**Global Şirket Dışı Taraf Kaynakları Gizlilik Bildirimi**

|  |  |
| --- | --- |
| **Gizlilik Bildirimi Konusundaki İletişim Kişisi:**  Global Veri Koruma Görevlisi | **Tarih: 1 Ocak 2023** |
| ([pgprivacyofficer.im@pg.com](mailto:pgprivacyofficer.im@pg.com))  **Bölge:** Global | **Kapsam:**  Tüm Harici Taraf Kaynakları |

# **A****maç**

Bu Bildirim (“Bildirim”) Procter & Gamble Company ve yan kuruluşlarının ve/veya bağlı kuruluşlarının (“P&G” veya “Şirket”) sizin Kişisel Verilerinizi nasıl toplayacağı ve yöneteceği hakkında tüm Kurum Dışı Taraf Kaynaklarını (“EPR”) bilgilendirir.

# **Bağımsız Yüklenici Durumu**

Bu Bildirim, P&G ile EPR arasında bir istihdam ilişkisi oluşturmaz. EPR’ler, hizmetlerin doğrudan P&G’ye veya P&G ile EPR’nin işvereni arasındaki bir anlaşmaya bağlı olarak sağlanıp sağlanmadığına bakılmaksızın, P&G’ye ilgili hizmetleri bağımsız yükleniciler olarak sağlarlar.

1. **Tanımlar**

**Şirket Dışı Kaynak:** Yükleniciler gibi, P&G’ye iş veya hizmet sağlayan ve söz konusu iş veya hizmetlerin sağlandığı tarihte P&G’nin kayıtlı işvereni olmayan herhangi bir kişi.

**Kişisel Veri:** İsim, diğer tanımlayıcılar, iletişim bilgileri, mesleki bilgiler ve kişisel özellikler gibi kimliği belirli veya belirlenebilir olan kişiyle ilgili her türlü bilgi.

**Şirket veya P&G:** Bu bildirimin amaçları doğrultusunda, Şirket veya P&G, Procter & Gamble Company, iştirakleri ve/veya bağlı kuruluşları anlamına gelir.

1. **İlkeler**

P&G’nin temel veri gizliliği işleme prensipleri şunlardır:

* Minimum miktarda EPR Kişisel Verisini toplamak ve yönetmek.
* Bireysel gizliliğe saygı göstermek.
* Amacımız, Değerlerimiz ve Prensiplerimiz (ADP’ler) ve ilgili yasalara uyumlu olmak.
* EPR Kişisel Verilerini toplarken ve/veya yönetirken uygun standartları ve prosedürleri izlemek.

1. **Bildirim**

P&G gizliliğinize saygı gösterir. Bu Bildirim, EPR Kişisel Verilerini nasıl işlediğimizi, doğrudan sizden ve/veya işvereninizden topladığımız bilgi türlerini, bunları kullanma amaçlarımızı, bunları paylaştığımız alıcı kategorilerini ve kullanımımız konusunda sizin yapabileceğiniz seçimleri açıklar. Ayrıca EPR Kişisel Verilerinin güvenliğini korumak için aldığımız önlemleri ve gizlilik uygulamalarımız hakkında bizimle nasıl iletişime geçebileceğinizi bu belge içinde açıklamaktayız.

* 1. **EPR Kişisel Verilerini Hangi Amaçlar İçin Toplar ve Kullanırız?**

P&G, P&G’nin sizinle ve/veya işvereninizle olan hizmet sözleşmesi ve bağımsız yüklenici ilişkisi kapsamında bulunan EPR’leri hakkında Kişisel Verileri toplar. Bizler, EPR Kişisel Verilerini sizden ve/veya işvereninizden genellikle aşağıdaki hizmetler ve/veya faaliyetler için toplar ve kullanırız:

