



POLİTİKA 08 · KRB-POL-08

Gizlilik ve Bilgi Güvenliği Politikası



DOKÜMAN ADI Gizlilik ve Bilgi Güvenliği Politikası	DOKÜMAN NO KRB-POL-08	YAYIN TARİHİ 03.03.2025
REVİZYON NO / TARİHİ 1 / 11.08.2026	HAZIRLAYAN Hukuk ve Uyum Birimi	ONAYLAYAN Yönetim Kurulu

8.1 Amaç

Bu Politika'nın amacı; Karub Enerji'nin sahip olduğu veya üçüncü taraflardan emanet aldığı gizli bilgilerin, ticari sırların, fikri mülkiyet varlıklarının ve kişisel verilerin korunmasına ilişkin ilke, kural ve sorumlulukları belirlemek; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almaktır.

Ar-Ge yoğun bir teknoloji şirketi olarak Karub Enerji için bilgi; hücre ve modül üretim reçeteleri, proses parametreleri, test verileri, tasarım dosyaları ve müşteri bilgileri gibi en değerli varlıklar arasındadır.

8.2 Kapsam

Bu Politika; hangi ortamda bulunduğu bakılmaksızın (basılı, elektronik, sözlü veya görsel) Şirkete ait veya Şirket kontrolündeki tüm bilgileri; bu bilgilere erişimi olan tüm çalışanları, yöneticileri, stajyerleri, danışmanları, tedarikçileri ve iş ortaklarını kapsar. Yükümlülükler, iş ilişkisinin sona ermesinden sonra da devam eder.

8.3 Dayanak

- 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil mevzuatı ile Kişisel Verileri Koruma Kurulu kararları
- 6698 sayılı Kanun m. 9 uyarınca yurt dışına aktarıma ilişkin standart sözleşme, bağlayıcı şirket kuralları ve açık rıza mekanizmaları
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun
- 6102 sayılı Türk Ticaret Kanunu m. 396 (rekabet yasağı) ve haksız rekabete ilişkin m. 54 vd. hükümleri
- 6098 sayılı Türk Borçlar Kanunu m. 396 (işçinin sadakat borcu) ve m. 444-447 (rekabet yasağı)
- 5237 sayılı Türk Ceza Kanunu m. 135-140 (kişisel verilere ilişkin suçlar) ve m. 239 (ticari sır niteliğindeki bilgilerin açıklanması)
- 6769 sayılı Sınai Mülkiyet Kanunu ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu
- Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) — kapsama girdiği ölçüde
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı

8.4 Gizli Bilginin Tanımı ve Sınıflandırma

Gizli bilgi; kamuya açık olmayan, açıklanması hâlinde Şirkete, çalışanlarına, müşterilerine veya iş ortaklarına zarar verebilecek her türlü bilgidir. Buna özellikle şunlar dâhildir: üretim reçeteleri ve proses parametreleri, teknik çizim ve tasarımlar, Ar-Ge proje çıktıları ve test sonuçları, patent başvurusuna konu edilmemiş buluşlar, maliyet ve fiyatlandırma verileri, teklif ve ihale bilgileri, müşteri ve tedarikçi listeleri, sözleşme koşulları, finansal veriler ve iş planları, çalışan özlük ve ücret bilgileri, bilgi sistemlerine ilişkin güvenlik bilgileri.

Bilgiler; "Açık", "İç Kullanım", "Gizli" ve "Çok Gizli" olmak üzere dört düzeyde sınıflandırılır. Her sınıf için erişim, saklama, iletim, çoğaltma ve imha kuralları ayrı ayrı belirlenir ve belgeler uygun şekilde etiketlenir.

8.5 Temel Gizlilik Yükümlülükleri

- ◆ Gizli bilgiler yalnızca işin gerektirdiği ölçüde ve "bilmesi gereken" (need-to-know) ilkesi çerçevesinde kullanılır.
- ◆ Gizli bilgiler, yetkisiz kişilerle — Şirket içindeki diğer çalışanlar dâhil — paylaşılamaz.
- ◆ Üçüncü taraflarla bilgi paylaşımı, önceden imzalanmış yazılı gizlilik sözleşmesine (NDA) dayanmalıdır.
- ◆ Gizli bilgiler, kişisel cihazlara, kişisel e-posta hesaplarına, onaylanmamış bulut hizmetlerine veya taşınabilir belleklere kopyalanamaz.
- ◆ Gizli bilgiler; sosyal medyada, konferanslarda, basın açıklamalarında veya yapay zekâ tabanlı genel kullanıma açık araçlarda paylaşılamaz.
- ◆ İş ilişkisinin sona ermesi hâlinde tüm gizli bilgiler ve bunları içeren tüm ortamlar Şirkete iade edilir; kopya saklanamaz.
- ◆ Gizlilik yükümlülüğü, iş sözleşmesinin sona ermesinden sonra da süresiz olarak devam eder.
- ◆ Üçüncü kişilerden hukuka aykırı yollarla rakip bilgisi edinilmesi ve kullanılması yasaktır.

