



Funded by
the European Union

E-Ticarette Ürün Güvenliği için Teknik Destek

Proje Tanımlama Numarası: NEAR/ANK/2022/EA-RP/0213

Sözleşme No: TR2021/W2T2/A03/OT14-1/001

Strateji ve Eylem Planı

Faaliyet 1.4. Strateji ve Eylem Planı Geliştirme

Ağustos, 2025

Ankara, TÜRKİYE



Funded by
the European Union

İÇİNDEKİLER

İÇİNDEKİLER.....	2
PROJE BİLGİ FORMU.....	5
KISALTMALAR	6
TANIM	7
1 YÖNETİCİ ÖZETİ.....	8
2 GİRİŞ.....	11
2.1 Raporun Amacı	11
2.2 Kapsam ve Hedefler.....	11
2.3 Kapsam ve Sorun Tanımı.....	12
3 KAPSAM VE SORUN TANIMI	13
3.1 Türkiye’de e-ticaretin büyümesi ve PGD faaliyetleri üzerindeki etkileri.....	13
3.2 Mevcut E-PGD Modeli ve Sınırlamaları	13
3.3 Dijital Yaptırımı Engelleyen Yasal Boşluklar	14
3.4 Veri ve Teknoloji Kısıtlamaları	14
3.5 İnsan Kaynakları Açığı	15
3.6 AB Uyum Etkenleri: GÜGT ve DSA	15
3.7 Paydaşlar	15
3.8 Neden Acil Eylem Gerekliyor?.....	16
4 SAPR METODOLOJİSİ	17
4.1 Sağlam Bir Doğrulama Zemini Oluşturmak	17
4.2 Derin ve Kapsayıcı Paydaş Katılımı	18
4.3 Analitik Süreç: Sorundan Eyleme.....	19
4.4 Varsayımları, Kısıtlamaları ve Bağlantılı İlişkileri Yönetme	19
4.5 Yol Gösterici Metodolojik İlkeler.....	20
4.6 Metodolojinin Sonucu.....	20
5 HUKUKİ UYUMLAŞTIRMA (1. BİLEŞEN).....	21
5.1 E-PGD’de Hukukun Merkezi Rolü	21
5.2 AB GÜGT ve DSA: Türkiye için Neden Önemlidir?.....	21
5.3 Yasal Boşluklar ve Gerçek Uygulamalara Etkileri	22
5.4 1. Bileşen için Reform Vizyonu.....	23
5.5 Öncelikli Yasal İşlemler	23
5.6 Ön Koşullar ve Sıralama.....	24
5.7 Riskler ve Azaltım Önlemleri	24
5.8 1. Bileşen’in Beklenen Etkisi.....	24
6 IT ARACI GELİŞTİRME VE ENTEGRASYON (2. BİLEŞEN).....	25



Funded by
the European Union

6.1	Dijital Araçlar Neden Artık İsteğe Bağlı Değil?.....	25
6.2	Mevcut Durum: Değerli Sistemler, Ancak İzole Yapılar Devam Ediyor	25
6.3	Vizyon: Birleşik bir e-PGD IT Platformu.....	26
6.4	Temel İşlevler ve İşleyişi Nasıl Değiştirdikleri	26
6.5	Eşgüdümlü Çalışabilirliği Gerçeğe Dönüştürmek	27
6.6	Geliştirme Aşamaları: Temellerden Tam Kapasiteye	27
6.7	Diğer Temel Unsurlarla İlişkiler	28
6.8	Riskler ve Azaltım Önlemleri	28
6.9	Beklenen Dönüşüm.....	28
7	RİSK TEMELLİ GÖZETİM VE ANALİTİK (3. BİLEŞEN).....	29
7.1	E-Ticarette Risk Temelli Gözetim Neden Vazgeçilmezdir?.....	29
7.2	Konseptten Uygulamaya: Ulusal Risk Değerlendirme Metodolojisi (URDM)	29
7.3	E-Ticaret Bağlamında Riski Tanımlama.....	30
7.4	Verileri Önceliklere Dönüştürmek: Risk Modeli Nasıl Çalışır?	30
7.5	Gelişmiş Analitik ve Yapay Zekanın Rolü	31
7.6	Risk Temelli Gözetimin Kurumsallaştırılması	31
7.7	Ön Koşullar ve Kolaylaştırıcı Unsurlar	32
7.8	Riskler ve Azaltım Önlemleri	32
7.9	Beklenen Etki.....	32
8	KURUMSAL KAPASİTE GELİŞTİRME (4. BİLEŞEN).....	34
8.1	Kurumsal Kapasite Neden E-PGD Reformunda Belirleyici Faktördür?	34
8.2	Mevcut Kurumsal Yapı ve Neden Reform Gerekliyor?.....	34
8.3	Kurumsal Kapasite Geliştirme Neden Önemlidir?	35
8.4	4. Bileşenin Stratejik Hedefleri.....	35
8.5	Temel Kurumsal Önlemler ve Gerekçeleri	36
8.6	PGDKK'nın Stratejik Rolünün Güçlendirilmesi	37
8.7	4. Bileşen Uygulanmazsa Ortaya Çıkacak Riskler	37
8.8	Beklenen Dönüşüm.....	37
9	İNSAN KAYNAKLARI VE EĞİTİM (5. BİLEŞEN)	39
9.1	Neden İnsanlar E-PGD'nin Gerçek "İşletim Sistemi"dir?.....	39
9.2	Dijital Piyasalar için Genişletilmiş Beceri Seti.....	39
9.3	Ad Hoc Eğitimden Ulusal E-PGD Öğrenim Sistemine	40
9.4	Bilginin Kurumsallaştırılması ve "Eğitim Kaybının" Önlenmesi.....	41
9.5	İnsan Kaynaklarının Planlanması ve Görevlendirilmesi.....	41
9.6	Stratejik Getiri.....	41
10	FARKINDALIK ARTIRMA VE PAYDAŞ İŞ BİRLİĞİ (6. BİLEŞEN)	43
10.1	E-PGD Zincirinde Farkındalık ve İş birliğinin Rolü.....	43
10.2	Satıcılar Arasında Uyum Kültürü Oluşturmak.....	43
10.3	Platformları Proaktif Ortaklara Dönüştürmek.....	44
10.4	Tüketicileri Güvenlik Aktörleri Olarak Güçlendirmek.....	45
10.5	Sektör Kuruluşları ve Sivil Toplum ile İşbirliğinden Yararlanma.....	45



Funded by
the European Union

10.6	İş birliğini Sisteme Yerleştirme	46
10.7	6. Bileşen'in Sistemik Faydaları	46
11	EYLEM PLANI.....	47
11.1	Eylem Planının Amacı ve Rolü.....	47
11.2	SAPR Bileşenleri ile Stratejik Entegrasyon.....	47
11.3	Sıralama ve Bağımlılıklar	48
11.4	Aşamalı Uygulama.....	48
11.5	Sorumluluk Dağılımı	48
11.6	İzleme ve Uyarılma	49
11.7	Beklenen Sonuçlar	49
12	RİSK YÖNETİMİ VE RİSKİN AZALTIMI	50
12.1	Risk Yönetimi SAPR için Neden Esastır?	50
12.2	Risk Türleri ve e-PGD Reformu ile İlgili Önemi	50
12.3	SAPR Risk Matrisi.....	51
12.4	Risk Yönetiminin Eylem Planıyla İlişkisi.....	51
12.5	Risk Azaltımı için Rehber İlkeler	51
12.6	Etkili Risk Yönetiminin Faydaları	52
13	SONUÇ.....	53
EKLER.....		54





Funded by
the European Union

PROJE BİLGİ FORMU

Proje Başlığı	E-Ticarete Ürün Güvenliği için Teknik Destek
Sözleşme Numarası:	TR2021/W2T2/A03/OT14-1/001
Proje Değeri:	2.090.221,00 Euro
Başlangıç Tarihi:	09 Eylül 2024
Bitiş Tarihi:	08 Eylül 2026
Süre:	24 Ay
Sözleşme Makamı	Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığı Merkezi Finans ve İhale Birimi (CFCU)
Adres:	Emek Mahallesi, Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığı Kampüsü İnönü Bulvarı No:36, E blok, 06490 Çankaya/Ankara
Proje Yöneticisi:	Barbaros Murat Köse
Telefon:	+ 90 312 295 49 00
Faks:	+90 312 286 70 72
Sözleşme Müdürü:	Hacer Bilge
E-posta	hacer.bilge@cfcu.gov.tr
Faydalancı	Türkiye Cumhuriyeti Ticaret Bakanlığı
Adres	Söğütözü, 2176. Sk. No:63, 06510 Çankaya/Ankara
Telefon	+90 312 449 60 00
Proje Genel Koordinatörü:	Hatice Menderes Toker
Telefon	+90 312 204 89 00
E-posta:	menderesh@ticaret.gov.tr
Yüklenici	WEglobal Danışmanlık A.Ş.
Proje Direktörü:	Selcan Özen
Adres:	Oran Mahallesi, Kudüs Caddesi No: 6/1, İç Kapı No: 15, Çankaya/Ankara
Telefon:	+90 312 447 91 40
E-posta:	selcan.ozen@weglobal.org
Proje Ofisi Adresi:	Oran Mahallesi, Kudüs Caddesi No: 6/1, İç Kapı No: 15, Çankaya/Ankara
Raporlama Dönemi	Ağustos 2025
Rapor Hazırlayan	Daniela - Elena Clejanu, <i>Ekip Lideri</i> Gürhan Hatipoğlu, <i>Kilit Uzman 2, IT Uzmanı</i> Selin Özşahin Aykent, <i>Kilit Olmayan Uzman, Ürün Güvenliği, PGD ve Eğitim Uzmanı</i> Murat Gülgör, <i>Kilit Olmayan Uzman, E-ticaret Uzmanı</i> Mehmet Mücahit Arvas, <i>Kilit Olmayan Uzman, Hukuk Uzmanı</i>
Raporu gözden geçiren:	Selcan Özen, <i>Proje Direktörü</i>
Gönderildiği tarih:	29.08.2025





Funded by
the European Union

KISALTMALAR

Kısaltma	Tam Form
AI	Yapay Zeka
API	Uygulama Programlama Arayüzü
CE	Conformité Européenne (Avrupa Normlarına Uygunluk İşareti)
CFCU	Merkezi Finans ve İhale Birimi
DSA	Dijital Hizmetler Yasası (Yönetmelik (AB) 2022/2065)
GM	Genel Müdürlük
ÜGDGM	Ürün Güvenliği ve Denetimi Genel Müdürlüğü
e-PGD	E-Ticarete Piyasa Gözetimi ve Denetimi
EBYS	Elektronik Belge Yönetim Sistemleri
AB	Avrupa Birliği
ETBIS	Elektronik Ticaret Bilgi Sistemi
GÜGD	Genel Ürün Güvenliği Direktifi (2001/95/EC)
GÜGT	Genel Ürün Güvenliği Tüzüğü (AB) 2023/988
ICSMS	Piyasa Gözetimi ve Denetimi için Bilgi ve İletişim Sistemi
IP	İnternet Protokolü
IT	Bilgi Teknolojisi
MERSIS	Merkezi Sicil Kayıt Sistemi
ML	Makine Öğrenimi
TB	Ticaret Bakanlığı
MZ	Mutabakat Zaptı
PGD	Piyasa Gözetimi ve Denetimi
PGDK/YK	Piyasa Gözetim ve Denetim Kuruluşu / Yetkili Kuruluş
İAR	İhtiyaç Analizi Raporu
URDM	Ulusal Risk Değerlendirme Metodolojisi
PGDBIS	Piyasa Gözetimi ve Denetimi Bilgi Sistemi
PGDKK	Piyasa Gözetimi ve Denetimi Koordinasyon Kurulu
RAPEX	Gıda Dışı Tehlikeli Ürünler için Hızlı Uyarı Sistemi (Yeni “Güvenlik Kapısı”)
SAPR	Strateji ve Eylem Planı Raporu
KOBİ	Küçük ve Orta Ölçekli İşletme
SİP	Standart İşletim Prosedürü
TAREKS	Dış Ticaret Risk Temelli İthalat Kontrol Sistemi
UI	Kullanıcı Arayüzü
KPI	Kilit Performans Göstergeleri



Funded by
the European Union

TANIM

Bu dokümanın amacı doğrultusunda, aşağıda yer alan terimler şu anlamlara gelmektedir:

- “çevrim içi platformlar”: Elektronik ticaret aracı hizmet sağlayıcıları / Elektronik ticaret hizmet sağlayıcıları, çevrim içi pazar yerleri
- “dijital ticaret” veya “dijital pazar”: e-ticaret
- “elektronik ticaret”: Fiziksel bir karşılaşma olmaksızın, elektronik ortamda çevrim içi olarak gerçekleştirilen her türlü ekonomik ve ticari faaliyet





Funded by
the European Union

1 YÖNETİCİ ÖZETİ

Strateji ve Eylem Planı Raporu (SAPR), Türkiye'nin piyasa gözetimi ve denetimi (PGD) sistemini, giderek dijitalleşen, küreselleşen ve hızla değişen piyasa ortamında tüketicileri etkili bir şekilde koruyabilecek şekilde dönüştürmek için ileriye dönük bir çerçeve sunmaktadır. SAPR, e-ticaretin katlanarak büyümesine, satış kanallarının çeşitlenmesine ve sınır ötesi ürün akışlarının artmasına doğrudan yanıt vermektedir. Bu gelişmeler, ürün güvenliğinin sağlanması açısından yasal, teknik ve kurumsal yeni zorluklar ortaya çıkarmaktadır.

Bu dönüşüm, sadece ulusal bir zorunluluk değil, aynı zamanda Türkiye'nin AB'ye katılım sürecinde stratejik bir gerekliliktir. SAPR, çevrimiçi PGD, şeffaflık ve risk yönetimi için daha ileri standartlar belirleyen **Genel Ürün Güvenliği Tüzüğü (GÜGT, AB) 2023/988** ve **Dijital Hizmetler Yasası (DSA, AB) 2022/2065**'in gerekliliklerine dayanmaktadır.