* Sağlıkla ilgili taramalar ve COVID-19 veya benzeri sağlık acil durumlarıyla ilgili tıbbi programlar dahil olmak üzere iş sağlığı/güvenliği
* Saha erişim yönetimi
* Kimlik doğrulama ve onaylama, kimlik ve yaka kartları oluşturma, sistem yönetimi, oturum açılış/kapanış kaydı ve erişim bilgilerinin yönetimi, bilgi güvenliği ve siber güvenlik dahil olmak üzere kimlik ve kullanıcı bilgisi yönetimi
* İş sürekliliği, görevlendirme, vardiya yönetimi ve acil durum/güvenlik protokolleri dahil olmak üzere acil durum planlama amaçları
* Elektronik cihaz kaydı ve yönetimi, ağ ve cihaz kullanım optimizasyonu
* Elektronik cihaz ve ağ izleme ve CCTV gibi güvenlik video kaydı dahil olmak üzere fiziksel ve siber güvenlik kontrolleri
* Davalar ve dâhili/harici soruşturmalar, denetimler ve anlaşmazlık çözümü
* Günlük iş işlemleri (örneğin sistemlerimizde doğrulama ve oturum açma)
* Toplantı, eğitim ve etkinliklere katılım
* Rüşvet önleme, çocuk işçiler, yolsuzluk önleme, yaptırımlar, ihracat kontrolleri, insan hakları ve diğer kurumsal yönetim ve idare gereksinimleri ile ilgili kanunlar, yönetmelikler ve Şirket politikaları ile uyum
* P&G ve/veya işvereniniz tarafından iş yeri suistimali veya süreç ihlalleri konusunda yürütülen soruşturmalar
* Hizmetlerin performansının değerlendirilmesi de dahil olmak üzere sizinle ve/veya işvereninizle imzalı hizmet sözleşmelerimizin yürütülmesi ve denetimi,
* Tüm yasal, düzenleyici, adli veya devlet gerekliliklerine uygunluk ve mahkeme kararlarına, mahkeme celplerine, araştırma taleplerine veya diğer resmi veri taleplerine yanıt verme ve bunlara uyma
  + Personel ve tesislerin güvenliği ve izlenmesi ve P&G’nin, çalışanlarımızın ve müşterilerimizin hırsızlığa, yasal yükümlülüğe, dolandırıcılığa veya suistimale karşı korunması dahil olmak üzere güvenlik ve risk yönetimi.
  1. **Hangi Türde EPR Kişisel Verilerini Topluyoruz?**

Bizlerin, sizden topladığı ve sizinle ilgili olarak temin edebileceği EPR Kişisel Veri türlerini ve oranlarını her zaman en az seviyede tutacağız. Aşağıdaki tablo, P&G’nin iş süreçleri ile alakalı olarak topladığı EPR Kişisel Verileri kategorilerini daha ayrıntılı olarak açıklamaktadır.

Veri toplama ve veriye erişim, ülkeye özgü yasal ve/veya iş gereksinimlerine göre farklılık gösterecektir.

EPR Kişisel Verilerini toplamak ve işlemek konusundaki yasal veya iş temelleri, aşağıdaki Bölüm 5.3’te tanımlandığı gibi veri türü ve amaçlanan kullanıma göre farklılık gösterecektir.