8.6 Kişisel Verilerin Korunması

Şirket, veri sorumlusu sıfatıyla işlediği kişisel veriler bakımından KVKK m. 4'te düzenlenen genel ilkelere uyar: hukuka ve dürüstlük kurallarına uygunluk; doğru ve güncel olma; belirli, açık ve meşru amaçlar için işleme; amaçla bağlantılı, sınırlı ve ölçülü olma; mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

- ◆ Kişisel veriler yalnızca KVKK m. 5 ve m. 6'da sayılan işleme şartlarından birinin varlığı hâlinde işlenir.
- ◆ İlgili kişiler, veri işleme faaliyetinden önce KVKK m. 10 uyarınca aydınlatılır; gerekli hâllerde açık rıza alınır ve rızanın geri alınabilir olduğu bildirilir.
- ◆ Kişisel Veri İşleme Envanteri hazırlanır ve güncel tutulur; VERBİS kayıt yükümlülüğü, kapsama girildiği ölçüde yerine getirilir.
- ◆ Kişisel Veri Saklama ve İmha Politikası uyarınca saklama süreleri belirlenir; süre sonunda veriler silinir, yok edilir veya anonim hâle getirilir.
- ◆ Veri işleyen sıfatıyla hizmet alınan taraflarla, KVKK'ya uygun veri işleme sözleşmeleri akdedilir.
- ◆ Yurt dışına aktarım; KVKK m. 9 çerçevesinde yeterlilik kararı, uygun güvenceler (standart sözleşme, bağlayıcı şirket kuralları) veya istisna hükümlerine dayanılarak gerçekleştirilir ve Kuruma bildirim yükümlülükleri gözetilir.
- ◆ İlgili kişi başvuruları, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ uyarınca en geç otuz gün içinde sonuçlandırılır.
- ◆ Çalışan izleme faaliyetleri (kamera, log kaydı, araç takip, e-posta denetimi) yalnızca meşru amaçla, ölçülü biçimde ve çalışanlar önceden bilgilendirilerek yürütülür.
- ◆ Kurumsal internet sitesinde çerez kullanımı, ayrı bir Çerez Politikası ve çerez yönetim aracı ile şeffaf biçimde yönetilir; zorunlu olmayan çerezler için açık rıza alınır.

8.7 Fikri ve Sınai Mülkiyet Haklarının Korunması

Çalışanların iş görme edimi kapsamında ürettiği buluş, tasarım, yazılım ve eserler üzerindeki haklar, mevzuat ve sözleşme hükümleri çerçevesinde Şirkete aittir. Çalışan buluşlarına ilişkin bildirim ve bedel süreçleri Sınai Mülkiyet Kanunu hükümlerine uygun olarak yürütülür. Patent başvurusu yapılması planlanan teknik çözümler, başvuru

tarihinden önce kesinlikle açıklanmaz; ticari sır olarak korunması tercih edilen bilgiler için erişim kısıtları uygulanır. Üçüncü kişilere ait fikri mülkiyet haklarına saygı gösterilir; lisanssız yazılım kullanımı yasaktır.

8.8

Bilgi Güvenliği Tedbirleri

- ◆ **Teknik tedbirler:** güvenlik duvarı ve ağ segmentasyonu, uç nokta koruma ve zararlı yazılım tespiti, disk ve iletim şifrelemesi, çok faktörlü kimlik doğrulama, yetki ve rol bazlı erişim yönetimi, log kaydı ve izleme, yama ve zafiyet yönetimi, düzenli yedekleme ile yedeklerin geri dönüş testleri.
- ◆ **İdari tedbirler:** bilgi güvenliği farkındalık eğitimleri, ortalama (phishing) simülasyonları, temiz masa ve temiz ekran uygulaması, gizlilik taahhütnameleri, işe giriş-çıkış yetki süreçleri, tedarikçi güvenlik değerlendirmesi.
- ◆ **Fiziksel tedbirler:** üretim alanları, sunucu odaları ve Ar-Ge laboratuvarlarına kartlı geçiş kontrolü, ziyaretçi kayıt ve refakat düzeni, kritik alanlarda kamera izleme, kâğıt belgeler için kilitli dolap ve evrak imha cihazı kullanımı.
- ◆ Üretim ve laboratuvar alanlarında yetkisiz fotoğraf ve video çekimi yasaktır.
- ◆ İş sürekliliği ve felaketten kurtarma planları hazırlanır ve düzenli olarak test edilir.

8.9

İhlal Yönetimi

Gerçekleşmiş veya şüphelenilen her türlü bilgi güvenliği ve veri ihlali, gecikmeksizin Bilgi Teknolojileri birimine ve Hukuk/Uyum birimine bildirilir. İhlal olayları; tespit, sınırlandırma, kök neden analizi, giderme ve raporlama aşamalarını içeren bir müdahale prosedürüne göre yönetilir. Kişisel veri ihlali hâlinde, Kişisel Verileri Koruma Kuruluna en kısa sürede ve her hâlde yetmiş iki saat içinde bildirim yapılır; ilgili kişiler makul en kısa sürede bilgilendirilir. İhlal kayıtları tutulur ve benzer olayların tekrarını önleyecek tedbirler alınır.

8.10

Yaptırım, İzleme ve Yürürlük

Bu Politikanın ihlali; iş sözleşmesinin haklı nedenle feshine kadar varan disiplin yaptırımlarını, tazminat sorumluluğunu ve suç teşkil eden fiiller bakımından cezai sorumluluğu doğurabilir. Üçüncü taraf ihlallerinde sözleşmesel yaptırımlar uygulanır ve ilişki sonlandırılabilir.

Politikanın etkinliği; ihlal olayı sayısı ve müdahale süresi, farkındalık eğitimi tamamlama oranı, ortalama simülasyonu başarı oranı, ilgili kişi başvuru sayısı ve yanıt süresi ile denetim bulguları üzerinden izlenir. Politika yılda en az bir kez veya mevzuat değişikliği hâlinde derhâl gözden geçirilir ve Yönetim Kurulu onayı ile yürürlüğe girer.

HAZIRLAYAN

Hukuk ve Uyum Birimi

Ad – Soyad / İmza / Tarih

ONAYLAYAN

Yönetim Kurulu

Ad – Soyad / İmza / Tarih