# Özel Nitelikli Kişisel Veri Güvenliği Politikası

## A. AMAÇ

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 özel nitelikli kişisel veridir. Amaç bu verilerin Kanuna uygun işlenmesini, korunmasını, gerekli hallerde güncellenmesini, ve silinmesini sağlayarak ulusal ve uluslararası yasalara uyum sağlamaktır.

## B. KAPSAM

Türk Ticaret Kanunu, İş Kanunu, Kişisel Verilerin Korunması Kanunu gibi faklı kanunlar gereği veya çalışma hayatı için gerekli olması durumunda özel nitelikli kişisel verilerin işlenmesi için manuel veya dijital ortamlar aracılığı ile kişisel veriler/özel nitelikli kişisel verilerin işlenmesi ve korunması ve veri güvenliği süreçlerini kapsar.

## C. UYGULAMA

1. Özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen şartların yerine getirilmesi ve Kurul tarafından belirtilen yeterli önlemlerin alınması gerekir.
2. Özel nitelikli kişisel veriler ile ilgili farkındalığın artırılması için çalışanlara farkındalık eğitimi, KVKK/GDPR Komitesi'ne ve Bilgi Güvenliği Yönetim Sistemi temsilcisine teknik eğitimler verilmelidir.
3. İş amacıyla ve kısıtlı olarak alınan özel nitelikli kişisel veriler için aydınlatma yükümlülüğü ve açık rıza beyanları alınır.
4. Özel nitelikli kişisel veriler için veri işleyenlerle gizlilik sözleşmeleri yapılır.
5. Özel nitelikli kişisel verilere yetkisiz erişimin engellenmesi için erişim yetki matrisi oluşturulur.
6. Oluşturulan erişim yetki matrisi aracılığı ile yetkiler sürekli kontrol edilir. Görevden ayrılanların yetkisi kaldırılır.
7. Özel nitelikli kişisel veriler üzerinde hassas olunması için bu verilere dijital ortamda erişenler zaman zaman log kaydı ile kontrol edilir.
8. Özel nitelikli kişisel verilerin korunması için güncellemeler, yamalar zamanında gerçekleştirilir.
9. Özel nitelikli kişisel verilere uzaktan erişim durumunda iki kademeli bir doğrulama oluşturulur.
10. Özel nitelikli kişisel verilerin bulunduğu ortamlar fiziki ortam ise bu ortamlar üzerindeki fiziki önlemler alınır. Giriş çıkışlar kontrol edilir. Kaza, yangın, sabotaj gibi durumlara karşı önlem alınır.
11. Özel nitelikli kişisel verilerin bulunduğu odalar, dolaplar vb kırmızı üçgen işareti ile işaretlenir. Bu alanlara o odada, o alanda çalışan biri olmaksızın, refakatçisiz girilemez.
12. Özel nitelikli kişisel veriler dijital ortamlar içinde ise: Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi; Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması; 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 aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması; Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekir.

13. 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 gerekir.

14. Özel nitelikli kişisel veriler aktarılacaksa: Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması; Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması; Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımının gerçekleştirilmesi; Verilerin kağıt ortamı yoluyla gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.

15. Çalışanların özlük dosyalarında özel nitelikli kişisel veriler yer aldığından klasörlerdeki dosyaların ilk sayfalarına beyaz boş A4 kağıt üzerine kırmızı kaşe ile “GİZLİ VERİ” kaşesi vurulur.

16. Açık rıza verenler eğer açık rızalarını yazılı ve kanunlara uygun olarak geri çekmek için kuruma başvururlarsa başvuru yapan ilgili kişilerin özel nitelikli kişisel verileri kullanılamaz.

## D. SORUMLULUKLAR



**KVKK Koordinatörü:** 6698 ile ilgili yasaya uyum için süreçlere destek olmak için gerekli tüm işleri yaptırmak, kaynak sağlamaktan, şirketler arası KVKKorganizasyonundan sorumludur.

**Veri Sorumlusu İrtibat Kişisi:** Dokümanın düzenlenmesi ve revize edilmesinden sorumludur. KVKK ile ilgili İç Tetkiklerde soruların hazırlanması ve İç Tetkikçilerin eğitimesinden sorumludur.

**KVKK/GDPR Komitesi:** Kişisel Veri Yönetimi ve Güvenliği Politikası’nın geliştirilmesinden ve politikanın yayımlanmasından, güncellenmesinden ve yayılımının sağlanmasından sorumludur.

**SOME Ekibi:** Siber saldırı veya veri güvenliği ihlali durumunda süreçleri yönetmenten sorumludur.

**İç Tetkikçiler:** Kişisel verilerin korunması ile ilgili soruları iç denetim sırasında sorulmasından sorumludur.

**Tüm Yöneticileri:** Kişisel verilerin yasalara uygun olarak alınmasından, işlenmesinden, güncellenmesinden, korunmasından, gerektiğinde silinmesinden, yok edilmesindenden sorumludur. İç tetkik sonuçlarının takibinden iyileştirilmesinden.

**Çalışanları:** Kişisel verilerin yasalara uygun olarak alınmasından, işlenmesinden, güncellenmesinden, korunmasından ve KVKK ile ilgili tüm kurumsal politikalara uygun iş yapmaktan ve davranmaktan sorumludur.

.