|  |  |
| --- | --- |
| **Ne Tür EPR Verilerini Toplar ve İşleriz?** | **Neden Bu Tür EPR Kişisel Verisi Türlerini Toplar ve İşleriz?**  *Bu veri türlerini, Bölüm 5.1’de ayrıntılarıyla belirtilen ve aşağıda daha ayrıntılı olarak açıklanan pek çok kurumsal süreç ve iş süreçleri için toplar ve işleriz:* |
| *İletişim Bilgileri ve Kişisel Özellikler*   * İsim/soyisim veya önceki isimler (kızlık soyismi gibi) * P&G tarafından verilen kimlik numaraları veya kimlik bilgileri (ör. e-posta ile oturum açma) veya işvereniniz tarafından verilen herhangi bir kimlik numarası gibi diğer özgün tanımlayıcılar. * Fiziksel/posta adresi * E-posta adresi * Telefon numarası | * İş yeri ve elektronik ağ erişimi * Vardiya yönetimi de dahil olmak üzere, iş acil durum planlamasıyla ilgili sizinle olan iletişimler * Toplantı, eğitim ve etkinliklere katılım * Günlük iş işlemleri (örneğin sistemlerimizde doğrulama ve oturum açma) * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi   + Personel ve tesislerin güvenliği ve izlenmesi ve P&G’nin, çalışanlarımızın ve müşterilerimizin hırsızlığa, yasal yükümlülüğe, dolandırıcılığa veya suistimale karşı korunması dahil olmak üzere güvenlik ve risk yönetimi * Sağlıkla ilgili taramalar ve COVID-19 veya benzeri sağlık acil durumlarıyla ilgili tıbbi programlar dahil olmak üzere iş sağlığı/güvenliği * Hizmetlerin performansının değerlendirilmesi de dahil olmak üzere sizinle ve/veya işvereninizle imzalı hizmet sözleşmelerimizin yürütülmesi ve denetimi * Tüm yasal, düzenleyici, adli veya devlet gerekliliklerine uygunluk ve mahkeme kararlarına, mahkeme celplerine, araştırma taleplerine veya diğer resmi veri taleplerine yanıt verme ve bunlara uyma |
| *Vatandaşlık Numarası/İş İçin Uygunluk Bilgileri/Çalışan Numarası*   * Vatandaşlık kimlik bilgileri (pasaport, vize, sosyal güvenlik numarası, sürücü belgesi ve devlet tarafından verilen diğer kimlik bilgileri gibi) * Uyruk * İkamet edilen yer * Milliyet * Doğduğu ülke * Ordu ve/veya gazilik durumu * P&G’nin sözleşmeli olduğu şirketin çalışanı olarak özgün kimlik | * Sizi yasal olarak tanımlamak ve kayıtlarımızın bütünlüğünü korumak * Göçmenlik ve diğer iş izni gereklilikleri ile uyum sağlama * Şirket otomobillerini kullanan EPR’ler için sürücü belgesi verileri toplama, profesyonel lisans doğrulama, yolsuzluk önleme ve benzer amaçlar için güvenlik ve risk yönetimi * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Güvenlik ve acil durum planlaması * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi |
| *Mali bilgiler*   * Banka hesap numarası ve detayları * Masraf geri ödeme amaçları için temin edilen hallerde kişisel ödeme kartı bilgileri | * Kolaylaştırıcı gider geri ödemesi * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Güvenlik ve acil durum planlaması * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi |
| *Sağlık Bilgileri*   * İş görevleri ve fonksiyonlarını gerçekleştirme konusundaki engel veya kısıtlamalar da dâhil olmak üzere bir bireyin fiziksel veya duygusal sağlığı ile ilgili bilgiler * Uyuşturucu testleri ve diğer sağlık muayenesi türleri | * Meslek sağlığı ve iş yeri güvenliği ve devlet raporlama gereklilikleri ile uyum sağlama * COVID-19 pandemisi ve diğer benzer acil sağlık durumları ile alakalı EPR güvenliği ve iş risklerinin idaresi * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Güvenlik ve acil durum planlaması * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi |
| *Elektronik Kimlik Verileri/ Özel Tanımlayıcılar / Görsel ve Ses*   * P&G sistem tanımlayıcılar (örneğin kullanıcı adları veya çevrimiçi kimlik bilgileri) * Dijital imza * P&G cihazlarına, sistemlerine, uygulamalarına, lisanslarına, veri tabanlarına ve P&G ağına (e-posta, internet ve sosyal medya kullanımınız gibi) erişim ve kullanımla ilgili elektronik kimlik belirleme verileri, kayıtları ve dökümleri. * Kapalı Devre Televizyonu (“KDT”), saha erişim sistemleri, hat süreci veya görev kameraları da dâhil olmak üzere P&G güvenlik sistemleri tarafından toplanan bilgiler * Fiziki P&G sahalarına ve erişimin kısıtlandığı alanlara erişiminiz ile ilgili, yaka kartı numarası/yaka kartı tanımlayıcı ve fotoğraf da dâhil olmak üzere elektronik kimlik belirleme verileri, kayıtları ve dökümleri * Toplantı/eğitim bağlamında video, fotoğraf ve diğer görsel/ses kayıtları * Çağrı merkezi kayıtları hakkında elektronik kimlik belirleme verileri | * Sistem idaresi, teknolojik ve bilgi teknolojileri varlık erişimi ve yönetimi * Dâhili ve/veya harici tehditler karşısında fiziksel güvenliğimiz, bilgi güvenliğimiz ve siber güvenlik çıkarlarımızı destekleme * Ofis ve imalat sahalarımızda kayıp önleme ve geri kazanım idaresi * Veri eşleştirme ve analitikler de dâhil olmak üzere dâhili kayıt tutma ve raporlama * P&G sahaları, ağı, araçları, uygulamaları ve diğer Şirket sistem ve varlıklarına erişime izin verme * Optimizasyon, kalite, denetim ve masraf amaçları için P&G araçları, lisansları, hizmetleri ve uygulamalarının tüketim amaçlı kullanımı ve masrafları konusunda görünürlük elde etme * Eğitim ve toplantıları hatırlama * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Güvenlik ve acil durum planlaması * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi |
| *Çerezler -* Çerezler, internette gezinirken bilgisayarınıza gönderilen küçük dosyalardır. Ziyaret ettiğiniz internet siteleri ile nasıl bir etkileşimde bulunduğunuz hakkında faydalı bilgiler barındırırlar. Çerezler, bilgisayarınızda veya cihazınızda veya dosyalarınızda saklanan herhangi bir bilgiyi toplamazlar. Çerezler, sizi doğrudan belirli bir kişi olarak tanımlayacak bilgileri içermezler. Çerezler bilgisayar ve cihazınızı yalnızca rastgele verilen numara ve harfler olarak (örneğin çerez kimliği ABC12345) gösterirler ve asla, örneğin John E. Smith olarak göstermezler. Kullandığımız çerez türleri şunlardır:   * *Oturum Çerezleri*.Oturum çerezleri sizi (rastgele oluşturulan bir kimlik kullanarak) sayfadan sayfaya gezindiğinizde hatırlarlar; böylece daha önce sağlanmış olan bilgiyi tekrar vermeniz istenmez. Bu çerezler, sitemizden ayrıldığınız veya tarayıcınızı kapattığınız anda silinirler. * *Kalıcı Çerezler*. Kalıcı çerezler, sitelerin, tekrar ziyaretiniz sırasında tercihlerinizi hatırlamasına izin verirler. Örneğin, siteyi ilk ziyaretinizde Fransızca olarak okumayı seçmişseniz, siteye bir dahaki gelişinizde sayfaları otomatik olarak Fransızca dilinde görüntülersiniz. * *Analitik Çerezler*. Bu çerezler bize internet sitelerimizin nasıl çalıştığını anlatır. Bazı durumlarda, sitelerimizin performansını gözlemlemek için Google Analytics çerezleri kullanırız. Google Analytics tarafından toplanan bilgileri kullanma ve paylaşma yetimiz, [Google Analytics Kullanım Koşulları](https://www.google.com/analytics/terms/us.html) ve [Google Gizlilik Politikası](https://policies.google.com/privacy) tarafından kısıtlanır. | P&G’nin EPR için olan internet sitelerinde çerezleri, aşağıdakilerin de dâhil olduğu çeşitli amaçlarla kullanırız:   * internet sitelerimiz ve P&G içerikleri ile etkileşiminiz hakkında daha fazla bilgi edinmek * internet sitelerimizi ziyaret ettiğinizdeki deneyimlerinizi geliştirmemize yardımcı olmak * web sitesini tercihlerinize göre özelleştirmek * hataları saptamak ve çözümlemek amacıyla * internet sitelerimizin performansının ne kadar iyi olduğunu analiz etmek |
| *Diğer Kişisel Özellikler*   * Parmak izi veya yüz taraması gibi biyometrik veriler * Adli sicil kaydı/geçmiş taraması | * Biyometrik veriler aracılığıyla Şirket siteleri ve sistemlerine erişiminizi kolaylaştırma * Yasal ve politika uyumluluğu * Kurumsal yönetişim ve yönetim * Güvenlik ve acil durum planlaması * Zorunlu harici raporlama * Soruşturmalar ve olay yönetimi |

