aksiyon ataması ve takibi yapılmaktadır. Ayrıca, ISO 27001 kapsamında standart gereği tüm çalışanlara periyodik olarak Bilgi Güvenliği Farkındalık eğitimleri atanmaktadır.

Ek olarak Türk Telekom'un mobil şebeke kapsamında PCI-DSS sertifikası bulunmaktadır. Bu kapsamda belirli periyotlarla sistemlerin zafiyet ve sızma testleri yapılmaktadır. PCI-DSS kapsamında standardın gereksinimi olan farkındalık eğitimleri periyodik olarak ilgili çalışanlara verilmektedir.