SAPR, projenin **Genel Hedefleri** ile tamamen uyumludur:

- **AB ürün güvenliği kuralları doğrultusunda tüketicilerin sağlık ve güvenliğini korumak.**
- **Türkiye'nin ürün güvenliği alanındaki katılım sürecini desteklemek.**

Ayrıca, aşağıdaki **Özel Hedefe** de katkı sağlamaktadır:

- **PGD faaliyetlerini hem elektronik hem de fiziksel piyasalarda daha etkin bir şekilde yürütmek.**

İhtiyaç Analizinden Elde Edilen Önemli Bulgular

İhtiyaç Analizi ve paydaş görüşmeleri, Türkiye'nin mevcut PGD modelinin tam etkinliğini engelleyen bir dizi sistemik eksiklik ve operasyonel kısıtlamaları ortaya koymuştur:

- **Mevzuat eksiklikleri:** Mevcut hukuki düzenlemeler, çevrimiçi pazar yerlerinin, sınır ötesi satıcıların veya e-platformların ürün güvenliği kapsamındaki yükümlülüklerini yeterince düzenlememektedir.
- **Kurumsal dağınıklık:** Birden fazla Piyasa Gözetim ve Denetim Kuruluşu (PGDK), tam entegre veri paylaşım sistemleri olmadan çalışmakta olup, bu da riskin zamanında tespit edilmesini ve koordineli uygulama imkanlarını sınırlamaktadır.
- **Sınırlı dijital uygulama araçları:** Özel bir e-PGD platformunun, otomatik izleme işlevlerinin ve yapay zeka destekli risk hedefleme mekanizmalarının bulunmaması, çevrimiçi denetimlerin etkinliğini ve kapsamını azaltmaktadır.
- **Kapasite kısıtlamaları:** IT, veri analizi ve dijital denetim uzmanlığına sahip nitelikli personel eksikliği, proaktif ve risk temelli yaklaşımlara geçişi yavaşlatmaktadır.
- **Paydaşların katılımı ile ilgili zorluklar:** Platformlar, KOBİ'ler ve tüketici örgütleri ortak bir uyum ve farkındalık artırma çalışmalarına henüz sistematik olarak dahil bulunmamaktadır.

Stratejik Yaklaşım - Altı Temel Bileşen

Buna karşılık olarak, SAPR hem acil ihtiyaçları karşılamak hem de sürdürülebilir, geleceğe hazır bir sistem oluşturmak amacıyla **birbirini tamamlayan altı temel bileşen** üzerine inşa edilmiş tutarlı bir strateji ortaya koymaktadır:

1. **Hukuki Uyum** - Gizli satın alma, otomatize PGD ve orantılı yaptırımlar da dahil olmak üzere e-PGD faaliyetleri kapsamında açık yetkiler tanıyan, AB ile tam uyumlu yasal bir çerçevenin



Funded by
the European Union

oluşturulması. Bu kapsamda platform yükümlülükleri, sınır ötesi iş birliği kuralları ve dijital denetimlerde delil geçerliliği konularını tamamlayacak birincil ve ikincil mevzuatın revize edilmesi.

2. **IT Aracı Geliştirme ve Entegrasyon** - İzleme, vaka yönetimi ve analitiğini tek bir sistemde birleştiren ulusal bir e-PGD platformunun geliştirilmesi. Bu platform, ulusal veri tabanları (ETBIS, MERSIS, PGDBIS, TAREKS) ile bağlantılı olacak ve platformlarla yapılandırılmış, güvenli veri alışverişini mümkün kılacaktır. Modüler tasarım sayesinde geleceğe hazır hale getirilmesi, sosyal medya tarama ve görüntü tanıma gibi yeni teknolojiler için ölçeklendirmeye olanak sağlayacaktır.
3. **Risk Temelli Gözetim ve Analitik** – PGDK’ların ürün, satıcı ve satış kanalı riskine göre denetimlere öncelik vermelerini sağlayan ulusal bir **risk değerlendirme metodolojisinin** tasarlanması ve uygulanması. Bu metodoloji, AI/ML analitiğini, mevsimsel trend analizini ve tüketici şikayetleri ile **sınır ötesi ürün güvenliği bildirim ağlarının** sistematik kullanımını entegre ederek ortaya çıkan tehditlerin öngörülmesine ve bunlara hızlı yanıt verilmesine imkan tanıyacaktır.
4. **Kurumsal Kapasite Geliştirme** - PGDK’lar, Ticaret Bakanlığı, PGDKK ile diğer paydaşlar arasındaki yönetişim ve koordinasyon mekanizmalarının güçlendirilmesi. Bu çalışmalar, görev tanımlarının netleştirilmesi, SİP’lerin tanımlanması, performans hedeflerinin belirlenmesi ve e-PGD faaliyetleri için düzenli koordinasyon forumlarının kurulmasını içermektedir.
5. **İnsan Kaynakları ve Eğitim** - E-PGD’ye özgü iş tanımlarının belirlenmesi, IT uzmanları, veri bilimcileri ve risk analistlerinin istihdamı ve özel eğitim programlarının uygulanmasıyla yetkinlik zemininin genişletilmesi ve çeşitlendirilmesi. "Eğiticilerin Eğitimi" modeli sayesinde, kurumlar arasında sürdürülebilir kapasite geliştirilmesi sağlanacaktır.
6. **Farkındalık Artırma ve Paydaş İş Birliği** - Çevrimiçi platformlar, satıcı ağları ve tüketici örgütleri ile yapılandırılmış iş birliği kanallarının kurulması. Kamu farkındalık kampanyaları, tüketicileri güvenli satın alma uygulamaları ve bildirim kanalları hakkında bilgilendirirken, hedefli bilgilendirme çalışmaları KOBİ’lere ve satıcılara uyum yükümlülükleri konusunda rehberlik edecektir.

Stratejiden Eyleme

Eylem Planı (Bölüm 10), altı temel bileşeni **53 önlemle** işlevselleştirmekte, bu önlemleri kısa, orta ve uzun vadeli eylemler olarak sıralayarak, sorumlu kurumlar, koşullar ve Kilit Performans Göstergeleri (KPI) ile eşleştirmektedir.

Acil öncelikler şunlardır:

- Yasal boşluk analizinin tamamlanması ve GÜGT ve DSA uyumu için öncelikli değişikliklerin taslak haline getirilmesi.
- Ulusal risk değerlendirme metodolojisinin tamamlanması ve pilot uygulaması.
- E-PGD platformunun geliştirilmesi ve ilk entegrasyonların başlatılması.
- Denetçilere, analistlere ve platform uyum personeline hedefli, görevlerine özel eğitimler verilmesi.
- Tüketici bilgilendirme kampanyaları ve platform iş birliği protokollerinin başlatılması.



Funded by
the European Union

Beklenen Sonular

SAPR uygulama dneminin sonunda Trkiye'de aŐaĐıda yer alan unsurların gerekleŐtirilmiŐ olması beklenmektedir:

- Gerek zamanlı izleme ve uygulama kapasitesine sahip, AB ile uyumlu, tam olarak iŐlevsel bir e-PGD sistemi.
- evrimii ve evrimdiŐı piyasalardaki rn gvenliĐi risklerinin tmn ele alan uyumlu bir yasal ereve.
- Tm PGDK'lar arasında netleŐtirilmiŐ kurumsal koordinasyon ve grev daĐılımı.
- Dijital uygulama ve risk temelli dzenleme konusunda uzmanlaŐmıŐ becerilere sahip yaygın iŐgc kapasitesi.
- rn gvenliĐi iin ortak sorumluluk modeline uygun Őekilde platformların, satıcıların ve tketicilerin alıŐmalara daha gl katılımı.

Bu alıŐmalar bir btn olarak, tketicileri koruyan, piyasaya olan gveni glendiren ve Trkiye'nin rn gvenliĐi alanında AB'ye katılım srecindeki ilerlemesini hızlandıran modern ve dayanıklı bir PGD sistemi saĐlayacaktır.





Funded by
the European Union

2 GİRİŞ

2.1 Raporun Amacı

SAPR, Türkiye'nin **e-PGD yürütme** kapasitesini güçlendirmek için bir yol haritasıdır. Rapor, tüketicilere çevrimiçi kanallar aracılığıyla sunulan ürünlerin AB ürün güvenliği kuralları ve en iyi uygulama örnekleriyle uyumlu, güvenli ve izlenebilir olmasını sağlamak için tasarlanmıştır.

E-ticaret, benzersiz zorluklar ortaya çıkarmaktadır: ürünler dünyanın her yerinden sunulabilir, birden fazla platformda listelenebilir ve tüketiciler tarafından dakikalar içinde satın alınabilir. Fiziksel piyasalar için tasarlanmış geleneksel PGD modelleri, bu hız ve ölçeğe ayak uydurmak için artık yeterli değildir. SAPR, Türkiye'nin PGD sistemini **dijital piyasalara** uyarlamak için net bir strateji ortaya koyarken, iyileştirmelerin fiziksel piyasalardaki denetime de fayda sağlamasını temin etmektedir.

SAPR'nin amacı:

- Türkiye'nin e-PGD'sini AB gerekliliklerine, özellikle **Genel Ürün Güvenliği Tüzüğü (GÜGT)** ve **Dijital Hizmetler Yasası (DSA)** ile uyumlu hale getirmek için **stratejik bir yol haritası belirlemek**.
- **Stratejik öncelikleri**, sıralı bir Eylem Planı aracılığıyla **operasyonel önlemlere dönüştürmek**.
- PGD Kuruluşlarından, platformlara ve tüketici örgütlerine kadar, çevrimiçi ürün güvenliği ile ilgili tüm paydaşlar için **bir koordinasyon aracı sağlamak**.

2.2 Kapsam ve Hedefler

SAPR, öncelikle e-PGD'ye odaklanarak - çevrimiçi ortamda ürün güvenliği gerekliliklerinin izlenmesi, denetlenmesi ve uygulanması kapsamında aşağıdaki konuları ele almaktadır:

- Platform yükümlülükleri, çevrimiçi denetim yöntemleri ve yaptırım yetkileri için **yasal hükümler**.
- Platformlar genelinde ürünleri, satıcıları ve uyum eğilimlerini izlemek için **dijital izleme araçları**.
- Hedefli denetimleri mümkün kılan, çevrimiçi **satış kanallarına özel risk değerlendirme metodolojileri**.
- PGDKK gibi koordinasyon organları altında PGD Kuruluşları, Ticaret Bakanlığı ve ilgili paydaşlar arasında iş birliği sağlayacak **kurumsal yapılar**.
- Etkili e-PGD faaliyetleri için gerekli **beceri ve kaynaklar**.
- Uyum düzeyi ve raporlamayı iyileştirmek için platformlar, satıcılar ve tüketiciler başta olmak üzere tüm **paydaşların katılımı**.

Ağırlık e-PGD'ye verilmiş olsa da, önlemlerin çoğu - özellikle kapasite geliştirme, eğitim ve yasal uyum ile ilgili konular - **fiziksel piyasalarda** da PGD'yi güçlendirecek ve tüm satış kanallarında yeknesaklık sağlayacaktır.



Funded by
the European Union

2.3 Kapsam ve Sorun Tanımı

Türkiye'de E-Ticaretin Yükselişi

Türkiye'nin e-ticaret sektörü, son on yılda çift haneli yıllık büyüme kaydetmiş ve yurt içi ve sınır ötesi platformlarda her gün milyonlarca işlem gerçekleştirilmiştir. Bu büyüme aşağıdaki hususları beraberinde getirmiştir:

- Çok çeşitli tedarikçilerden ve coğrafyalardan gelen ürünlerle **tüketici seçeneklerinin artması**.
- **Ürünlerin piyasada daha hızlı dolaşması**, yani güvenli olmayan ürünlerin tespit edilmeden tüketicilere kolayca ulaşabilme ihtimali.
- Satıcıların yurtdışında bulunabilmesi, birden fazla platform kullanabilmesi ve minimum fiziksel altyapıyla faaliyet gösterebilmesi nedeniyle, **denetimlerin daha karmaşık hale gelmesi**.

E-PGD'de Mevcut Boşluklar

İhtiyaç Analizi, Türkiye'nin mevcut PGD modelinin esas olarak fiziksel piyasa denetimleri etrafında oluşturulduğunu vurgulamıştır. Ticari kayıt ve ürün takibi için elektronik sistemlerin geliştirilmesinde ilerleme kaydedilmiş olmakla birlikte, e-PGD'de de kritik boşluklar bulunmaktadır:

- E-platformlara yükümlülükler getirilmesi ve gizli satın alma gibi kimliğin ortaya konulmadan e-PGD faaliyeti yürütülmesi için **yetersiz yasal dayanak**.
- E-platformlardan, tüketici şikayetlerinden ve diğer yetkililerden elde edilen bilgileri bir araya getirmeyi zorlaştıran **parçalı veri sistemleri**.
- Otomatik ürün taraması, veri madenciliği ve yapay zeka destekli risk hedeflemesi için **sınırlı teknolojik araçlar**.
- Dijital soruşturma, veri analizi ve sınır ötesi uygulama iş birliği alanlarında **uzmanlık açığı**.

Değişimin itici gücü olarak AB uyumu

AB'nin **GÜGT'si**, çevrimiçi pazar yerlerinin PGDK'larla iş birliği yapmasını, güvenli olmayan ürünleri hızla kaldırmasını ve tüketicilerin doğru ürün bilgilerine erişebilmesini gerektirmektedir. **DSA**, risk değerlendirmeleri, raporlama ve tüketici koruma mekanizmaları dahil olmak üzere çevrimiçi araçlara yükümlülükler getirerek bunu tamamlamaktadır. Bu çerçeve düzenlemelere uyum sağlamak, hem **tüketici güvenliği** hem de Türkiye'nin **AB'ye katılım hedeflerini** ilerletmek için önem arz etmektedir.

SAPR'nin rolü

SAPR, teşhis ve eylem arasındaki boşluğu doldurmayı amaçlar. Bu bağlamda:

- Türkiye'nin e-PGD'sinin **proaktif, veriye dayalı ve uluslararası düzeyde eşgüdümlü çalışabilir hale** getirilmesi için gerekli reformları belirler;
- Bu reformları, net sorumluluklar içeren **pratik ve takvime bağlı önlemlere** dönüştürür;
- Tüm paydaşların öncelikler konusunda uyum sağlamaları ve çalışmalarını koordine etmeleri için **ortak bir referans noktası** sağlar.

Kısacası, SAPR geleneksel denetim modellerinden **modern, entegre ve AB ile uyumlu bir e-PGD sistemine** geçiş için **anlaşılır ve veriye dayalı bir plan** sunar.



Funded by
the European Union

3 KAPSAM VE SORUN TANIMI

3.1 Türkiye'de e-ticaretin büyümesi ve PGD faaliyetleri üzerindeki etkileri

Son on yılda, Türkiye'nin e-ticaret sektörü özgün bir kanaldan çıkarak perakende ticaretinde **baskın bir güce dönüşmüştür**. Bu dönüşüm, hızlı dijitalleşme, internet ve akıllı telefon kullanımının artması, değişen tüketici tercihleri ve rekabetçi lojistik çözümler tarafından desteklenmiştir. Sonuç, hem yerli hem de yabancı satıcıların dahil olduğu ve çocuk oyuncaklarından elektrikli ev aletlerine, kozmetik ürünlerden gıda takviyelerine kadar çok geniş ürün yelpazesini kapsayan ve **günlük milyonlarca işlemin gerçekleştiği** bir pazar haline gelmiştir.