* 1. **EPR Kişisel Verilerini Hangi Yasal ve/veya İş Temelinde İşleme Koyarız?**

Sizinle ve/veya işvereninizle olan bağımsız yüklenici ilişkimize ilişkin sözleşmeden doğan ve/veya yasal yükümlülüklerimize uymak, gizlilik çıkarlarınıza uygun şekilde Şirketin meşru ticari çıkarlarını desteklemek ve uygun olduğunda, rızanızla sağlanan Kişisel Verileri amaçlanan amaçları doğrultusunda işlemek için gerekli minimum EPR Kişisel Verilerini toplar ve yönetiriz.

EPR Kişisel Verilerini işleme konusundaki yasal temeller ve/veya iş temelleri, P&G’nin geçerli kanun ve yönetmeliklere; sözleşmesel yükümlülüklere; Şirketin meşru menfaatine; kamu sağlığı çıkarlarına ve/veya sizin izninize uygun ve tabi olabilir.

EPR Kişisel Verilerini işleme konusundaki yasal temeller ve/veya iş temelleri, yasal yetki alanının yanı sıra veri kategorisi/türü ve bu tür bilgileri toplama ve kullanma nedenlerimize göre değişiklik gösterebilir.

Bu veri kategorilerinin işlenmesi için genel olarak dayanacağımız yasal dayanaklar şunlardır:

|  |  |
| --- | --- |
| **Kişisel Veri Türü** | **İşleme için Yasal/İş Temeli** |
| İletişim Bilgileri, Vatandaşlık Kimliği, Finansal Bilgiler, Sağlık Bilgileri | P&G’nin sözleşmeden doğan ve yasal yükümlülüklere uyumu |
| Vatandaşlık Numarası/İş İçin Uygunluk | P&G’nin geçerli kanunlarla uyumu |
| Mesleki Veriler, İletişim Bilgileri | P&G’nin meşru menfaati |

* 1. **EPR Kişisel Verilerini Nasıl Paylaşırız?**

P&G EPR Kişisel Verilerini yalnızca yasal bir iş gereği bilmesi gereken kişilerle paylaşacaktır.

