

# CANON'UN GİZLİLİK TAAHHÜDÜ: TEKNİK VE ORGANİZASYONEL ÖNLEMLER (TOM)

VERİ KORUMA VE GİZLİLİK

Canon

Bu teknik ve organizasyonel önlemler, Canon'un veri koruma yükümlülüklerine uymasını sağlamaya yardımcı olur.

## ORGANİZASYONEL ÖNLEMLER

### POLİTİKALAR



Canon'un Gizliliğe İlişkin Hesap Verebilirlik Çerçevesi, veri koruma ve gizlilik mevzuatına uyumun farklı yönlerini yansıtan bir dizi politika beyanından oluşur.

### YÖNETİŞİM



Hesap Verebilirlik Çerçevesinin EMEA bölgesi genelinde uygulanması için görev ve sorumlulukları net bir şekilde tanımlanmış DPO ve Gizlilik Öncülerinden oluşan kapsamlı bir yönetim yapısından yararlanılmaktadır.

### RİSK YÖNETİMİ



Gizlilik Etki Değerlendirmeleri, Veri Koruma Etki Değerlendirmeleri, Teknik ve Organizasyonel Önlemler anketleri ve kapsamlı Tedarikçi Durum Tespiti prosedürleri dahil olmak üzere Kişisel Verilere ilişkin riskleri hafifletmek için bir dizi risk yönetimi yaklaşımından yararlanılmaktadır.



### GİZLİLİK



Müşteri verilerine erişim yetkisi yalnızca geçerli veri işleme amaçlarını yerine getirmek için gerekli ölçüde verilir ve müşteri verilerine erişimi bulunan tüm personel gizlilik yükümlülüklerine tabidir.

### EĞİTİM VE FARKINDALIK



Eğitim ve Farkındalık, Hesap Verebilirlik Çerçevesini pekiştirmekte olup kişisel verilerin işlenmesine erişimi veya bu doğrultuda sorumluluğu bulunan tüm personelin Canon Gelişim Merkezi aracılığıyla uygun eğitimleri tamamlaması şart koşulur.

### TEDARİKÇİ DURUM TESPİTİ



Üçüncü Taraf şirketler durum tespiti değerlendirmelerinden geçer ve müşteri verilerini yalnızca sözleşme mutabakatlarına göre işler.

# CANON'UN GİZLİLİK TAAHHÜDÜ: TEKNİK VE ORGANİZASYONEL ÖNLEMLER (TOM)

VERİ KORUMA VE GİZLİLİK

Canon

## ORGANİZASYONEL ÖNLEMLER (DEVAMI)

### MUHAFAZA



Canon, müşterilerimiz adına işlediğimiz kişisel verilerin güvenli bir şekilde yönetileceğini taahhüt eder ve gizlilik yönetmeliklerine uyulmasını sağlamak için iş ortaklarımızla yakın iş birliği yaparız.

### VERİ AKTARIMI



Canon, uygun tedbirler olmadıkça verileri belirli bir yargı bölgesinin dışına aktarmaz (örneğin, AEA özelinde Standart Sözleşme Maddeleri).

### BİLDİRİM VE ŞEFFAFLIK



Canon'un Gizlilik bildirimleri, Grubun kişisel verileri nasıl yönettiğini yansıtır. Şeffaflık ve güven, kişisel verilerin işlenmesinde temel ilkelere sahiptir.

### PRIVACY BY DESIGN



Gizlilik, veri yaşam döngüsü boyunca tüm ürünlerimize, çözümlerimize ve hizmetlerimize dahil edilmiştir.

### DAVRANIŞ KURALLARI



Canon, Grubun yönetici ve çalışanlarının her türlü kişisel bilgiyi sıkı bir şekilde yöneteceğini ve tüm geçerli yasalara, yönetmeliklere ve belirlenen şirket prosedürlerine uyacağını belirten Grup Davranış Kurallarına bağlıdır.

### HESAP VEREBİLİRLİK



Canon; tüm kişisel veri işleme faaliyetleri, bilgi hakları talepleri, veri ihlalleri ve risk değerlendirme süreçlerinin kapsamlı dahili kayıtlarını tutarak hesap verebilir olduğunu kanıtlar. Ayrıca, müşterilerimizi kendi hesap verebilirlik yükümlülükleri bakımından da destekliyoruz.