Bu büyümenin hızı olağanüstü olmuştur. 2019 ile 2024 yılları arasında, çevrimiçi satışların parasal değeri üç katından fazla artmış, e-ticaretin toplam perakende satışlardaki payı rekor seviyelere ulaşmıştır. Bu hızlanmanın yavaşlaması beklenmemektedir; nitekim küresel eğilimler, dijital pazarın geleneksel fiziksel perakende pahasına payını genişletmeye devam edeceğini göstermektedir.

Bu durum tüketicilere daha fazla seçenek, kolaylık ve rekabetçi fiyatlar sunarken, **ürün güvenliği konusunda faaliyette bulunan kuruluşlarının denetim ortamını da köklü bir şekilde değiştirmektedir**. Geleneksel piyasalarda PGD faaliyetleri limanlar, depolar, mağazalar gibi sabit noktalarda gerçekleştirilir ve fiziksel tedarik zincirlerine bağlıdır. Ancak e-ticarette:

- Satıcılar dünyanın herhangi bir yerinde bulunabilir ve çoğunlukla Türkiye'de fiziksel bir varlıkları olmayabilir.
- Ürünler, farklı isimler ve açıklamalarla aynı anda birden fazla çevrimiçi platformda görünebilir.
- İlanlar, geleneksel PGD iş akışlarının çalışabileceğinden daha hızlı bir şekilde, dakikalar içinde oluşturulabilir, değiştirilebilir veya kaldırılabilir.

Bu dinamikler, **müdahale için mevcut fırsat penceresini** daraltmaktadır. Uygun olmayan bir ürün, denetçi onu risk olarak tanımlamadan önce satışa sunulabilir, satın alınabilir ve tüketiciye teslim edilebilir. Yaptırımların etkili olmaya devam etmesi için, PGD'nin, **reaktif, mekan temelli denetimlerden**, dijital ticaretin hızına ayak uydurabilen **proaktif ve teknoloji destekli izleme yöntemlerine** geçmesi gerekmektedir.

3.2 Mevcut E-PGD Modeli ve Sınırlamaları

Türkiye'nin PGD sistemi, geleneksel sektörlerde güçlü olmakla birlikte, hala **dijital çağa geçiş** aşamasındadır. Ticaret Bakanlığı genel politika yönünü belirlemekte, çeşitli PGDK'lar ise kendi sorumlulukları altındaki ürünlere dair PGD gerçekleştirmektedir. Koordinasyon, **Piyasa Gözetim ve Denetim Koordinasyon Kurulu (PGDKK)** tarafından desteklenmektedir.

E-ticaret alanında ise yetkili kurumlar **ETBİS, MERSİS, PGDBİS ve TAREKS** gibi mevcut sistemleri uyarlamaya çalışmaktadır. Ancak, bu araçlar **çevrimiçi pazar yerlerinin sürekli ve otomatik olarak gözetimi için tasarlanmamış olup**, eşgüdümlü çalışabilirlik veya gerçek zamanlı veri paylaşımı sağlanmaksızın birbirinden bağımsız şekilde kullanılmaktadır.

Mevcut e-PGD'nin operasyon modeli büyük ölçüde **denetçi eliyle yapılan web aramalarına** ve platformların geçici izlenmesine dayanmaktadır. Denetçiler şüpheli listeleri tek tek belirlemekte, ürün



Funded by
the European Union

bilgilerini doğrulamakta ve sonrasında yaptırım için önlemler almaktadır. Bu yöntem, bazı öncelikli vakalarda etkili olsa da, **kaynak yoğun, yavaş ve e-ticaret faaliyetlerinin hacmine uyum sağlayacak şekilde ölçeklenemeyecek durumdadır.**

Ayrıca, dijital yaptırımlara ilişkin kurumsal yetki alanları her zaman net değildir. Görev alanlarının çakışması, özellikle birden fazla risk kategorisi içeren ilanlar söz konusu olduğunda (örneğin, hem elektrikli ürün hem de çocuk ürünü olan elektronik bir oyuncak), **hangi PGDK'nın sorumlu olduğu konusunda** belirsizlikler yaşanabilmektedir. Bu parçalı yapı, uygulamalarda tutarsızlıklara yol açmakta ve denetim etkinliğini azaltmaktadır.

3.3 Dijital Yaptırımı Engelleyen Yasal Boşluklar

Yasal hükümler, e-PGD faaliyetlerinin ölçeklenmesi açısından **kritik bir engel** olmaya devam etmektedir. İhtiyaç Analizi, yasal çerçevenin dijital operasyonları tam olarak desteklemediği birkaç önemli alanı belirlemiştir:

- **Platform yükümlülükleri:** Mevcut mevzuat, çevrimiçi pazar yerlerine ürünlerin uygunluğunu doğrulama, yapılandırılmış verileri yetkililerle paylaşma veya güvenli olmayan ürünleri proaktif olarak kaldırma konusunda güçlü ve uygulanabilir yükümlülükler getirmemektedir.
- **Gizli denetim araçları:** **Gizli satın alma** gibi yöntemler (ürünlerin güvenliğini test etmek ve uygunluğunu doğrulamak için çevrimiçi olarak gizli kimliklerle ürün satın almak) açıkça düzenlenmemiş olup, satın alınan numunelerin kanıt olarak kabul edilebilirliği konusunda belirsizlik yaratmaktadır.
- **Dijital delil yönetimi:** İdari yaptırma ilişkin davalarda kullanılmak üzere dijital delillerin toplanması, saklanması ve kullanılmasına ilişkin usuller tam olarak standartlaştırılmamıştır.
- **Sınır ötesi iş birliği:** Türkiye bazı uluslararası güvenlik bildirim mekanizmalarına katılıyor olsa da, yabancı platformları veya satıcıları içeren **gerçek zamanlı bildirimler** için tam entegre bir mekanizma mevcut bulunmamaktadır.

Bu yasal yapı taşları olmadan, yetkililer sistematik olarak iş birliği talep edemez, zamanında veri elde edemez veya etkili risk azaltımı için gerekli olan çevrimiçi denetim faaliyetlerini tam gerçekleştiremez.

3.4 Veri ve Teknoloji Kısıtlamaları

Hukuki yetkilerin bulunduğu durumlarda dahi, **teknik sınırlamalar** uygulamaları yavaşlatmaktadır. ETBİS, MERSİS, PGDBİS ve TAREKS gibi mevcut sistemler değerli veriler içermekle birlikte, çapraz işlevli iş birliği eksikliği nedeniyle tam kullanılamamaktadır. Örneğin:

- ETBİS, kayıtlı e-ticaret işletmeleri hakkında bilgi sağlamakta, ancak denetim kayıtlarıyla doğrudan entegre olmamaktadır.
- MERSİS, işletme kayıtlarını takip etmekte, ancak ürün listeleriyle otomatik olarak eşleştirememektedir.
- PGDBİS, ürün güvenliği verilerini içermekte, ancak e-platformlardaki ürün ilan bilgilerine otomatik bağlantıları bulunmamaktadır.

Bu sistemler henüz birbirine bağlı olmadığından, denetçilerin verileri manuel olarak çapraz kontrol etmesi gerekmekte, bu da iş yükünü artırarak müdahaleleri geciktirmektedir. Ayrıca, mevcut izleme



Funded by
the European Union

süreci - kısıtlanmış terimleri, eksik güvenlik uyarılarını veya yüksek riskli ürün kategorilerini gerçek zamanlı olarak tespit edebilecek algoritmalar gibi –**otomatik ürün tarama araçlarından yoksundur.**

Bu, Türkiye'nin e-PGD faaliyetlerinin **proaktif değil reaktif** olduğu, sürekli gözetim yerine belirlenmiş dönemsel tespitlere dayandığı anlamına gelir. Yüksek hacimli, hızlı hareket eden bir dijital pazar için bu yaklaşım, tüketici korumasında önemli boşluklar bırakmaktadır.

3.5 İnsan Kaynakları Açığı

Etkili bir e-PGD, geleneksel denetim uzmanlığını dijital yetkinliklerle birleştiren **yeni bir beceri seti** gerektirir. İhtiyaç Analizi, birçok denetçinin fiziksel denetimlerde son derece yetkin olduğunu, ancak aşağıdaki konularda sınırlı eğitim aldığını ortaya koymuştur:

- Dijital soruşturma teknikleri (ör. çevrimiçi satıcı takibi, IP analizi).
- Trend ve risk tespiti için veri analizi.
- Otomatik izleme araçlarının ve yapay zeka destekli taramanın kullanımı.

Kapasite eksiklikleri, kaynakların daha sınırlı olduğu ve personelin genellikle birbiriyle çelişen taleplerle karşı karşıya kaldığı **taşra düzeyinde** özellikle belirgindir. Hedefli bir eğitim planı ve özel dijital PGD rolleri olmadan, çevrimiçi riskleri belirleme ve bunlara müdahale etme yeteneği sınırlı kalacaktır.

3.6 AB Uyum Etkenleri: GÜGT ve DSA

AB Genel Ürün Güvenliği Tüzüğü (2023/988) ve **Dijital Hizmetler Yasası (2022/2065)**, çevrimiçi pazar yerlerinin nasıl çalıştığı ve yetkili paydaşlarla nasıl iş birliği yaptığına ilişkin beklentileri önemli ölçüde artırmaktadır. GÜGT kapsamında, platformlar şunları yapmalıdır:

- Bildirildikten sonra güvenli olmayan ürünleri hızlı bir şekilde kaldırmak.
- Ürünlerin ve satıcıların izlenebilirliğini sağlamak.
- Yapılandırılmış, güvenli veri paylaşımı yoluyla PGDK'larla iş birliği yapmak.

DSA, çevrimiçi araçlardan **gerekli özeni göstermeleri, risk değerlendirmeleri yapmaları ve şeffaflık prensibi kapsamında raporlama sunmalarını** talep ederek bu yükümlülükleri güçlendirmektedir. Türkiye için bu gerekliliklere uyum sağlamak, sadece AB'ye katılım yükümlülüğü değil, aynı zamanda ulusal uygulamanın çevrimiçi ticaretin hızına ve ölçeğine ayak uydurabilmesini sağlamak için **pratik bir gerekliliktir.**

3.7 Paydaşlar

Başarılı bir e-PGD sistemi, çeşitli aktörler arasında koordineli eyleme bağlıdır:

- **Ticaret Bakanlığı (TB)** - Politika oluşturma, yasal reform ve kurumlar arası koordinasyonu sağlamakta; önemli ulusal uygulama sistemlerini yürütmektedir.
- **Piyasa Gözetim ve Denetim Kuruluşları (PGDK'lar)** – Sorumlulukları altındaki sektörler itibarıyla ürün mevzuatlarının uyumlaştırma çalışmalarını ve uygulamalarını yürütmekte ve e-PGD için net yetkiye ihtiyaç duymaktadır.
- **PGDKK** - Ticaret Bakanlığı'nın başkanlığında, kurumlar arası stratejileri koordine etmekte; e-PGD'ye özgü riskleri ele almak için kapasitesinin artırılması gerekmektedir.



Funded by
the European Union

- **Çevrimiçi platformlar** - E-ticaretin bekçileri olup; ürün güvenliği ve mevzuata uygunluğu sağlamak için proaktif ortaklar haline gelmelidir.
- **Tüketici örgütleri** - Şikayetler yoluyla risk istihbaratı toplamak ve kamuoyunun farkındalığını artırmak için gereklidir.

3.8 Neden Acil Eylem Gerekliyor?

E-ticaret, onu düzenlemek için tasarlanmış sistemlerden daha hızlı büyümektedir. Kararlı şekilde faaliyete geçilmezse:

- Uygun ve/veya güvenli olmayan ürünler, mevcut uygulama boşluklarından geçmeye devam edecektir.
- Tüketicilerin çevrimiçi pazar yerlerine olan güveni azalacaktır.
- Türkiye'nin AB standartlarına uyum sağlama yeteneği gecikecek ve bu durum pazar erişimi ve üyelik sürecine olumsuz etkiler yapacaktır.

SAPR, bu aciliyete yanıt olarak, yasal, teknik, kurumsal ve beşeri kapasite boyutlarında **kapsamlı ve takvimlendirilmiş bir dizi reform** planlayarak Türkiye'nin PGD sisteminin **dijital çağda** amacına uygun olmasını sağlamaktadır.





Funded by
the European Union

4 SAPR METODOLOJİSİ

Türkiye'nin e-PGD faaliyetleri için **Strateji ve Eylem Planı Raporu'nu (SAPR)** tasarlamak, teknik bir kontrol listesinden daha fazlasını gerektirmiştir. Hukuki boşluklar, kurumsal parçalanmışlık, teknolojik kısıtlamalar ve değişen piyasa dinamikleri gibi karmaşık bir dizi zorluğu **tutarlı ve uygulanabilir bir yol haritasına** dönüştürebilecek, **dikkatle aşamalandırılmış bir süreç** gerektirmiştir.

Metodoloji, **üç genel ilke** etrafında oluşturulmuştur:

1. **Kapsamlılık** - mevzuat ve kurumlardan IT araçları, beşeri kapasite ve kamu bilincine kadar e-PGD ekosisteminin her unsurunu kapsamak.
2. **Kanıt temelli tasarım** - önerileri verilere, yasal analizlere ve yaşanmış operasyonel deneyimlere dayandırmak.
3. **Paydaşların sahiplenmesi** - stratejiyi uygulamakla yükümlü olanların stratejinin şekillendirilmesine katkıda bulunmalarını mümkün kılarak, stratejinin gerçekçi ve siyasi açıdan sürdürülebilir olmasını sağlamak.

Bu yaklaşım, **e-PGD'nin geleneksel denetimin basit bir uzantısı olmadığını kabul etmekte olup**, araçlar, süreçler ve kültürde **bir dönüşüm anlamına geldiğini**, ancak hassas bir şekilde planlanması ve sahipliğin açıkça tanımlanması durumunda başarılı olabileceğinin önemini vurgulamaktadır.

4.1 Sağlam Bir Doğrulama Zemini Oluşturmak

İlk metodolojik adım, **mevcut durumu** derinlemesine **anlamak olmuştur**. Bu nedenle SAPR, her bir kaynağın birbirini tamamlayan bilgiler sağladığı çok katmanlı doğrulama temeline dayanmaktadır.

İhtiyaç Analizi Raporu (NAR)

NAR, dijital çağda Türkiye'nin PGD sistemine ilişkin en kapsamlı değerlendirmeyi sunmuştur. E-PGD ile ilgili yasal çerçeveyi, kurumsal yapıları, denetim uygulamalarını, IT kapasitelerini ve beşeri kaynakları ayrıntılı olarak incelemiştir.