P&G, verilerinizi işvereninizle (ve işvereniniz tarafından talimat verildiğinde diğer tüzel kişiliklerle), P&G yüklenicileriyle, tedarikçileriyle, alt yüklenicileriyle, geçici işçilerle veya P&G namına hareket eden diğer taraflarla (“Harici Taraflar”) paylaşabilir.

EPR Kişisel Verileri, yukarıdaki Bölüm 5.2’de belirtilen işleme amaçları doğrultusunda gerektiğinde genel merkezimiz ve bağlı şirketlerimizle paylaşılabilir.

EPR Kişisel Verilerini, kanunların veya hukuki süreçlerin gerektirmesi halinde, P&G’nin hak ve politikalarını uygulamak veya korumak ve/veya şüpheli veya fiili suistimal veya yasa dışı faaliyetlerin soruşturulmasına yardımcı olmak üzere ifşa edebiliriz.

* 1. **Gizlilik Haklarınız Nelerdir?**

Bizimle iletişime geçme ve sizin hakkınızda işlediğimiz EPR Kişisel Verilerine erişim talebinde bulunma hakkına sahipsiniz. Yürürlükteki yasalara uygun olması halinde yanlış, eski veya gereksiz verilerin düzeltilmesini, silinmesini veya kısıtlanmasını talep edebileceğiniz gibi P&G’den size ait verileri mevcut duruma uygun şekilde bir hizmet sağlayıcısına iletebileceğiniz formata getirmesini de talep edebilirsiniz. EPR Kişisel Verilerin işlenmesi onaya bağlı olduğu zaman onayınızı her an geri çekme hakkına sahipsiniz. EPR Kişisel Verilerin işlenmesinin makul çıkarları temel aldığı hallerde, belirli koşullarla verilerin işlenmesine itiraz etme hakkınız bulunmaktadır.

Bu hakları kullanırken, endişelerinizi öncelikle saha sponsorunuz olarak görev yapan P&G çalışanıyla görüşmenizi öneririz. Alternatif olarak, aşağıdaki adresten Veri Koruma Görevlimizle iletişime geçebilirsiniz. Taleplerinize verdiğimiz yanıtlardan veya Kişisel Verilerinizi işlememizden memnun değilseniz, ülkenizdeki veri koruma makamına şikâyette bulunabilirsiniz.

* 1. **EPR Kişisel Verilerini Nasıl Aktarırız?**

P&G global bir şirkettir ve birçok ülkede EPR’leri bulunmaktadır. Yasal olarak izin veriliyorsa ve ülkeye özgü gereklilikler ve/veya sınırlamalara tabi olarak, EPR Kişisel Verileri toplandığı ülke dışındaki ülkelere aktarılabilir. EPR Kişisel Verileri Amerika Birleşik Devletleri’ndeki sistemlerde depolanabilir, dünya genelindeki P&G bağlı şirketleri tarafından bu bilgilere ulaşılabilir. Bilgilerin aktarılması kapsamına bu şirketlerin hizmet sağlayıcıları ve ilgili faaliyetlerin yerine getirilmesi amacıyla diğer ülkelerine iletilmesi de dahildir. Bu ülkeler, ikamet ettiğiniz ülke ile aynı veri koruma yasalarına sahip olmayabilir. Size ait Kişisel Veriler bulunduğunuz ülkenin dışına aktarıldığı veya bu ülkelerden erişildiği zaman, bunları korumak için uygun güvenlik tedbirlerini uyguladığımız gibi, yasal bakımdan gerekli idari, teknik ve/veya sözleşmeye dayalı gereklilikleri yerine getiririz. Avrupa Ekonomik Alanı (AEA), Birleşik Krallık (Birleşik Krallık) ve İsviçre dışında, hem P&G kuruluşları arasında hem de hizmet sağlayıcılarımıza Standart Sözleşme Maddelerine dayanarak transferler gerçekleştiririz. Bir Maddelerin kopyasını isterseniz, [corporateprivacy.im@pg.com](mailto:corporateprivacy.im@pg.com) adresi ile iletişime geçin. P&G aynı zamanda verilerin toplanan ülke dışına çıkarılmasını kısıtlayan ülkeye özgü diğer gerekliliklere de uyacaktır.

