BOROVALI OTOMOTİV SANAYİ VE TİCARET ANONİM ŞİRKETİ ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

1. POLİTİKA, KAPSAM ve AMAÇ

1.1 Amaç

Özel Nitelikli Kişisel Veri İşleme Politikası'nın ("Politika") amacı, Borovalı Otomotiv Sanayi ve Ticaret A.Ş.'nin ("Şirket") mevcut ve potansiyel müşterileri, iş ortakları, ziyaretçileri, pay sahipleri, şirket yöneticileri, personel adayları, personelleri ve yetkilileri ile ilgili üçüncü kişilere ait özel nitelikli kişisel verilerin aktarılması, depolanması, imha edilmesi ve saklanması gibi her türlü veri işleme faaliyetlerindeki prensiplerin, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (''Kanun'') ve "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 Kararının belirttiği usul ve esaslara göre belirlenmesidir.

1.2 Kapsam

Politika hükümleri, Şirket'in faaliyet konuları ve çalışma alanlarında kişisel verilerin işlenmesi süreçlerine dahil olan tüm bilgi sistemlerini ve alt bilgileri, kontratları, çevre ve fiziksel alanları ve tüm bunlar için üretilen sistem ve düzenlemeleri kapsamaktadır.

Bu politika Şirket adına çalışan bir üçüncü tarafın, mevcut ve potansiyel müşterileri, iş ortakları, ziyaretçileri, pay sahipleri, Şirket yöneticileri, personelleri, personel adayları ve ilgili üçüncü tarafları ve üçüncü taraf personelleri ile yetkililerini kapsamaktadır.

2. TANIMLAR

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Özel nitelikli (hassas) 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 verilerini,

Kişisel verilerin 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

KVK: Kişisel verilerin korunması,

KVKK: 6698 sayılı Kişisel Verilerin Korunması Kanununu,

KVK Kurulu: Kişisel Verileri Koruma Kurulunu,

KVK Kurumu: Kişisel Verileri Koruma Kurumunu,

KVK Komitesi: Şirket organizasyonunun denetimi için yönetim kurulu tarafından atanan Kişisel Verilerin Korunması Komitesini,

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

3. GÖREV ve SORUMLULUKLAR

3.1 Şirket KVKK uyarınca veri sorumlusudur.

3.2 Üst Yönetim, yönetici ve denetçi pozisyonlarında olanlar başta olmak üzere tüm personeller Şirket bünyesinde özel nitelikli kişisel verilerin işlenmesinde doğru uygulamaların geliştirilmesi ve teşvik edilmesinden ve ayrıca bireysel görev tanımlarında yer verilmiş bu konuya ilişkin diğer yükümlülüklerden sorumludur.

3.3 KVK Komitesi, kişisel veri koruma sisteminin yönetilmesi ve KVKK ve sair ilgili mevzuata uyumun sağlanması ve belgelenmesi konularında görevli birimlerin denetlenmesinden ve bu konularda Yönetim Kuruluna karşı sorumludur.

3.4 Personellerin Görev ve Sorumlulukları:

Özel nitelikli kişisel veri işleyen personeller KVK Politikasında belirtilen sorumluluklarına ek olarak aşağıdaki konulardan da sorumludurlar;

a. Özel Nitelikli Kişisel Veri İşleme Politikası'na ve ilgili diğer politika ve prosedürlere uyumlu davranmak,
b. Görev ve sorumluluklarını Özel Nitelikli Kişisel Veri İşleme Politikası'nda yer alan talimatlara uygun olarak yerine getirmek.

3.5 KVK Komitesinin Görev ve Sorumlulukları

Kişisel Verilerin Korunması Komitesi KVK Politikasında belirtilen sorumluluklarına ek olarak aşağıdaki konulardan sorumludur;

a. Özel Nitelikli Kişisel Veri İşleme Politikası'nın oluşturulması ve güncellenmesinin sağlanması,
b. Özel nitelikli kişisel veri işleme süreçlerinin bu politikaya göre düzenlemek ve ilgili iş birimlerince uygulanmasını koordine etmek,
c. Şirket içindeki özel nitelikli kişisel verilerin işleme prensiplerinin geliştirilmesi, uygulanması ve güncellenmesine yönelik bir çerçeve oluşturulması ve sürdürülmesinde ilgili birimler ile birlikte çalışarak gerekli tedbirlerin ve eğitimlerin alınmasını sağlamak,
d. Personellere bu politika kapsamında oluşturulan süreçlerin uygulanması için destek olmak,
e. Bu politikaya yönelik ihlalleri altı ayda bir yönetime raporlamak,
f. Özel nitelikli kişisel veri işleme konularını ve gelişmeleri, politika/standart ve/veya diğer iç yönetmelikleri Şirket personeline uygun bir şekilde iletmek,
g. Özel nitelikli kişisel verilerin işlenmesine yönelik ihlaller ile ilgili şikâyetlerin raporlanması, yanıtlanması ve çözümlerin koordine edilebilmesinde temel rol üstlenmek,