Örneğin,

- ETBİS, MERSİS, PGDBİS ve TAREKS'in **entegre bir ekosistem olarak değil, paralel olarak** nasıl çalıştığını haritalandırarak, eşgüdümlü çalışabilirliğin gerekliliğini vurgulamıştır.
- **Belirli yasal boşlukları** (örneğin, gizli çevrimiçi denetimler için net bir yetki olmaması) ve bunun operasyonel erişim üzerindeki sonuçlarını belgelemiştir.
- Sektörler arası yürütülen e-PGD vakaları için görev dağılımının belirsizliği dahil olmak üzere **kurumsal darboğazları** belirlemiştir.

İhtiyaç Analizi Çalıştayı

Çalıştay, tespit edilen temel bulguların **doğruluğunun teyidi** işlevi görmüştür. Çalıştay, Ticaret Bakanlığı, sektörel PGDK'lar, e-platformlar ve tüketici örgütlerinden temsilcileri bir araya getirerek, paydaşlara aşağıda yer verilen çalışmalarını yürütme imkanı sağlamıştır:

- İhtiyaç Analizi Raporunun sonuçlarını **onaylamak veya sorgulamak**.
- **Zorlukları öncelik sırasına koymak** – örneğin, belirli önlemler için IT entegrasyonu mu yoksa yasal reform mu öncelikli olmalı kararını vermek.



Funded by
the European Union

- Anonim satıcıları takip etmekten dijital kanıtları korumaya kadar, denetçilerin karşılaştığı **pratik engelleri** çevrimiçi olarak paylaşmak.

Çalıştay ile sadece bir doğrulama yapılmamış; potansiyel çözümlerin şekillenmeye başladığı bir **ortak alan yaratılmıştır**.

Hukuki Analiz

Bu çalışma, Türkiye'nin yasal çerçevesini AB'nin **Genel Ürün Güvenliği Tüzüğü (GÜGT)** ve **Dijital Hizmetler Yasası (DSA)** ile karşılaştırmaya odaklanmıştır. İnceleme:

- Türkiye'nin mevzuatıyla ilgili **olabilecek tüm maddeleri** haritalandırarak kısmi veya tam uyumsuzlukları belirlemiştir.
- **Operasyonel gereklilikler** belirlenmiştir - örneğin, platform verilerini merkezi bir e-PGD IT aracına entegre etme yeteneği, platformları bu tür verileri paylaşmaya zorunlu kılan yasal hükümlere bağlıdır.
- Daha geniş bir dönüşümü mümkün kılacak, **hızlı sonuç veren reformlara** ⁽¹⁾ öncelik verilmiştir.

Uluslararası ve AB En İyi Uygulama Örneklerinin İncelenmesi

Son olarak, metodoloji dışı dönük bir yaklaşım benimsemiş ve AB üye ülkeleri de dahil olmak üzere diğer ülkelerin yetki bölgelerinde **dijital öncelikli PGD sistemlerinin** nasıl kurulduğunu incelemiştir. Bu çalışma, çözümleri doğrudan veya bütünüyle almakla ilgili olmayıp, **başka ülkelere uygulanan örneklerden etkili olanlarının tespit edilerek Türkiye'nin kurumsal ve yasal ortamına uyarlamakla** ilgili bir bakış açısı taşımaktadır. İncelenen örnekler arasında yer alanlar aşağıda sunulmaktadır:

- Anahtar kelimeler, görseller veya satıcı geçmişine dayalı olarak riskli ürünleri tespit eden otomatik ürün ilan tarayıcıları.
- Yetkililer ve büyük platformlar arasında, net veri formatları ve yanıt süreleri içeren yapılandırılmış iş birliği anlaşmaları.
- Tüketici şikayetleri, pazar verileri ve sınır ötesi uyarıları birleştiren ulusal risk puanlama modelleri.

4.2 Derin ve Kapsayıcı Paydaş Katılımı

E-PGD faaliyetleri ortak bir sorumluluk gerektirdiğinden, SAPR'nin güvenilirliği ekosistemdeki her aktörün katılımına bağlıdır. Bu nedenle, paydaş katılım süreci tek bir danışma aşamasıyla sınırlı kalmayıp, **sürekli ve çok katmanlı bir süreç** olarak yürütülmüştür.

- **Kurumsal paydaşlar** (Ticaret Bakanlığı ve PGDK'lar) hem stratejik tartışmalar hem de teknik çalışma grupları aracılığıyla sürece dahil edilmiş, böylece üst düzey politika uyumu ve operasyonel uygulanabilirlik sağlanması hedeflenmiştir.

¹ E-PGD için müfettişlerin atanması, bunların eğitimi, net SİP'ler, kılavuz belgeler vb. gibi nispeten hızlı ve minimum maliyetle gerçekleştirilebilecek reformlar



Funded by
the European Union

- **İktisadi İşletmeciler** (çevrimiçi platformlar, imalatçılar, endüstri dernekleri, lojistik sağlayıcılar), ürün ilanlarının nasıl listelendiği, ürünlerin nasıl tanıtıldığı ve ürünlerin tüketiciye nasıl teslim edildiği konusunda pratik bilgiler sağlamış; bu bilgiler, gerçekçi veri paylaşım protokolleri tasarlamak için büyük önem arz etmiştir.
- **Tüketici örgütleri**, şikayetlerin ele alınması süreçlerinin ve farkındalık kampanyalarının gerçek güvenlik endişelerini ele almasını sağlayarak **kamuoyunun bakış açısını** ortaya koymuştur.

Katılım yöntemleri, gerekli girdinin niteliğine uygun olarak çeşitlendirilmiştir:

- **İkili toplantılar**, hassas veya kuruma özgü konuların derinlemesine incelenmesine olanak sağlamıştır.
- **Tematik atölye çalışmaları**, katılımcıları konuya göre gruplandırarak (yasal reform, IT sistemleri veya risk temelli gözetim) odaklanmış ve teknik tartışmaları teşvik etmiştir.
- Önerilen taslak metinler üzerine yapılan **tekrarlı geri bildirimlerle**, paydaşların nihai plana sadece tepki vermekle kalmayıp, onu şekillendirebilmelerini sağlamıştır.

Bu yaklaşım, SAPR'nin önerilerinin kesinleşmeden önce **gerçek dünyadaki kısıtlamalara karşı stres testine tabi** tutulduğu anlamına gelmektedir.

4.3 Analitik Süreç: Sorundan Eyleme

Metodolojinin merkezinde, önerilerin hem hedefe yönelik hem de uygulanabilir olmasını sağlayan **problemden çözüme doğru ilerleme mantığı** bulunmaktadır.

1. Sorunun **teşhis edilmesi** - İAR bulguları, atölye tartışmaları ve yasal incelemelerin kullanılması.
2. Stratejik hedefin **tanımlanması** - sorunlu alan için istenen nihai durumun belirlenmesi.
3. Potansiyel önlemlerin **tasarlanması** - uluslararası modellerden yararlanılarak bunların Türkiye'ye uyarlanması.
4. **Fizibilitenin test edilmesi** - yasal, kurumsal, teknik ve finansal gerçeklerin göz önünde bulundurulması.
5. Eylemlerin doğru sırayla **sıralanması** - bazı önlemlerin diğerlerini tetiklediğinin kabul edilmesi (örneğin, IT sistemlerini entegre etmeden önce bir platform veri paylaşımı yasasını kabul edilmesi gibi).
6. Sorumlulukların net bir şekilde **belirlenmesi** - her eylem için öncü ve destekleyici kurumların belirlenmesi.
7. Ölçülebilir çıktıların **belirlenmesi** - ilerlemenin izlenebilmesinin ve değerlendirilebilmesinin sağlanması.

Adım adım bu süreç, SAPR'nin sadece bir strateji olarak değil, aynı zamanda **pratik bir çalışma planı** olarak da işlev görmesini sağlamaktadır.

4.4 Varsayımları, Kısıtlamaları ve Bağlantılı İlişkileri Yönetme

Metodoloji, uygulamayı etkileyebilecek faktörleri açıkça ele almaktadır:

Varsayımlar;

- E-PGD reformuna yönelik siyasi taahhüt sürdürülecektir.
- Yasal çerçeveler oluşturulduktan sonra e-platformlar yapıcı bir şekilde devreye girecektir.



Funded by
the European Union

- IT, eğitim ve kamuoyunun katılımı için yeterli bütçe kaynakları ayrılacaktır.

Kısıtlamalar;

- PGDK'lar arasında teknik hazırlık düzeylerinde farklılıklar.
- Yasa tasarısı hazırlama ve parlamento onayı süreçlerinde olası gecikmeler.
- Özellikle yabancı e-platformlardan veri paylaşma istekliliğinde farklılıklar.

Çapraz Bağlantılar;

- E-PGD IT platformu, veri alışverişi ve dijital kanıt kullanımı için yasal yetkilere bağlıdır.
- Risk temelli gözetim, şikayetler, e-platformlar ve sınır ötesi ürün güvenliği uyarı ağlarından elde edilen verilerin birleştirilmesini gerektirir.
- Kamuoyunun farkındalığı, görünür uygulama başarılarıyla birlikte başlatıldığında etkili olacaktır.

4.5 Yol Gösterici Metodolojik İlkeler

SAPR'nin hazırlanma süreci, hem iddialı hem de uygulanabilir bir çerçeve sunacak ilkelere dayandırılmıştır:

1. **Kanıt dayalı yaklaşım** - gerçeklere veya analitik temele dayanmayan hiçbir öneri yapılmamıştır.
2. **AB müktesebatı ile uyum** - her önlem GÜGT ve DSA yükümlülüklerinin yerine getirilmesine katkı sağlamaktadır.
3. **Operasyonel gerçekçilik** - öneriler mevcut kurumsal yapıları ve kaynak seviyelerini dikkate almaktadır.
4. **Geleceğe hazırlık** – Yapay zeka destekli ilan oluşturma veya çapraz platform satıcı ağları gibi teknolojik ve piyasa değişikliklerini öngörmektedir.

4.6 Metodolojinin Sonucu

Bu sistematik yaklaşımın sonucu, **ilk günden itibaren uygulanabilir bir Eylem Planı olmuştur**. Plan, kısa vadeli “hızlı kazanım” reformlarını uzun vadeli kapasite geliştirme adımlarıyla dengelemekte, darboğazlardan kaçınmak için eylemleri mantıklı bir sıraya koymakta ve sorumlulukları net biçimde tanımlamaktadır. En önemlisi, paydaşların ortak katkısıyla tasarlanmış bir ürün olmasıdır – bu da uygulamada sahiplenilme ve taahhüt düzeyini önemli ölçüde artırmaktadır.



Funded by
the European Union

5 HUKUKİ UYUMLAŞTIRMA (1. BİLEŞEN)

5.1 E-PGD’de Hukukun Merkezi Rolü

PGD bir kamu görevidir. Denetçiler, analistler ve yaptırım organları, ancak **açık ve uygulanabilir yasal yetkilere** sahip olduklarında ve iktisadi işletmecilerin uymaları gereken **açık ve bağlayıcı yükümlülükler bulunduğunda** tüketicileri korumak için harekete geçebilirler.

Geleneksel piyasalarda, bu yasal yetkiler uzun zamandır yerleşiktir: denetçiler mağazaları ziyaret edebilir, güvenli olmayan ürünlere el koyabilir, geri çağırma emri verebilir ve uygunsuz davranan imalatçıları veya dağıtıcıları cezalandırabilir. Ancak, **sınır tanımayan ve hızla değişen e-ticaret dünyasında**, bu yetkilerin çoğu **kendiliğinden karşılık bulmamaktadır**.

Fiziksel bir mağazada satılan güvenli olmayan bir çocuk oyuncakı denetim için elverişlidir - incelenebilir, test edilebilir ve piyasadan toplatılabilir. Aynı oyuncak, çevrimiçi ortamda farklı şekillerde, farklı e-platformlarda, muhtemelen yurtdışında bulunan platformlarda birden çok kez ortadan kaybolup yeniden ortaya çıkabilir. Şayet mevzuat, e-platformların güvenli olmayan ürünleri önlemesini, tespit etmesini ve kaldırmasını **açıkça gerektirmiyorsa** veya **denetçilere gizli çevrimiçi soruşturmalar yürütme yetkisi vermiyorsa**, uygulama yetkililerin nadiren kazandığı bir "saklambaç" oyununa dönüşür.

Bu nedenle, **1. Bileşen – Hukuki Uyumlaştırma**, SAPR'nin diğer tüm bileşenlerinin dayandığı temel oluşturur. Bu bileşen olmadan:

- 2. Bileşen'in IT sistemleri, ihtiyaç duydukları verilere yasal olarak erişemeyecektir.
- 3. Bileşen'in risk temelli analitiğine kritik girdiler sağlanamayacaktır.
- 4. Bileşen kapsamındaki kurumsal iş birliği, tanımlanmış sorumluluklar ve veri paylaşımı görevleri olmadan durma noktasına gelecektir.

Hukuki reform, sadece AB üyeliği için bir uyum çalışması olmayıp, dijital piyasalar açısından **tamamen yeni bir uygulama modelinin hayata geçirilmesini sağlayan** bir unsurdur.

5.2 AB GÜGT ve DSA: Türkiye için Neden Önemlidir?

Avrupa'da e-PGD'yi şekillendiren iki AB yasal aracı bulunmaktadır: **Genel Ürün Güvenliği Tüzüğü (GÜGT)** ve **Dijital Hizmetler Yasası (DSA)**.

Bu iki düzenleme, düzenleyici yaklaşımı **reaktif uygulamadan proaktif gözetim anlayışına kaydırmakta** ve yetkililer ile çevrimiçi araçlar arasında **paylaşılan sorumluluk ilkesini yerleştirmektedir**.

GÜGT kapsamında:

- Çevrimiçi pazar yerleri, bildirildikten sonra güvenli olmayan **ürünleri kaldırmak** için hızlı bir şekilde (bazen 2 iş günü içinde) harekete geçmelidir.
- Satıcıların ve ürünlerin **izlenebilirliğini** sağlamalıdır, böylece yetkililer sorumlu iktisadi işletmecilere ulaşabilmektedir.



Funded by
the European Union

- **Yapılandırılmış, güvenli ve zamanında veri paylaşım mekanizmaları** aracılığıyla iş birliği yapmakla yükümlüdür.

DSA kapsamında:

- Platformlar **risk değerlendirmeleri** yapmalı ve tüketici güvenliğine yönelik riskleri azaltmak için önlemler almalıdır.
- Büyük platformlar, içerik denetimi ve ürün ilanlarını kaldırma konusunda düzenli olarak kamuya raporlama yapmak da dahil olmak üzere, **daha ileri şeffaflık gerekliliklerine** tabidir.