* 1. **EPR Kişisel Verilerini Nasıl Güvence Altına Alırız?**

EPR Kişisel Verilerini kaza sonucu, kanuna aykırı veya yetki verilmemiş şekilde imha edilmeye, kaybolmaya, değiştirilmeye, ifşa edilmeye, erişime veya kullanıma ve başka her tür kanuna aykırı işleme şekillerine karşı korumak için tasarlanmış olan takma ad kullanma, şifreleme ve erişim denetimleri gibi gerekli fiziki, idari ve teknik önlemleri uygularız. EPR Kişisel Verileri, P&G adına Üçüncü Kişiler tarafından işlendiğinde, bu Üçüncü Kişiler ile de bu tür verileri işlerken uygun fiziksel, idari ve teknik tedbirleri aldıklarından emin olmak adına sözleşmeler imzalarız.

**5.8 Kişisel Verilerimi Ne Kadar Süre Saklıyorsunuz?**

Geçerli yasa daha uzun bir elde tutma süresi gerektirmediği veya buna izin vermediği sürece, EPR Kişisel Verilerini toplama amaçlarını yerine getirmek için gereken süre boyunca saklarız. Bu genellikle hizmetler için kullanım yaptığınız dönem ile sınırlı olacaktır. Bazı durumlarda, yasadan veya sözleşmeden doğan yükümlülüklere uymak için EPR Kişisel Verilerini P&G ile ilişkiniz sona erdikten sonra bir süre saklamamız gerekebilir.

* 1. **P&G Ağ ve Cihaz Kullanımını İzliyor mu?**

Şirket bazı P&G ağını ve P&G cihaz kullanımlarını izlemektedir. P&G’nin kendi çalışanlarını, varlıklarını ve tesislerini koruma yükümlülüğü vardır. P&G, şirket ağ ve cihazlarını üç amaç için izlemektedir: i) P&G çalışanlarının, verilerinin, ağının, varlığının, tesislerinin, itibarının ve rekabetçi çıkarlarının güvenliğini (gizlilik, dürüstlük ve mevcudiyet kapsamlarında) korumak; ii) kuşku duyulan veya teyit edilmiş olan kusurlu davranışları veya yasa ihlallerini (yargılama sürecini desteklemek amacı dâhil olmak üzere) soruşturmak ve iii) iş süreçleri ve finansal raporlama konusunda dürüstlüğü korumak.

P&G, meşru bir neden bulunmadığı veya yasal yaptırım makamının isteği dahil olmak üzere yasa uyarınca gerekli olmadığı sürece belli bir bireyin P&G ağını ve cihazlarını izlemez. Yürürlükteki yasalara uygun olarak, yukarıda belirtilen amaçlar için gerekli olduğu şekilde ağlarımız ve cihazlarımız aracılığıyla oluşturulan, saklanan, gönderilen veya alınan tüm elektronik dosyalara, verilere ve mesajlara erişme, bunları inceleme, ifşa etme ve imha etme hakkını saklı tutarız. Bu izleme her zaman ilgili yasa ve yönetmeliklere uygunluktur. P&G, yerel yasal gereklilikleri yerine getirmek için gerektiği zaman ilave prosedürler, standartlar, iç yönergeler ve/veya aktif önlemler uygulayacaktır.

P&G özellikle, P&G çıkarlarına yönelik potansiyel tehditleri belirlemek için P&G ağlarını ve EPR’lere verilen P&G’ye ait cihazları pasif ve aktif olarak izleyecektir. Bu “pasif izleme” bireyin davranışını aktif şekilde incelemez, bunun yerine risk göstergeleri araştırır. Bu risk göstergeleri P&G ve uzman güvenlik sağlayıcılar tarafından önceden tanımlanır ve P&G’nin güvenlik ihtiyaçlarını karşılayacak şekilde ayarlanır. Böyle bir risk göstergesi tetiklendiği zaman (bir “Vaka”) sistemler ilgili verileri günlüğe kayıt eder ve müteakip inceleme ve soruşturma için kayıt altında tutar. Özellikle, P&G ağlarında ve EPR’lere verilen P&G’ye ait cihazlarda aşağıdaki pasif izleme teknikleri kullanılacaktır:

1. **Kullanma Düzeni İzlemesi** bir izleme tekniğidir ve yazılım ve donanım önceden tanımlanmış bir dizi risk göstergesi bakımından P&G’nin kişilik tanımlayıcı olmaktan çıkarılmış ağ ve web verilerini kontrol eder. Bu teknik, P&G’nin ağının ve/veya P&G’ye ait cihazların *kullanılma* şeklinde kuşku çeken düzenler bulunup bulunmadığını inceler. Örneğin, P&G, Kullanma Düzeni İzleme aracını P&G oturum açma yerinde risk göstergeleri bulunup bulunmadığını inceleyecek şekilde ayarlayabilir. P&G Güvenliği bu aracı o şekilde ayarlayabilir ki bir kullanıcının oturum açma bilgileri bir kişinin söz konusu iki yer arasında makul şekilde yolculuk yapabileceği süreden daha hızlı şekilde iki farklı P&G lokasyonunda girildiği zaman alarm verir.
2. **Gelen Trafik Taraması** web üzerinden gelen iletişimleri (eposta dahil) P&G ağına girerken risk göstergeleri bakımından tarayan bir izleme aracıdır. Virüsten koruma ve güvenlik duvarı yazılımı bu aracın en yaygın örneğidir çünkü gelen trafiği eklerdeki, bağlantılardaki, web sitelerindeki, vb. kötü amaçlı yazılım göstergeleri bakımından sürekli şekilde tarar.
3. **Periyodik Tarama**, Gelen Trafik Taramasının yaptığı çevresel taramalardan kurtulabilecek belirli risk göstergelerini yakalamak için P&G ağı ve P&G cihazları düzeyinde tarama yapan bir izleme aracıdır. Bazen ilave bir kapsam ile bakıldığı zaman Vakaların belirlenmesi daha kolay olduğu için bu araç yararlıdır. Virüsten koruyucu tam disk taraması bu olanağın başlıca örneğidir.
4. **Giden Trafik Taraması** P&G giden web trafiğini belirli, önceden tanımlanmış risk göstergeleri bakımından tarama olanağına sahiptir. Bu araç belirli risk göstergesi kurallarına göre bir Vaka tetiklenip tetiklenmediğini anlamak üzere giden trafiği tarar. Örneğin, P&G, P&G ağı dışındaki yerlere yeni bir ürün formülünde kullanılan belirli bir kimyasal bileşik gibi bazı anahtar kelimeler veya Son Derece Kısıtlı veriler içeren büyük dosyaların yüklenmesine dikkat çekmek üzere bir kural yazabilir

P&G, pasif izleme araçları tarafından işaretlenen veya başka bir şekilde (örneğin dava açılması, kusurlu davranış suçlaması, yasal yaptırım, vb.) P&G’nin dikkatine getirilmiş olan bir riskin özellikleri temelinde riskin daha ayrıntılı şekilde soruşturulması/analiz edilmesi gerekip gerekmediğini değerlendirir. P&G bu değerlendirmede çalışanlara, tüketicilere, diğer paydaşlara ve/veya Şirkete ve ayrıca söz konusu olan tüm bireylerin yasal ve gizlilik haklarına gelebilecek zararı dikkate alır. P&G, varlıkları korumak ve iş süreçlerinin bütünlüğünü garanti etmek için yasal veya politika gerekliliklerine dayalı olarak daha fazla analiz gerekip gerekmediğini de belirleyebilir. Bu analize dayalı olarak, P&G ya daha başka bir soruşturma yapmayacak veya aktif izleme araçlarını kullanarak orantılı bir soruşturma yürütecektir.

P&G beş temel türde Aktif İzleme aracı kullanır: (1) Cihaz Tarama, (2) İnternet Tarama, (3) Yazılım İzleme, (4) Donanım İzleme (5) Veri Kaybını Önleme.