### OLAY YÖNETİMİ VE İŞ SÜREKLİLİĞİ



Canon; kişisel veri ihlallerini tespit etme, bildirme, yönetme, düzeltme ve çözüme kavuşturmaya yönelik süreçlere sahiptir.

# CANON'UN GİZLİLİK TAAHHÜDÜ: TEKNİK VE ORGANİZASYONEL ÖNLEMLER (TOM)

VERİ KORUMA VE GİZLİLİK

Canon

## TEKNİK ÖNLEMLER



### SERTİFİKA

Belirli bir ürün/çözüm/hizmet için uygun durumlarda Canon, ISO/IEC 27001 gibi ilgili sertifikaları sürdürür.



### KİMLİKSİZLEŞTİRME VE SİLME

Kimliksizleştirme teknikleri ürün ve çözümlerimizde yerleşik olup anonimleştirme, yarı anonimleştirme ve referans bütünlüğüne zarar vermeden silme işlemlerini içerebilir.



### BELGE GÜVENLİĞİ

Canon; uygun kriptografi kontrolleriyle geçiş, üretim ortamı ve üretim dışı ortamda kişisel verileri korur. Uygun durumlarda, cihaz güvenliğini sağlamak üzere yapılandırmalar "sıkılaştırılır".

## ERİŞİM POLİTİKASI



İşletme ve bilgi güvenliği gerekliliklerine dayanan erişim kontrolü politikaları ve süreçleri resmen belgelendirilmiş ve uygulanmakta olup düzenli aralıklarla gözden geçirilmektedir. Bu politikalar ve süreçler, ayrıcalıklı kullanıcı erişimi ve ev/mobil çalışma düzenlemelerini ele alır.

## KULLANICI ERİŞİMİ KONTROLÜ



Mantıksal erişim kontrolleri uygulanmaktadır. Benzersiz kullanıcı hesapları yalnızca yetkili bireylere atanır ve bilgilere asgari düzeyde erişim sağlamak üzere yönetilir. Parola kontrolleri uygulanır.

## FİZİKSEL GÜVENLİK



İş bakımından hassas veya kritik bilgileri içeren alanlara ve bilgi işlem tesislerine yalnızca yetkili personelin erişmesine izin verilmesini sağlamak üzere, güvenli alanlar uygun giriş kontrolleriyle korunmaktadır.



# CANON'UN GİZLİLİK TAAHHÜDÜ: TEKNİK VE ORGANİZASYONEL ÖNLEMLER (TOM)

VERİ KORUMA VE GİZLİLİK

Canon

## TEKNİK ÖNLEMLER (DEVAMI)



### ORTAM AYRIMI

Bir çözümün barındırıldığı durumlarda mantıksal istemci ayrımı uygulanır.



### SİLİNEBİLİR MEDYALAR

Silinebilir medyalarda saklanan kişisel verilerin izinsiz açıklanması, değiştirilmesi, kaldırılması veya imhasını önlemek amacıyla Silinebilir medyaların kullanımını yönetmek için kontroller oluşturulmuştur.



## EKİPMANLARIN GÜVENLİ ŞEKİLDE BERTARAF EDİLMESİ VEYA YENİDEN KULLANIMI

Tüm medyalar için güvenli bertaraf süreçleri mevcuttur ve saklama medyası içeren tüm ekipmanlar, bertaraf edilmeden veya yeniden kullanılmadan önce tüm kişisel verilerin uygun bir standarda göre kaldırılmış veya güvenle üzerine yazılmış olmasını sağlamak için doğrulanır.



## ETKİNLİK KAYDI

Çözüm veya hizmet, etkinlik kayıtlarını saklayabilir (örneğin, kullanıcı ve yönetici erişiminin kaydı ve veri girişi, verilerin değiştirilmesi ve silinmesi).



## İZLEME

Veri ihlallerini önlemeye yardımcı olmak için kullanıcı ve sistem etkinliği izlenmektedir.



## KULLANILABİLİRLİK

Hizmet güvenilirliği ve düşük kesinti oranını sağlamak için kontroller mevcuttur.



## DONANIM VE YAZILIM ENTEGRASYONU

uniFLOW ve IRIS gibi Canon'a ait belge çözümleri, ortaya çıkan güvenlik ihtiyaçlarına daha hazırlıklı olarak uyum sağlamamıza ve sistem ihlallerine ilişkin olasılığı düşürmemize olanak tanımaktadır.