Türkiye açısından, bu yükümlülüklerle uyum sağlamak iki sonucu beraberinde getirmektedir:

1. AB'ye katılımın temel şartlarını yerine getirmek.
2. Ulusal sistemine, dijital ticaretin hızına, ölçeğine ve karmaşıklığına uygun **modern uygulama araçları kazandırmak.**

5.3 Yasal Boşluklar ve Gerçek Uygulamalara Etkileri

İhtiyaç Analizi ve hedefli hukuki analiz, Türkiye'nin ürün güvenliği mevzuatının (7223 sayılı Kanun) fiziksel piyasalarda güçlü olmasına rağmen, AB'de standart olan **çevrimiçi ortama özgü bazı yetki ve yükümlülüklerden yoksun olduğunu** ortaya koymuştur.

Boşluk 1 – Sınırlı platform yükümlülükleri

Mevcut durumda, Türkiye'deki çevrimiçi pazar yerleri için aşağıdaki hususlarda yasal bir zorunluluk bulunmamaktadır:

- Ürün ilanı yayına girmeden önce ürün uygunluğunu doğrulamak.
- Daha önce benzer ilanlarda güvensiz olduğu tespit edilen ürünleri proaktif şekilde kaldırmak.
- Satıcı ve ürün verilerini yetkililerle standart formatta ve yapılandırılmış biçimde paylaşmak.

Bu durum, güvenli olmayan ürünler tespit edildiğinde bile, **birkaç gün içinde yeni ilanlar altında yeniden ortaya çıkabilecekleri** anlamına gelmektedir.

Boşluk 2 – Gizli çevrimiçi denetimler için net bir yetki yok

Gizli satın alma (test için çevrimiçi ürün satın alma) mevzuatta açıkça düzenlenmemiştir. Bu yasal dayanak olmadan:

- Yetkililer, açılacak yaptırım davalarına **usul yönünden itiraz edilmesi** riskiyle karşı karşıyadır.
- Denetçiler, gizli uyumsuzlukları tespit etmek için gizli olarak güvenle hareket edemeyecektir.

Boşluk 3 – Dijital kanıtlar için zayıf yasal dayanak

Çevrimiçi denetimler genellikle ekran görüntüleri, ürün sayfası kayıtları veya işlem belgelerine dayanmaktadır. Ancak, bu tür kanıtların nasıl toplanacağı, saklanacağı ve doğrulanacağına ilişkin net bir yasal çerçeve olmadan, delillerin **mahkemede geçerliliğinin sorgulanmasına** yol açabilmektedir.

Boşluk 4 – Sınır ötesi iş birliği yetkilerinin kısıtlı olması

Satıcının yurtdışında bulunması durumunda, mevcut mevzuat -söz konusu satıcı Türk pazarına tekrar tekrar güvenli olmayan ürünler arz etse bile- yabancı denetim kuruluşlarıyla **gerçek zamanlı veri alışverişi** için güçlü ve hızlı müdahale mekanizmaları sunmamaktadır.



Funded by
the European Union

Boşluk 5 – IT sistemlerinin eşgüdümlü çalışabilirliği için açık bir çerçeve bulunmaması

ETBİS, MERSİS, PGDBİS, TAREKS gibi mevcut sistemler değerli verileri barındırsa da, mevzuat bu verilerin e-PGD'de otomatik ve entegre bir şekilde kullanılması için erişim haklarını, veri akışlarını ve güvenlik önlemlerini tam olarak tanımlamamaktadır.

5.4 1. Bileşen için Reform Vizyonu

1. Bileşen kapsamındaki hukuki uyumlaştırma aşağıdaki amaçlarla tasarlanmıştır:

- Türkiye'nin e-PGD mevzuatını GÜGT ve DSA gerekliliklerinin ilgili maddeleriyle **tam olarak uyumlu hale getirmek**.
- PGDK'ları dijital öncelikli modern denetim yetkileri ile donatmak.
- Sistem entegrasyonu, veri paylaşımı ve uluslararası iş birliği için hukuki altyapıyı **oluşturmak**.

Bu yalnızca “kanun metnini değiştirmek” değil, piyasa gözetiminin **yetki kapsamını dönüştürmek** anlamına gelmektedir. Doğru hükümler devreye alındığında denetçiler:

- Satıcı kimlikleri, satış hacimleri ve işaretlenmiş yüksek riskli ilanları gösteren platformlardan otomatik veri akışları alabilecek,
- Sonuçların mahkemede geçerli olacağını bilerek, yasal olarak gizli satın alma uygulamaları gerçekleştirebilecek,
- Ortaya çıktıkları gün acil güvenlik uyarılarını yabancı denetim kuruluşlarıyla paylaşabilecektir.

5.5 Öncelikli Yasal İşlemler

İhtiyaç Analizi Raporu'nun bulgularına dayanarak, SAPR **aşamalı bir reform paketi** önermektedir:

1. 7223 sayılı Kanunda değişiklik yapılması:

- Çevrim içi platformlara, uygunluğu doğrulama ve güvensiz ilanları tanımlanmış süreler içinde kaldırma yönünde açık yükümlülükler getirilmesi.
- AB modellerine paralel olarak, uyulmaması durumunda ciroya dayalı orantılı para cezaları uygulanması.
- Satıcı/ürün verilerinin yetkililerle yapılandırılmış ve standart formatta paylaşılmasının zorunlu hale getirilmesi.

2. Gizli dijital denetimlerin yasal **zemin kazanması**:

- E-ticarete gizli satın almanın (mystery shopping) kapsamı, güvenceleri ve delil geçerliliği kurallarının tanımlanması.
- Denetçilere, satıcılara önceden bildirim yapılmaksızın normal tüketici gibi hareket etme imkânı tanınması.

3. **Dijital kanıtlar için yasal bir çerçeve oluşturulması**:

- Kabul edilebilir formatların (ekran görüntüleri, loglar, işlem verileri) ve metadata gereksinimlerinin belirlenmesi ve kanıt olarak kabul edilmesi.
- Kurumlar arasında saklama ve doğrulama süreçlerinin standartlaştırılması.

4. **Platform veri paylaşım protokolleri için yasal düzenlemeler yapılması**:



Funded by
the European Union

- Platformların PGDK'lara gerçek zamanlı veya periyodik veri akışı sağlamasının zorunlu hale getirilmesi.
 - Türkiye'ye satış yapan hem yerli hem de yabancı platformların kapsama alınması.
5. **Sınır ötesi yaptırım iş birliğinin mümkün kılınması:**
- AB ve AB dışı düzenleyicilerle hızlı uyarı ve kanıt paylaşımı yetkilerinin sağlanması.
 - Sınır ötesi ürün güvenliği uyarı ağlarına** katılım için hazırlık yapılması.

5.6 Ön Koşullar ve Sıralama

Yasal önlemler, teknik gelişmelerden **önce** veya **bunlarla eşzamanlı olarak** hayata geçirilmelidir. Örneğin:

- Platform verilerine erişim için yasal yetki olmadan, 2. Bileşen kapsamındaki IT araçları ihtiyaç duydukları girdilere sahip olamayacaktır.
- Dijital kanıtların kabul edilebilirliğine dair kurallar olmadan, 3. Bileşen kapsamındaki risk temelli denetimlerin mahkemede kullanım gücü zayıflayacaktır.

Bu nedenle, SAPR uygulamasının **ilk 12-18 ayında**, 2-6. Bileşenlerin gecikme olmadan ilerleyebilmesi için temel yasal reformların kabulüne öncelik verilmelidir.

5.7 Riskler ve Azaltım Önlemleri

Platform yükümlülükleri ve veri alışverişi gibi hassas alanlarda yasal reformlar dirençle karşılaşılabılır. Riskleri azaltmak için:

- AB uyumunun faydalarına dair uzlaşma sağlanabilmesi için kanun yapıcılarının erken aşamada sürece dahil edilmesi,
- Yükümlülükleri netleştirmek ve uygulama sürtüşmelerini azaltmak için taslak hazırlama aşamasında platformlarla istişareler yapılması,
- Veri koruma ve rekabetle ilgili endişeleri gidermek için mevzuata şeffaflık ve adil yargılama güvencelerinin eklenmesi.

5.8 1. Bileşen'in Beklenen Etkisi

1. Bileşen reformları yürürlüğe girdiğinde Türkiye:

- Modern e-ticaret risklerini yönetebilecek **GÜGT/DSA uyumlu bir yasal çerçeveye** sahip olacaktır.
- Yetkililere **dijital öncelikli uygulama yetkileri** verilmesi sağlanmış olacaktır.
- SAPR'nin geri kalanındaki teknik, analitik, kurumsal ve kamuya yönelik reformlar için yasal temeller oluşturulmuş olacaktır.

Özetle, 1. Bileşen Türkiye'yi **e-ticarete reaktif uygulamadan proaktif, önleyici ve teknoloji destekli bir modele** taşıyacak; bu model tüketicileri daha etkili bir şekilde korurken, ülkeyi AB'nin ürün güvenliği ekosisteminde aktif ve güvenilir bir katılımcı olarak konumlandıracaktır.



Funded by
the European Union

6 IT ARACI GELİŞTİRME VE ENTEGRASYON (2. BİLEŞEN)

6.1 Dijital Araçlar Neden Artık İsteğe Bağlı Değil?

Fiziksel piyasalarda, bir denetçi bir mağazaya girip rafları tarayabilir, bir ürünü eline alarak o anda test edilip edilmemesi veya piyasadan çekilmesi gerektiğine karar verebilir. Çevrimiçi piyasalarda ise **teknoloji olmadan bu kararlara varmak imkansızdır**.

Türkiye'deki tek bir büyük e-ticaret platformu bile, binlerce satıcı tarafından sürekli güncellenen **milyonlarca aktif ürün ilanına ev sahipliği yapabilmektedir**. Bu listeler statik değildir - isimleri, resimleri ve açıklamaları değişir; kaybolup yeniden ortaya çıkabilirler; üstelik çoğu fiziksel denetimlerin erişimi dışında kalan yurtdışı merkezli satıcılar tarafından sunulabilmektedir.

Türkiye'nin PGDK'ları bu ekosistemi manuel olarak izlemeye çalışırsa, her zaman birkaç **adım geride** kalacaktır. Bir denetçi çevrimiçi piyasada tehlikeli bir oyuncuğu tespit edene kadar, o ürün yüzlerce kez satın alınmış veya yeni bir satıcı adı altında yeniden ilana çıkmış olabilir.

2. Bileşen bu gerçeği kabul etmektedir: **E-ticarette ürün güvenliği mücadelesi, aslında bir veri mücadelesidir**. Bu mücadeleyi kazanmak için, yetkililerin dijital pazarı gerçek zamanlı olarak görebilen, riskleri anında işaretleyebilen ve denetçilere doğrudan eyleme geçirilebilir istihbarat sağlayabilen **merkezi, teknoloji destekli bir araca** ihtiyacı vardır.

6.2 Mevcut Durum: Değerli Sistemler, Ancak İzole Yapılar Devam Ediyor

Türkiye, e-ticaret pazarının denetimini destekleyebilecek birkaç gelişmiş dijital sisteme sahiptir:

- **ETBİS** - E-ticaret işletmelerini kaydeder ve faaliyetlerinin niteliği ve sektör sınıflandırması dahil olmak üzere temel operasyonel verileri toplar.
- **MERSİS** - Mülkiyet ve kurumsal geçmiş dahil olmak üzere resmi ticaret sicil bilgilerini depolar.
- **PGDBİS** - Denetim sonuçlarını, uygunsuzluk kayıtlarını ve ürün güvenliği bilgilerini saklar.
- **TAREKS** - Risk temelli bir yaklaşım kullanarak ithalatı güvenlik riskleri açısından tarar.

Bu sistemlerin her biri, **yapbozun bir parçasını** oluşturmaktadır. Sorun, bu sistemlerin **proaktif ve çevrimiçi gözetimi destekleyecek şekilde birbirine bağlı olmamasıdır**. Şüpheli bir ilanı çevrimiçi olarak tespit eden bir denetçi bugün şu adımları izlemek zorundadır:

1. ETBİS'i kontrol ederek satıcının kayıtlı olup olmadığını görmek.
2. MERSİS'te sahiplik ayrıntılarını aramak.
3. PGDBİS'i inceleyerek ürünün veya satıcının uygunluk geçmişini kontrol etmek.
4. Muhtemelen TAREKS'i ithalatla ilgili riskler için kontrol etmek.

Bu manuel ve çoklu sistemli süreç yavaş ve verimsizdir. Daha da önemlisi, **otomatik bir "erken uyarı" sisteminin mümkün olmamasıdır** – çünkü sistemler birbirleriyle gerçek zamanlı olarak "iletişim kurmamaktadır".



Funded by
the European Union

6.3 Vizyon: Birleşik bir e-PGD IT Platformu

2. Bileşen, Türkiye'nin modernize edilmiş PGD sisteminin **dijital omurgasını** oluşturacak **birleşik ve merkezi bir e-PGD IT platformunun** kurulmasını önermektedir. Bu platform:

- Ulusal veri tabanları, çevrimiçi pazar yerleri, tüketici şikayetleri ve sınır ötesi ürün güvenliği uyarı ağları gibi **çok sayıda kaynaktan veri alacaktır**.
- Otomatik kurallar ve gelişmiş analitik yöntemler kullanarak bu verileri **analiz edecek**.
- Risk eşikleri aşıldığında denetçileri **uyaracak**.
- İlk tespit aşamasından yaptırım ve takip aşamasına kadar vakaları **yönetecektir**.

Bu sadece iç kullanım için bir veri tabanı değil, günlük PGD için **canlı ve operasyonel bir araçtır**. Pratikte bu şu anlama gelmektedir:

- İthalat sırasında (TAREKS aracılığıyla) güvenli olmayan bir elektrikli cihaz tespit edilirse, platform çevrimiçi pazarlardaki **aynı veya benzer ürünün ilanlarını derhal işaretleyecek** ve tüketicilere zarar gelmeden kaldırılması için talep gönderecektir.
- Başka bir ülkede ürünün geri çağırılması kararı alınırsa (sınır ötesi uyarılar yoluyla), sistem **Türk platformlarında eşleşen ilanları arayacak** ve denetçilere acil uyarılar gönderecektir.
- Bir satıcı, uygun olmayan ürünleri tekrar tekrar listelerse, platform **bunları risk puanlama modelinde öncelikli hale getirerek** hedefli yaptırım uygulanmasını sağlayacaktır.

6.4 Temel İşlevler ve İşleyişi Nasıl Değiştirdikleri

Birleştirilmiş platformun birkaç temel modülü olacaktır:

1. Otomatik Pazar Yeri İzleme

- Günlük milyonlarca ilanı taramak için tarayıcılar (crawlers) ve yapay zeka tabanlı görsel tanıma kullanılacaktır.
- Anahtar kelimelere, görsel benzerliklere veya bilinen uygunsuzluk kalıplarına göre ürünleri işaretleyecektir.

Örnek: Bir tarayıcı, AB'de yasaklanmış bir oyuncak modelinin birden fazla listesini tespit eder; sistem denetçileri uyarır ve otomatik olarak platforma kaldırma talebi gönderir.