1. **Cihaz Tarama:** Bu araçlar P&G’nin, bazen üçüncü bir taraf vasıtası ile, P&G mülkiyetindeki bir bilgisayarın veya başka bir P&G cihazının *tüm* içeriğini bir soruşturmada kullanılmak üzere zamandaki belli bir noktaya çekmesini sağlar. Cihaz Tarama araçları yalnızca P&G cihazına kaydedilmiş ve depolanmış dosyaları ve uygulamaları çekmekle kalmaz aynı zamanda elde edilme sırasında cihazda bulunan belleği de alabilir. P&G, araca bağlı olarak, yalnızca fiziki dosyaları (yani bellek dışındakileri) seçebilir veya cihazın kısmi bir görüntüsünü alabilir – bu olanak, orantılı olma ilkesine uygun şekilde soruşturmanın yalnız belirli tür dosyalara veya uygulamalara odaklanmasını sağlar.
2. **İnternet Tarama:** P&G üç temel özelliğe sahip olan bulut tabanlı üçüncü taraf bir web proxy aracı kullanmaktadır. Birincisi, EPR P&G’ye ait bir Cihaz kullanırken kamuya açık internet kullanımını URL (yani ziyaret edilen web sayfalarının isimleri) düzeyinde izleme yeteneğine sahiptir. Bu özellik, onaylanmış bir soruşturmada kullanma potansiyeli ile, kırpılmış kişisel tanımlayıcılar kullanarak (ve böylece kullanıcının kimlik bilgilerini kaldırarak) internet faaliyetini izler ve kaydeder. İkincisi, şifrelenmemiş bir web sayfasına girilen veriler ve şifrelenmemiş web sayfalarını ziyaret ederken yüklenen veya indirilen dosyalara görünürlük sağlar. Üçüncüsü, önceden yüksek riskli olarak tanımlanan sınırlı bir web trafiği alt kümesinin şifresini çözme yeteneğine sahiptir (örneğin, bilinen kötü amaçlı web sayfalarına giden bağlantılar, cihazlara kötü amaçlı yazılım sağladığı bilinen web sayfaları veya onaylanmamış dosya paylaşım siteleri). Bu çözüm, son kullanıcı hakkında hassas kişisel verileri işleyebilecek web sitelerine (ör. bankacılık ve sağlık hizmetleri siteleri) bağlı trafiğin şifresini çözmeyecek şekilde yapılandırılmıştır.
3. **Yazılım İzleme:** Bunlar, (a) kişinin soruşturma yapıldığı bildirildiği ve (b) kişinin soruşturmanın konusu olmadığı durumlarda, kimliği belirlenebilir kişileri içeren bir soruşturmanın parçası olarak kullanılan tekniklerdir. Örneğin, coğrafi şekilde tetiklenen bir Vakanın meşru olup olmadığını anlamak amacı ile *belirlenmiş* bir EPR’nin yerleşik/oturum açmış durumda olup olmadığını belirlemek üzere bir telefon araması veya bir eposta bir Yazlım İzleme aracı olabilir.
4. **Donanım ve Uygulama İzleme**: Donanım ve Uygulama İzleme araçları üreticilerin donanımın ve/veya uygulamanın içine yerleştirdiği kaydetme ve izleme yetenekleridir ve belirlenebilir bir EPR ile bir araya geldiği zaman Aktif İzleme oluştururlar. Yaygın şekilde kullanılan örnekleri arasında sunucu günlükleri, SAP girişleri, yaka kimlik kartı okuyucu raporları, ağ kimliği doğrulama, vb. bulunmaktadır.
5. **Veri Kaybı Önleme:** P&G veya onaylı bir hizmet sağlayıcı, veri kaybı göstergeleri için P&G harici adreslere bağlı e-postaları tarar. Örneğin, bir EPR, P&G harici bir e-posta adresine Son Derece Kısıtlı eki olan şifrelenmemiş bir e-posta gönderirse, veri kaybı önleme çözümü bu e-postayı bir bilgi güvenliği riski olarak işaretler ve kullanıcıyı gelecekteki iletişimler için onaylanmış bir şifreleme çözümü kullanması gerektiği konusunda bilgilendirilebilir. Benzer şekilde, Son Derece Kısıtlı veya Gizli olarak sınıflandırılan bir giden e-posta (özellikle belirlenmiş anahtar kelimeler dahil) işaretlenirse, bu e-posta güvenlik riski açısından incelenir. Uygun görülürse soruşturma başlatılabilir. P&G, “Kişisel” veya “Özel” olarak sınıflandırılan veya konu satırında “Kişisel” veya “Özel” olarak işaretlenen mesajları taramaz.
6. **Gelecekte Yapılacak Değişiklikler**

P&G, örneğin yasalarda, düzenlemelerde, şirket uygulamalarında ve prosedürlerinde yapılan değişikliklere uymak veya yeni tehditlere karşı koymak için veya veri koruma makamlarının getirdiği yeni gereklere karşılık olarak bu Bildirimi ihtiyaç duyulan şekilde değiştirme hakkını saklı tutar. Bu tür değişikliklerin EPR Kişisel Verilerinizi işlememizi esaslı şekilde etkilediği durumlarda, sizi buna göre haberdar edeceğiz.

1. **İletişim Bilgileri**

Kişisel verilerinizi/EPR Kişisel Verilerinizi işlememizle alakalı soru veya endişelerinizin olması veya gizlilik haklarınızı kullanmak istiyorsanız, Global Veri Koruma Yetkilimiz ile iletişime geçebilirsiniz. E-posta: [pgprivacyofficer.im@pg.com](mailto:pgprivacyofficer.im@pg.com), Telefon: +1 (513) 622-0103, Posta Adresi: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, A.B.D.

EPR Kişisel Verileriniz veya P&G tarafından işlenen herhangi bir kişisel veriyle ilgili olası bir veri ihlali endişeniz varsa, lütfen bize [securityincident.im@pg.com](mailto:securityincident.im@pg.com) adresinden e-posta gönderin.