h. Özel Nitelikli Kişisel Verilerin işlenmesi söz konusu olan; yeni ürün ve hizmetlerin geliştirilmesi sürecinde yer almak, işleme gereksinimlerinin belirlenmesine, yeni ürün veya hizmet üretim ortamına uygulanmadan önce konu hakkında görüş ve önerilerde bulunmak,
i. Özel nitelikli kişisel verilerin bulunduğu sistemlerin idari, teknik ve fiziksel güvenlik kontrollerini geliştirmek ve uygulanmasını sağlamak,
j. Yetkili iş birimleriyle birlikte çalışarak, özel nitelikli kişisel verilerin bulunduğu sistemlere iyileştirmelerin ve güvenlik değerlendirmelerinin yapılmasını sağlamak,
k. Şirket sistemlerinde bulunan ya da dağıtılan özel nitelikli kişisel verilerin korunmasını ve kullanımını izlemek ve değerlendirmek için prosedürleri ve teknolojiyi uygulamak.

4. VERİ GÜVENLİĞİ

Tüm personel, Şirket tarafından işlenen ve kendi sorumluluklarında olan verilerin güvenli olarak tutulmasını ve KVK Taahhütnamesi imzalamadıkça hiçbir üçüncü tarafa açıklanmamasını sağlamakla yükümlüdür.

Kişisel verilere, yalnızca bunlara erişimi gerekli olanlar erişebilmelidir. Erişimler, erişim yönetimi prosedürü uyarınca sağlanır.

Veri güvenliği, Şirket'in KVK Politikası ve buna bağlı dokümanlar uyarınca sağlanır.

Kişisel verilere ilişkin bilgi güvenliği olayları KVK Komitesince en kısa süre içerisinde KVK Kuruluna ve ilgili kişiye bildirilir.

Özel nitelikli kişisel verilerin işlenmesi söz konusu olduğunda ayrıca KVKK tarafından belirlenen yeterli güvenlik önlemlerinin veri sorumlusu olan Şirket tarafından yerine getirilmesi gerekmektedir.

4.1 Personellere Yönelik Güvenlik Önlemlerinin Alınması

İnsan Kaynakları, Muhasebe, Hukuk Birimi, İş Sağlığı ve Güvenliği Birimi, İdari İşler Birimi gibi özel nitelikli kişisel veri işlemek suretiyle iş süreçlerini yürüten iş birimlerinde bulunan personeller hakkında;

a. Gizlilik sözleşmeleri yapılmalı ve bu sözleşmenin ekinde Özel Nitelikli Kişisel Veri Politikası da bulunmalıdır.
b. Yukarıda sayılan ilgili birimlere yılda bir kişisel verilerin güvenliği konusunda eğitimlerin verilmesi,
c. Özel nitelikli kişisel verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması ve periyodik olarak yetki kontrollerinin gerçekleştirilmesi gerekir.
d. Görev değişikliği olan ya da işten ayrılan personellerin bu alandaki yetkilerinin derhal kaldırılması, mevcut hesaplarının derhal kapatılması gerekmektedir. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen kişisel veri barındıran envanterlerin (bilgisayar, harddisk, dosya, klasör vb.) iade alınması sağlanmalıdır.

4.2 Elektronik Ortamlarda Güvenlik Önlemlerinin Alınması

Söz konusu 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,
d. Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
e. 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,
f. Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekmektedir.

4.3 Fiziki Ortamlarda Güvenlik Önlemlerinin Alınması

Verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziki 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 gerekmektedir.

5. VERİ PAYLAŞIMI

Özel Nitelikli Kişisel Veriler ancak ilgili kişinin açık rızası veya 6698 sayılı kanunun 6. maddesinin 3. fıkrasında bulunan istisnalar kapsamında hukuka ve hakkaniyete uygun olarak üçüncü kişilerle paylaşılabilir.

Buna göre kişisel verilerin paylaşılabilmesi için aşağıdaki koşullardan birinin bulunması aranır:

a. Veri sahibin açık rızasının alınmış olması,
b. Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler için kişisel verilerin işlenmesi durumlarının kanunlarda açıkça öngörülmesi,
c. Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ise kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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 işlenebilir.

Özel nitelikli kişisel verilerin paylaşıldığı aşağıda belirtilen önlemleri alacak ve bu kapsamda aktarım faaliyetlerini yerine getirecektir;

Özel Nitelikli Kişisel Verilerin;

a. E-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılmalıdır,
b. Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması gerekir,

c. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi gerekir,
d. 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.

6. POLİTİKANIN GÜNCEL TUTULMASI *Doküman Sahipliği ve Onay*

Bu doküman sahibi KVK Komitesidir ve bu politikanın yukarıda belirtilen gözden geçirme gereklilikleri uyarınca düzenli olarak gözden geçirilmesinden sorumludur.

Bu dokümanın güncel versiyonu, tüm Şirket personeli ile paylaşılmış ve şirket web sitesi üzerinden yayınlanmıştır.

Bu politika 10.5.2021 tarihinde Yönetim Kurulu tarafından onaylanmış ve yayımlanmıştır.