2. Platformlardan Gerçek Zamanlı Veri Akışı

- Bileşen 1 kapsamındaki yasal düzenlemeler sayesinde yapılandırılmış veri paylaşımı mümkün olacaktır.
- Veriler, satıcı kimliklerini, ürün açıklamalarını, uygunluk belgelerini ve satış rakamlarını içerecektir.
- Bu sayede denetimler düzensiz olmaktan çıkar ve **sürekli gözetim** yapılmasına olanak sağlanır.

3. Sistemler Arası Eşleştirme

- ETBİS kayıt verileri, MERSİS mülkiyet kayıtları, PGDBİS uygunluk geçmişi ve TAREKS ithalat verileri otomatik olarak ilişkilendirilecektir.

Örnek: Bir satıcının ithalat kayıtları tekrarlayan güvensiz sevkiyatlar gösterirse; sistem bu satıcının tüm çevrimiçi ilanları için risk puanını yükseltecektir.



Funded by
the European Union

4. Entegre Vaka Yönetimi

- Denetçiler, vakaları doğrudan platformda açabilecek, atayabilecek ve takip edebilecektir.
- Tüm eylemler (ör. denetimler, platform kaldırma talepleri, test sonuçları) tek bir yerde kaydedilecektir.

5. Dijital Kanıt Saklama

- Ekran görüntüleri, metadata ve işlem verileri otomatik olarak toplanacak ve yasal açıdan geçerli formatlarda saklanacaktır.
- Bu sayede delillerin idari ve yargısal süreçlerde bütünlüğü korunacaktır.

6.5 Eşgüdümlü Çalışabilirliği Gerçeğe Dönüştürmek

Gerçek eşgüdümlü çalışabilirlik, **verilerin sorunsuz bir şekilde taşınması** anlamına gelir. Yeni e-PGD Platformu, güvenli API'ler üzerine inşa edilerek aşağıdakileri sağlayacaktır:

- **ETBIS ↔ PGDBIS:** satıcı kimliğinin uygunluk geçmişiyle ilişkilendirilmesi.
- **TAREKS ↔ e-PGD Platformu:** riskli ithalat için çevrimiçi gözetim görevlerinin otomatik oluşturulması.
- **MERSİS ↔ e-PGD Platformu:** satıcılar için anında sahiplik doğrulaması sağlanması.
- **Platform API'leri ↔ e-PGD Platformu:** güncel ilan ve satış verilerinin kesintisiz aktarılması.

Ancak bu, teknik kodlamadan daha fazlasını gerektirir - aynı zamanda verilere kimin sahip olduğu, verileri kimin yönettiği ve eriştiğini tanımlamak için **hukuki netlik** (1. Bileşen) ve **kurumsal uzlaşılar** (4. Bileşen) da bağlıdır.

6.6 Geliştirme Aşamaları: Temellerden Tam Kapasiteye

Bu, çok kaynaklı ve karmaşık bir entegrasyon olduğu için SAPR, **aşamalı bir geliştirme süreci** önermektedir:

- **Aşama 1 – Temeller**
 - ETBIS, PGDBIS ve MERSİS'in birbirine bağlanması.
 - Denetçilerin yüksek riskli ilanları belirlemelerine yardımcı olmak için temel bir tarayıcının (crawler) kullanılması.
 - Manuel kanıt saklama işlevlerinin başlatılması.
- **Aşama 2 – Risk Puanlaması ve Yarı Otomasyon**
 - Bileşen 3'ün ulusal risk değerlendirme metodolojisinin platforma entegre edilmesi.
 - Yüksek riskli ürünler ve satıcılar için otomatik uyarıların üretilmeye başlanması.
 - Seçilen pazar yerleri ile API entegrasyonlarının pilot uygulanması.
- **Aşama 3 – Tam Otomasyon ve Uluslararası Bağlantı**
 - Gerçek zamanlı veri akışlarıyla tüm büyük platformlara genişletilmesi.
 - Anlık risk yayılımı için **uluslararası güvenlik uyarı ağlarına** bağlanması.
 - Ortaya çıkan yeni tehditlerin tespit edilmesi için AI destekli görüntü tanıma ve tahmine dayalı analitik kullanılması.



Funded by
the European Union

6.7 Diğer Temel Unsurlarla İlişkiler

Platform, ancak aşağıdaki koşullar yerine getirildiğinde tam potansiyeline ulaşabilecektir:

- **1. Bileşen**, platform verilerine erişim ve dijital kanıtların kullanımı için gerekli hukuki yetkileri sağlar.
- **Bileşen 3**, analitik modüllere entegre edilecek güçlü bir risk puanlama metodolojisi sunar.
- **Bileşen 4**, kurumların sistemi ortak kullanabilmesi için gerekli yetki ve koordinasyon mekanizmalarını güvence altına alır.
- **Bileşen 5**, denetçilerin platformu etkin biçimde kullanabilmesi için gerekli eğitimi sağlar.
- **6. Bileşen**, kamuya açık raporlama araçlarını kullanarak tüketici uyarılarını doğrudan sisteme aktarır.

6.8 Riskler ve Azaltım Önlemleri

- **Risk:** Veri paylaşımında platform iş birliğinin düşük olması.
- **Azaltma:** Bağlayıcı yasal yükümlülükler (1. Bileşen) ve aşamalı teknik entegrasyon.
- **Risk:** Etkili filtreleme olmadan aşırı veri yüklemesi.
- **Azaltma:** Yüksek öncelikli vakalara odaklanmak için risk temelli analitik (3. Bileşen).
- **Risk:** Kurumların iş akışlarını değiştirme konusunda isteksiz davranması.
- **Azaltma:** Erken paydaş katılımı, pilot projeler ve görünür hızlı kazanımlar.

6.9 Beklenen Dönüşüm

Birleşik e-PGD IT platformu faaliyete geçtiğinde, Türkiye’de **PGD’nin yürütülme şekli** köklü bir şekilde **değişecektir**. Yetkililer, tüketici şikayetlerine ve ad-hoc denetimlere tepki vermek yerine, **sürekli, ülke çapında ve istihbarat odaklı bir izleme sistemi** işletecektir. Güvenli olmayan ürünler daha hızlı tespit edilip piyasadan toplatılacak, tekrar eden ihlaller sistematik olarak tespit edilecek ve Türkiye, sınır ötesi güvenlik iş birliğine **eşit bir ortak** olarak yer alabilecektir.

Özetle 2. Bileşen, 1. Bileşen’in yasal yetkilerini **günlük operasyonel gerçekliğe** dönüştürmekte ve Türkiye’ye e-ticaretin hızına eşdeğer teknolojik kapasite kazandırmaktadır.



Funded by
the European Union

7 RİSK TEMELLİ GÖZETİM VE ANALİTİK (3. BİLEŞEN)

7.1 E-Ticarette Risk Temelli Gözetim Neden Vazgeçilmezdir?

Fiziksel piyasalarda, bir denetçinin günü, sektörler arasında dönüşümlü denetim, şikayet takibi ve uzman değerlendirmesinin birleşimine dayanarak seçilen az sayıda saha ziyareti etrafında planlanabilir. Karmaşık bir risk modeli olmasa bile, bir denetçi rafları tarayabilir ve test için ürünleri fiziksel olarak seçebilir. Ancak, e-ticaret bu denklemi tamamen değiştirmektedir. Tek bir büyük platform dahi:

- Herhangi bir anda on milyonlarca canlı ürün ilanını barındırabilir.
- Saatte binlerce ilan ekleyebilir veya güncelleyebilir.
- Satıcıların birden fazla hesapla faaliyet göstermesine ve bir gecede ortadan kaybolup yeni isimlerle yeniden ortaya çıkabilmelerini imkan tanıyabilir.

Bu ortamda, rastgele örnekleme veya şikayete dayalı denetimlere güvenmek, **bir kova ile denizi boşaltmaya çalışmak gibidir** - yüksek riskli ürünler fark edilmeden gözden kaçarken, değerli denetim zamanı düşük riskli, düşük öncelikli vakalarda boşa harcanır.

Bu nedenle, risk temelli gözetim sadece yurt dışından alınmış bir **en iyi uygulama değil** – e-PGD için **tek uygulanabilir yaklaşımdır**. Bu yöntem, denetimi **reaktif yangın söndürme** faaliyetlerinden **proaktif olarak önleme** faaliyetlerine dönüştürerek, sınırlı kaynakların **tüketici güvenliği üzerinde en yüksek etkiyi** yaratacak alanlarda kullanılması sağlanır.

7.2 Konseptten Uygulamaya: Ulusal Risk Değerlendirme Metodolojisi (URDM)

3. Bileşen'in merkezinde, Türkiye'nin e-ticaret yapısına uyarlanmış bir **Ulusal Risk Değerlendirme Metodolojisi (URDM)** oluşturulması yer almaktadır. Bu metodoloji, genel bir "öncelik listesi" değildir; ürünleri, satıcıları ve satış kanallarını, üzerinde uzlaşılan, şeffaf bir dizi risk faktörüne göre sürekli olarak değerlendiren, **veriye dayalı, yaşayan bir sistemdir**.

URDM şunları sağlayacaktır:

- **"Risk"i operasyonel terimlerle tanımlayacak:** tehlike potansiyeli, uygunluk geçmişi, satıcı davranışı ve piyasa bağlamını birleştirecektir.
- Tüm PGDK'ların, oyuncak, elektronik, kozmetik veya diğer ürün kurallarına tabi kategorileri denetlerken aynı mantığı uygulayabilmeleri için **standart bir puanlama çerçevesi oluşturmak**.
- **Mümkün olduğunda puanlamayı** (Bileşen 2) IT platformuna entegre ederek **otomatikleştirecek**; böylece yüksek riskli vakalar anında uygulama sırasının en üstüne çıkacaktır.

Bu ortak çerçeve, bir PGDK'nın önemseydiği bir vakayı diğerinin görmezden gelmesi gibi mevcut parçalanmışlığı sona erdirecek; **risk, kurumlar arasında ölçülebilir, karşılaştırılabilir ve şeffaf hale gelecektir**.



Funded by
the European Union

7.3 E-Ticaret Bağlamında Riski Tanımlama

E-PGD'de risk çok boyutludur. Değerlendirme yapılırken ürün, satıcı, pazar ve dış bilgi kaynakları birlikte dikkate alınmalıdır::

1. Ürüne Özgü Risk Faktörleri

- **İşsel tehlikeler:** boğulma, elektrik çarpması, yangınlık, kimyasal toksisite.
- **Ürün kategorisi hassasiyeti:** oyuncaklar, kozmetikler, elektrikli ürünler ve çocuk bakım ürünleri doğası gereği daha risklidir.
- **Uygunsuzluk geçmişi:** Türkiye'de veya yurtdışında yaşanmış test başarısızlıkları, geri çağırımlar veya yasaklar.

2. Satıcıya Özgü Risk Faktörleri

- **Uygunluk sicili:** Tekrar eden ihlalleri bulunan satıcılar risk açısından daha yüksek derecelendirilir.
- **Kuruluş ülkesi:** Türkiye veya AB dışındaki satıcılara yaptırım uygulamak daha zordur.
- **Satıcının şeffaflığı:** İletişim bilgilerinin olmaması, belirsiz açıklamalar veya eksik uygunluk belgeleri ciddi uyarı işaretleridir.

3. Piyasaya Özgü Risk Faktörleri

- **Platform özellikleri:** büyüklük, tür (pazar yeri mi perakendeci mi), PGDK'larla iş birliği geçmişi.
- **Mevsimsellik:** tatillerden önce oyuncak satışlarında, festivallerden önce kozmetik ürünlerinde, indirim dönemlerinde elektronik ürünlerinde artışlar.
- **Ürün yaşam döngüsü hızı:** hızlı moda ürünleri birkaç hafta içinde piyasadan kaybolabilir, bu nedenle erken tespit çok önemlidir.

4. Dış Kaynaklı İstihbarat

- **Sınır ötesi ürün güvenliği uyarı ağları:** AB, OECD veya diğer ticaret ortaklarından gelen bildirimler.
- **Tüketici şikayetleri:** tehlikeler resmi olarak tespit edilmeden önce erken uyarı göstergeleri.
- **Medya raporları:** viral hikayeler, yüksek zarara ve itibar kaybına yol açabilecek ürünleri gösterebilir.

7.4 Verileri Önceliklere Dönüştürmek: Risk Modeli Nasıl Çalışır?

URDM, faaliyete geçtikten sonra, ham verileri net bir süreç ile **uygulama öncelikleri** haline dönüştürecektir:

1. Veri Toplama

2. Bileşen'deki IT platformu otomatik olarak şu verileri içe aktarır:

- Bağlı platformlardan ürün ilanları.
- ETBIS'ten satıcı kayıt verileri ve MERSİS'ten sahiplik bilgileri.
- PGDBIS'ten uygunluk geçmişi.



Funded by
the European Union

- TAREKS'ten ithalat verileri.
- Sınır ötesi ürün güvenliği ağlarından gelen uyarılar.
- Resmi kanallardan gelen tüketici şikayetleri.

2. Risk Puanlaması

Her ürün veya satıcıya, ağırlıklandırılmış faktörlere göre sayısal bir puan verilir.

Örnek: Yabancı bir satıcıdan alınan, güvenlik belgeleri eksik, AB'de benzer bir modeli geri çağırılan pille çalışan bir oyuncak 90/100 puan alabilir ve bu da onu "Acil Müdahale" kategorisine yerleştirir.

3. Önceliklendirme ve Görevlendirme

Yüksek riskli vakalar, denetçiler için otomatik uyarılar oluşturur:

- Platformlara acil kaldırma talepleri.
- Laboratuvar testleri için gizli satın alma siparişleri.

4. Dinamik Güncelleme

Risk puanları, yeni veriler geldikçe sürekli olarak yeniden hesaplanır.

Örnek: Bir satıcı, işaretlenen tüm ilanları kaldırır ve uygunluk kanıtı sunarsa, puanı düşer; yeni şikayetler ortaya çıkarsa, puanı yükselir.

7.5 Gelişmiş Analitik ve Yapay Zekanın Rolü

Risk modeli sadece sabit kurallarla sınırlı kalmayacak, aynı zamanda **tahmine dayalı analitik ve yapay zeka destekli algılama** ile de gelişecektir. Potansiyel yetkinlikler arasında şunlar yer almaktadır:

- **Satıcı davranışlarında örüntü tespiti:** cezaları önlemek için hesaplarını sık sık kapatıp yeniden açan satıcıların işaretlenmesi.
- **Trend analizi:** başka piyasalarda bilinen tehlikelere sahip ürünlerin satışlarında ani artışların fark edilmesi.
- **Metin madenciliği:** Tüketici yorumlarının güvenlik odaklı anahtar kelimeler açısından analiz edilmesi (ör. "aşırı ısındı", "bir kullanımdan sonra bozuldu", "kızarıklığa neden oldu").

Bu analitik araçların, geleneksel uygulama bilgisiyle birleştirilmesi sayesinde Türkiye'nin PGDK'ları **riskleri yaygın bir zarara yol açmadan tespit** edebilecektir.

7.6 Risk Temelli Gözetimin Kurumsallaştırılması

Risk temelli yaptırımın norm haline gelmesi için, isteğe bağlı bir araç olarak bırakılmamalı ve **günlük operasyonlara entegre edilmelidir**. Bu şu anlama gelir:

- Risk modelini kullanma konusunda her denetçiye rehberlik edecek **Standart Çalışma Prosedürleri (SİP'ler) hazırlanması**.
- Ulusal ve sektörel tüm kuruluşların aynı puanlama ve önceliklendirme kurallarını kullanmasını sağlayacak **çok kurumlu koordinasyon**.
- Denetim sonuçlarının modele geri beslenmesiyle, zaman içinde öngörü gücünü artıracak **geri bildirim mekanizmaları**.



Funded by
the European Union

- Denetçilerin otomatik uyarıları nasıl yorumlayacaklarını ve bunlara nasıl tepki vereceklerini anlamalarını sağlamak için **eğitim ve kapasite geliştirme** (5. Bileşen ile bağlantılı).

Örnek: Kozmetik bir krem için "yüksek risk" uyarısı alan bir denetçi, bu uyarının neden verildiğini de görebilecektir - örneğin, "AB uyarısına göre yasaklanmış bileşen içerir; satıcı daha önce testlerden geçememiştir; yüksek riskli bir ülkeden ithal edilmiştir." Bu yaklaşım, sisteme olan güveni artıracak ve tutarlı uygulamaları güçlendirecektir.

7.7 Ön Koşullar ve Kolaylaştırıcı Unsurlar

3. Bileşen'in başarısı şunlara bağlıdır:

- **1. Bileşen – Hukuki Uyum:** yetkililere risk puanlaması için gerekli verileri toplama, paylaşma ve işleme yetkisi verilmesi.
- **2. Bileşen – IT Aracı Geliştirme:** puanlama algoritmasını çalıştırmak ve uyarıları yönetmek için teknoloji sağlaması.
- **4. Bileşen – Kurumsal Kapasite Geliştirme:** PGDK'lar arasında metodolojinin koordineli kullanımını sağlaması.
- **5. Bileşen – İnsan Kaynakları ve Eğitim:** denetçilerin veri okuryazarlığı ve analitik becerilerini geliştirmesi.
- **6. Bileşen – Farkındalık Artırma:** Tüketicileri, risk puanlamasına katkı sağlayan raporlar sunmaya teşvik etmesi.

7.8 Riskler ve Azaltım Önlemleri

- **Risk:** Veri eksiklikleri veya düşük kaliteli girdiler puanlama doğruluğunu zayıflatır.
Azaltma: Platformlardan eksiksiz ve yapılandırılmış veri sağlanmasını zorunlu kılan hukuki yükümlülükler; otomatik veri kalite kontrolleri.
- **Risk:** Kurumların geleneksel denetim modellerinden vazgeçme konusundaki isteksizliği.
Azaltma: Risk odaklı denetim sayesinde güvenli olmayan ürünlerin daha hızlı tespit edilmesini ve kaldırılmasını gösteren pilot projeler.
- **Risk:** Uzmanlık görüşü olmadan algoritmalara aşırı güvenme.
Azaltma: Önemli yaptırım kararlarında insan gözetimini koruyan **hibrit bir model** uygulamak.

7.9 Beklenen Etki

Tam olarak faaliyete geçtiğinde, 3. Bileşen şunları sağlayacaktır:

- Türkiye'deki PGDK'ların **öncelikle en tehlikeli ürünlere** odaklanmasını sağlayarak tüketicilerin tehlikelere maruz kalma riskini azaltacaktır.
- Ortaya çıkan risklere müdahale hızını önemli ölçüde artıracak ve genellikle **büyük çaplı zararlar meydana gelmeden ürünleri piyasadan kaldıracaktır.**
- **Şeffaf ve kanıta dayalı bir önceliklendirme süreci** sağlayarak kamu güvenini ve hesap verebilirliği artıracaktır.
- Türkiye'nin PGD yaklaşımını **AB'nin risk temelli uygulama modeliyle** uyumlu hale getirerek, kritik bir katılım şartını yerine getirecektir.



Funded by
the European Union

Sonuç olarak, 3. Bileşen, **e-ticaretin ham verilerini hedefli ve zamanında uygulanan yaptırımlara dönüştürerek**; böylece Türkiye'nin, hiç uyumayan bir pazarda, tüketicileri etkili bir şekilde korumasını sağlayacaktır.





Funded by
the European Union

8 KURUMSAL KAPASİTE GELİŞTİRME (4. BİLEŞEN)

8.1 Kurumsal Kapasite Neden E-PGD Reformunda Belirleyici Faktördür?

Kurumsal kapasite, yasaları, araçları ve yöntemleri gerçek dünyadaki uygulamaya dönüştüren **bağ dokusudur**. Türkiye, **AB ile uyumlu mevzuatı** (1. Bileşen) benimseyecek, **gelişmiş bir IT izleme platformu** (2. Bileşen) geliştirecek ve **karmaşık bir risk değerlendirme modeli** (3. Bileşen) uygulayacak olsa bile, aşağıdaki durumlarda bu reformların hiçbiri tam etkisini gösteremeyecektir:

- Yetkililerin e-PGD faaliyetleri için **net yetki alanları yoksa**.
- PGDK'lar arasındaki **koordinasyon yavaş veya tutarsız kalırsa**.
- Personel, istihbarat bilgilerini gerçek zamanlı olarak harekete geçirecek **beceri ve kaynaklara sahip değilse**.

Bunun nedeni açıktır: **E-ticaret tehlikeleri sektör sınırlarını veya bürokratik zaman çizelgelerini dikkate almaz**. Tehlikeli bir ürün:

- Birden fazla teknik düzenlemeye (elektrik güvenliği + kimyasal güvenlik + etiketleme) tabi olabilir.
- Birden fazla satıcı tarafından birkaç platformda aynı anda satılabilir.
- Haftalar değil, saatler içinde müdahale gerektirebilir.

Dolayısıyla kurumsal zorluk, farklı sektörel sorumluluklara sahip birden fazla kurumdan oluşmasına rağmen, tek **bir operasyonel ağ** olarak işleyen **ulusal bir e-PGD sistemi** kurmaktır.

8.2 Mevcut Kurumsal Yapı ve Neden Reform Gerekliyor?

Türkiye'nin mevcut yapısı altında:

- **Ticaret Bakanlığı (TB)**, ürün güvenliği konusunda yatay koordinasyon ve politika yönlendirmesi sağlar.
- **PGDKK** (Ulusal Piyasa Gözetim ve Denetim Koordinasyon Kurulu) kurumlar arası koordinasyonu politika düzeyinde yürütür.
- **Sektörel PGDK'lar** belirli ürün kategorilerinden sorumludur (örneğin, kozmetik ürünler için Sağlık Bakanlığı, elektrikli ürünler için Sanayi ve Teknoloji Bakanlığı, gıda ile temas eden malzemeler için Tarım ve Orman Bakanlığı).
- **Gümrük idareleri** (TAREKS aracılığıyla) ithalatı kontrol eder.
- **Tüketici koruma örgütleri** şikayetleri ve tazminat taleplerini ele almaktadır.

Bu düzenleme, Türkiye'ye **fiziksel PGD** ortamında önemli katkılar sağlamıştır. Ancak, üç ana nedenden dolayı **e-ticarete tam olarak uyarlanamamıştır**:

1. Parçalı Operasyonel Kontrol

Her kuruluş yalnızca "kendi" ürün kategorisini izlemektedir. E-ticarete, tek bir çevrimiçi mağaza onlarca ürün türü satabilir; bu da, kurumlar bilgiyi hızlı bir şekilde paylaşmazlarsa, güvenli olmayan ürünlerin boşluklardan geçebileceği anlamına gelmektedir.

2. Reaktif, Proaktif Değil

Mevcut iş akışları genellikle şikayetlere veya periyodik izlemeye yanıt vermektedir. Oysa, e-ticaret **sürekli ve proaktif tarama** gerektirir.



Funded by
the European Union

3. Platformlarla Parçalı İletişim

Platformlar, farklı kurumlardan, bazen çelişen formatlarda ve zaman çizelgelerinde talepler almaktadır. Bu durum, **uyum verimliliğini düşürmekte** ve ürün kaldırma süreçlerini yavaşlatmaktadır.

İhtiyaç Analizi, bu kurumsal özelliklerin aşağıdakilere yol açtığını doğrulamıştır:

- Kurumlar arası koordinasyonda gecikmeler.
- İşlerin tekrarlanması.
- Bazı gri alanlarda hiçbir PGD yapılmaması.
- Benzer riskler için tutarsız yaptırım uygulamaları.
- Ortak soruşturma fırsatlarının kaçırılması.

8.3 Kurumsal Kapasite Geliştirme Neden Önemlidir?

Bu boşluklar giderilmezse, Türkiye şu risklerle karşı karşıya kalacaktır:

- Çevrimiçi ticaretin hızına ayak uyduramayan hukuki yetkiler.
- 2. ve 3. Bileşen'ler kapsamında geliştirilen IT ve risk puanlama araçlarının yeterince kullanılmaması.
- Güvenli olmayan ürünlerin gereğinden uzun süre çevrimiçi kalması.
- AB'ye, dijital ortam için **operasyonel olarak olgun ve koordineli bir PGD sistemine** sahip olduğunu gösterememe.

Bu nedenle, kurumsal kapasite geliştirme sadece "daha fazla eğitim" ile ilgili değildir; e-PGD'nin aşağıdaki özelliklere sahip olması için **operasyonel yönetişimin yeniden şekillendirilmesi** ile ilgilidir:

- **Koordinasyon açısından merkezi**, ancak uygulama açısından **sektörel uzmanlık sahibi olması**.
- Kağıt tabanlı veya periyodik değil, **gerçek zamanlı iletişim sağlaması**.
- Hangi PGDK'nın süreci yürüttüğünden bağımsız, **yaklaşımın yeknesak olması**.

8.4 4. Bileşenin Stratejik Hedefleri

4. Bileşen şunları amaçlamaktadır:

1. E-ticaret pazarının denetimi için **tek bir operasyonel koordinasyon noktası oluşturmak**.
Gerekçe: Merkezi bir koordinasyon noktası, mükerrer çalışmaları önler, iletişimi hızlandırır ve platformlar ile yabancı düzenleyicilere tek bir iletişim noktası sağlar.
2. Tüm PGDK'lar arasındaki **usulleri ve veri paylaşım formatlarını standartlaştırmak**.
Gerekçe: Standardizasyon yapılmazsa, risk puanlama sistemi tutarsız eylemler üretebilir ve bu ise kamu güvenliğini ve hukuki meşruiyeti zedeleyecektir.
3. Kurumlar arasında **gerçek zamanlı bilgi alışverişini kurumsallaştırmak**.
Gerekçe: E-ticarette, birkaç günlük gecikmeler bile binlerce adet güvensiz ürünün satışına neden olabilir.



Funded by
the European Union

- Platformlarla üzerinde mutabakata varılmış hizmet seviyeleri kapsamında **iş birliğini resmileştirmek.**

Gerekçe: Gönüllü iş birliği düzensizdir; net yükümlülükler ve zaman çizelgeleri uyum oranlarını artırır.

- Tüm kurumları e-PGD araçlarını kullanabilecek **eşit dijital kapasiteyle donatmak**

Gerekçe: Bazı kuruluşlar IT platformunu kullanamıyor veya risk verilerini analiz edemiyorsa, sistem genelindeki performans en zayıf halka tarafından sınırlandırılacaktır.

8.5 Temel Kurumsal Önlemler ve Gerekçeleri

1. Ulusal E-Ticaret Piyasa Gözetim Koordinasyon Birimi

- Nedir:** Ticaret Bakanlığı veya PGDKK bünyesinde, günlük e-PGD faaliyetlerini gözeten, IT platformunu yöneten, yüksek riskli uyarıları doğrulayan ve vakaları ilgili PGDK'ya atayan merkezi bir operasyon birimi.
- Neden:** Merkezi operasyonel denetim, öncelikli vakaların hızlı bir şekilde ele alınmasını sağlar, kurumlar arasında çakışmayı önler ve platformlar ile AB ortakları için tek bir irtibat noktası oluşturur.
- Etkisi:** Vakaların daha verimli bir şekilde ele alınması, daha hızlı önlem alınması, uluslararası iş birliğinin iyileştirilmesi.

2. Kurumlar Arası E-Ticaret Görev Gücü

- Nedir:** E-PGD SİP'leri kapsamında eğitim almış ve yüksek riskli vakaları incelemek ve karara bağlamak üzere haftalık olarak (veya kriz durumlarında günlük olarak) çevrimiçi toplanacak, PGDK'lar tarafından atanan personelden oluşan sürekli bir yapı.
- Neden:** Karmaşık e-ticaret vakaları genellikle birden fazla düzenlemeyi kapsar; kalıcı ortak bir yapı, kararların koordineli ve anında alınmasını sağlar.
- Etki:** Sektörler arası yaptırımlar norm haline gelir ve çoklu tehlike içeren ürünler için gecikmeler azalır.

3. E-Ticaret PGD için Ulusal SİP'ler

- Nedir:** İzleme, dijital delil saklama, kurumlar arası vaka aktarımı, platform bildirimleri ve konuyu üst mercilere taşıma yolları gibi standart prosedürleri kapsar.
- Neden:** Standartlaşmış usuller olmadan, aynı vakalar farklı PGDK'lar tarafından farklı şekilde ele alınabilir ve bu da hukuki itirazlara ve caydırıcılığın azalmasına yol açar.
- Etki:** İşletmeler ve e-platformlar için tutarlılık, yasal meşruiyet ve öngörülebilir sonuçlar.

4. Tüm PGDK'lar için Dijital Kapasite Artırımı

- Nedir:** Tüm yetkililerin, Bileşen 2 IT platformunu ve risk araçlarını etkili bir şekilde kullanmak için gerekli donanım, güvenli erişime ve eğitimli personele sahip olmalarını sağlamak.
- Neden:** Merkezi bir sistem, en zayıf katılımcısı kadar güçlüdür. Genel erişim ve beceriler olmadan, bilgi darboğazları devam edecektir.
- Etki:** Tüm kurumlar aynı dijital düzeyde çalışarak gerçek anlamda ulusal bir sistemin kurulmasını sağlar.



Funded by
the European Union

5. Platform İş birliği Çerçevesi

- **Nedir:** Tüm büyük pazar yerleri ile yasal olarak desteklenmiş mutabakat zaptları yapmak, önlemlere ilişkin faaliyetler, veri paylaşımı ve acil risk yönetimi için uygulama sürelerini belirler.
- **Neden:** Resmi anlaşmalar, platformların yükümlülüklerini yeknesak bir şekilde yerine getirmelerini sağlayarak belirsizliği ve farklı muameleleri ortadan kaldırır.
- **Etki:** Daha hızlı, standartlaştırılmış platform uyumu; vaka başına müzakere süresinin kısalması.

6. Hızlı Müdahale Protokolleri

- **Nedir:** Denetmenlere, yüksek riskli uyarılar temelinde, soruşturma sürerken dahi güvensiz ürün ilanlarının derhal kaldırılmasını emretmelerine olanak tanıyan acil durum önlemleri.
- **Neden:** Acil durumlarda (örneğin, güvenli olmayan çocuk ürünleri), 48 saatlik bir gecikme bile tüketicilerin yaygın maruziyetine neden olabilir.
- **Etki:** Tüketicilere verilen zararın önemli ölçüde azalması; uygunsuz satıcılar için caydırıcılığın artması.

8.6 PGDKK'nın Stratejik Rolünün Güçlendirilmesi

PGDKK (Ticaret Bakanlığı başkanlığında):

- URDM'nin tüm PGDK'larda **tutarlı bir şekilde uygulanmasını denetleyecektir.**
- IT platformu tarafından oluşturulan KPI'ları kullanarak **uygulama performansını izleyecektir.**
- Uluslararası ürün güvenliği ağlarında **Türkiye'yi temsil edecek** ve her iki yönde veri akışını sağlayacaktır.
- E-PGD'nin etkinliği hakkında **kamuoyuna rapor verecek**, hesap verebilirliği ve kamu güvenini güçlendirecektir.

Not: AB'de, PGDKK gibi ulusal koordinasyon organları, sektörel düzenleyicilerin sınır ötesi ve dijital pazarlarda **tek bir stratejiye bağlı** çalışmasını sağlamak açısından kritik öneme sahiptir.

8.7 4. Bileşen Uygulanmazsa Ortaya Çıkacak Riskler

- **Operasyonel parçalanmışlık** devam edecek ve kurumlar ayrı ayrı çalışmayı sürdürecektir.
- **Denetimlerin tekrarlanması** kaynak israfına ve platformların memnuniyetsizliğine neden olacaktır.
- Bilgi akışının yavaşlığı nedeniyle **ciddi risk taşıyan ürünler** gereğinden uzun süre çevrimiçi kalacaktır.
- Türkiye, dijital ortamda koordineli PGD için **AB uyum hedeflerini karşılamakta zorlanacaktır.**

8.8 Beklenen Dönüşüm

4. Bileşen tam olarak uygulandığında:

- Türkiye, hızlı ve sektörler arası çapraz uygulama yapabilen, **uyumlu ve ulusal ölçekte koordine edilmiş bir e-PGD sistemine** sahip olacaktır.



Funded by
the European Union

- Platformlar, **tek ve yapılandırılmış bir iş birliği süreciyle** çalışacak ve uyum hızını artıracaktır.
- 2. ve 3. Bileşen'lerden gelen IT platformu ve risk metodolojisi, sadece öncü kullanıcılar tarafından değil, **tüm kurumlar tarafından etkin olarak kullanılacaktır.**
- Türkiye'nin kurumsal modeli, e-ticarete koordineli PGD için AB kriterlerini karşılayacak ve potansiyel olarak aşacaktır.





Funded by
the European Union

9 İNSAN KAYNAKLARI VE EĞİTİM (5. BİLEŞEN)

Yasa (1. Bileşen) ne kadar gelişmiş olursa olsun, IT sistemleri (2. Bileşen) ne kadar ileri veya risk değerlendirme metodolojisi (3. Bileşen) ne kadar karmaşık olursa olsun, bir PGD sistemi onu yöneten kişiler kadar güçlüdür. E-PGD’de, insan kapasitesi sadece önemli bir faktör değil, aynı zamanda belirleyici bir unsurdur.

E-ticaret, PGD çalışmalarının doğasını temelden değiştirmiştir. Fiziksel piyasalarda, denetçiler güvenli olmayan ürünleri tespit etmek için gözlerine, ellerine ve laboratuvar testlerine güvenebilirler. E-ticaret ortamı ise buna tamamen yeni boyutlar eklemektedir: denetçiler artık onlarca e-platforda binlerce ilanı takip etmek, algoritmalar tarafından oluşturulan risk puanlarını yorumlamak, verilerde gizli olan uyumsuzluk kalıplarını tespit etmek ve tehlikeli ürünler tüketicilere ulaşmadan acilen harekete geçmek zorundadır. Bu ise yeni nesil beceri, zihniyet ve operasyonel hazırlık gerektirir.

9.1 Neden İnsanlar E-PGD'nin Gerçek "İşletim Sistemi"dir?

Teknoloji, e-platfordlarda milyonlarca ürünü saniyeler içinde tarayabilir, ancak bir ürünün düzenlemeleri ihlal edip etmediğine, hangi otoritenin yetki alanına girdiğine veya hızlı bir şekilde kaldırılmasını nasıl sağlayacağına hukuki ve pratik bir hassasiyetle karar veremez. Bu kararı alma süreci şunları gerektirir:

- Test sonuçlarını ve risk sinyallerini yorumlamak için **teknik değerlendirme**.
- Hukukten geçerli yaptırım adımlarını takip edecek **usule ilişkin uzmanlık**.
- E-platfordların iş birliğini sağlamak için **müzakere becerileri**.
- Bir ürün birden fazla düzenlemeyi aynı anda ihlal ettiğinde harekete geçmek için **sektörler arası farkındalık**.

İhtiyaç Analizi, Türkiye'deki denetçilerin **kendi sektörlerinde son derece yetkin** olduklarını göstermiştir, ancak e-PGD henüz günlük rutinlerinin bir parçası değildir ve yetkililer arasında eğitim eşit düzeyde bulunmamaktadır. Birçok PGDK’nın, e-PGD konusunda deneyimi olsa da, standart bir ulusal yaklaşım olmadığından sonuçlar değişkenlik göstermektedir. Bir denetçi bir ilanı birkaç saat içinde kaldırabilirken, başka bir denetçi aynı tür bir vakayı incelemek için daha fazla zaman harcayabilir. Bu tutarsızlıklar, caydırıcılığı ve kamu güvenini zedelemektedir.

9.2 Dijital Piyasalar için Genişletilmiş Beceri Seti

E-PGD çağında, denetçiler **geleneksel PGD’nin teknik titizliğini siber araştırmacıların çevikliğiyle** birleştirmek zorundadır. İş tanımı artık aşağıdakileri içermektedir:

- **E-ticaret platformlarının nasıl çalıştığını** anlamak - arama algoritmaları, ilan süreçleri ve satıcı kayıt sistemleri.
- Tespitlerden kaçmak için kullanılan çift hesaplar, değiştirilmiş ürün fotoğrafları veya yanıltıcı etiketleme gibi **aldatma taktiklerini** tespit etmek.
- **Veri açısından zengin ortamlarda** gezinme, otomatik uyarıları yorumlama ve gerçek tehditlerden gelen gürültüyü filtreleme.
- **Dijital kanıtların korunmasında** uzmanlaşmak - çevrimiçi içeriği mahkeme tarafından kabul edilebilir hale getirmek için nasıl yakalanıp saklanacağını bilmek.



Funded by
the European Union

- Platformlar, yabancı düzenleyiciler ve bazen acil risk senaryolarında doğrudan tüketicilerle **etkili iletişim kurmak**.

Bunlar “ekstra” beceriler değil – **görevin merkezinde yer alan kritik yetkinliklerdir**. Bu beceriler olmadan, en gelişmiş IT araçları bile sonuç üretmeyecektir.

9.3 Ad Hoc Eğitimden Ulusal E-PGD Öğrenim Sistemine

5. Bileşen, Türkiye’yi **düzensiz ve kurum bazlı eğitimlerden koordineli ve ulusal bir e-PGD öğrenim sistemine** geçirmektedir. Bu eğitim sistemi **entegre, sektöre duyarlı ve sürekli** olacak ve PGDK’lardaki her denetçinin aynı yetkinlikte çalışmasını sağlayacaktır.

Ulusal eğitim programı üç katman üzerine inşa edilecektir:

1. Temel E-PGD Yetkinlikleri - Tüm denetçiler için

Bu aşama şunları kapsayacaktır:

- Çevrimiçi PGD’nin temelleri.
- Ulusal IT platformu ve risk puanlama araçlarının kullanımı.
- Ulusal e-PGD SİP’lerinin uygulanması (4. Bileşen kapsamında geliştirilmiştir).
- Dijital delil yönetimi ve veri koruma mevzuatına uyum.

2. Sektöre Özgü Uzmanlaşma - Farklı PGDK’lar için özel modüller

Örnekler:

- Çevrimiçi satılan kozmetik ürünlerde yasaklanmış maddelerin tespiti.
- İlandaki görseller ve açıklamalardan uygun olmayan elektrikli ürünleri belirleme.
- Gıda ile temas eden malzemelerde yanıltıcı güvenlik iddialarının tespiti.
- Birden fazla tehlike barındıran ürünlerde ortak PGDK müdahalesi yönetimi.

3. İleri Düzey Uzmanlık Becerileri - Seçilmiş e-PGD uzmanları için

Bu eğitim programı aşağıdaki alanlarda üst düzey beceriler geliştirecektir:

- Platform tarayıcılarının yapılandırılması.
- Tekrarlayan uygunsuzluk örüntülerini belirlemek için büyük veri analizi.
- Uluslararası ürün güvenliği uyarı ağlarını kullanarak sınır ötesi iş birliği.
- Acil ve yüksek riskli vakalar için kriz yönetimi.

Eğitim yaklaşımı **uygulamalı, senaryo bazlı ve pratik ağırlıklı** olacaktır - denetçiler sadece çevrimiçi denetimler hakkında bilgi almakla kalmayacak, kontrollü simülasyon ortamlarında bunları uygulayacaklardır. Alıştırmalar arasında yüksek riskli ürünlerin belirlenmesi, kaldırma taleplerinin hazırlanması ve kurumlar arası koordinasyonun gerçek zamanlı olarak yönetilmesi yer alacaktır.

Ek IV – Eğitim ve Farkındalık Faaliyetleri, e-PGD personeli için öngörülen ilk kapasite geliştirme önlemlerini sunmakta olup, ortaya çıkacak yeni ihtiyaçlara göre ek konularla zaman içinde genişletilecektir. Bu ek, e-PGD personelinin sürekli gelişimini destekleyen ve ilgili tüm paydaşlar arasında yetkinliği teşvik eden, yaşayan bir araç olarak hizmet etmeyi amaçlamaktadır.



Funded by
the European Union

9.4 Bilginin Kurumsallaştırılması ve "Eğitim Kaybının" Önlenmesi

Takibi yapılmayan eğitimler genellikle "beceri kaybına" yol açar; bu, bilgi düzenli olarak kullanılmadığında yetkinliğin yavaş yavaş kaybolması anlamına gelmektedir. 5. Bileşen bu sorunu şu şekilde ele alır:

- SİP'ler, vaka çalışmaları, platform rehberleri ve mevzuat güncellemelerinin depolandığı ve tüm PGDK'ların erişebileceği çevrimiçi bir portal olan **kalıcı bir e-PGD bilgi deposu** oluşturulması.
- Denetçilerin zor vakalardan öğrendiklerini paylaşabilecekleri ve ulusal uygulamalarda iyileştirmeler önerebilecekleri **akranlar arası öğrenme ağları** kurulması.
- Yetkinliklerin güncel tutulması için, güncel mevzuatı, platform politikalarını veya teknoloji güncellemelerini kapsayacak **yıllık tazeleme eğitimi** uygulanması.

Bu yaklaşım, bilginin **korunmasını, paylaşılmasını ve sürekli yenilenmesini** sağlayarak e-PGD sisteminin personel kapasitesinin sürdürülebilirliğini sağlar.

9.5 İnsan Kaynaklarının Planlanması ve Görevlendirilmesi

Doğru becerilere sahip olmak önemlidir, ancak insan kaynağının nasıl tahsis edildiği de en az o kadar kritiktir. İhtiyaç Analizi, birçok PGDK'da şu bulguları ortaya koymuştur:

- e-PGD görevleri, özel bir zaman ayrılmadan mevcut görevlerin üstüne ek olarak verilmektedir.
- IT veya analitik uzmanlığı olan personel yetersizdir ve bazen birden fazla birimde görev yapmaktadır.
- Fiziksel piyasalardaki denetimler hala iş yükü planlamasında baskındır.

Bu sorunu çözmek için 5. Bileşen şunları önermektedir:

- Her PGDK'da, çevrimiçi izleme için planlı zaman aralıklarıyla çalışan **özel e-PGD denetmenleri görevlendirmek**.
- Gelişmiş dijital soruşturma konusunda eğitim almış, karmaşık veya çoklu tehlike içeren vakaları desteklemek için hazır olan **kurumlar arası bir e-PGD uzman havuzu** oluşturmak.
- Fiziksel ve çevrimiçi denetimler arasındaki dengenin e-ticaretin büyümesini yansıtmasını sağlamak için personel dağılımını yıllık olarak gözden geçirmek.

Bu yaklaşım, mutlaka çok sayıda yeni personel istihdam edilmesi anlamına gelmemekte; daha çok, e-PGD'nin yan görev değil, temel görev olarak ele alınması için **mevcut kaynakların stratejik olarak dağıtılması** anlamına gelmektedir.

9.6 Stratejik Getiri

Dijital becerilere sahip, operasyonel olarak kendine güvenen ve stratejik olarak dağıtılmış ulusal bir e-PGD işgücü oluşturarak Türkiye:

- Çevrimiçi tehditlere **haftalar değil, saatler içinde** tepki verecektir.
- Tüm sektörlerde **tutarlı bir uygulama** gerçekleştirerek adaleti ve caydırıcılığı artıracaktır.
- Denetçilerin çıktıları doğru yorumlamalarını ve harekete geçmelerini sağlayarak IT platformunun ve risk modelinin **değerini en üst düzeye çıkaracaktır**.
- "Ortak teknik dil" konuşarak platformlarla **iş birliğini güçlendirecektir**.



Funded by
the European Union

- AB'ye, Türkiye'nin PGD sisteminin sadece hukuki olarak uyumlu değil, aynı zamanda hızlı dijital ortamda **operasyonel olarak da yetkin** olduğunu gösterecektir.

Kısacası, 5. Bileşen, **ön saflarda çalışan personele** çevrimiçi pazarda tüketicileri korumak için gerekli becerileri, araçları ve güveni kazandırmakla ilgilidir. Bu bileşen olmadan, diğer bileşenlerin yeterince kullanılmayan varlıklar haline gelme riski bulunmaktadır ve bu bileşenle Türkiye, tüm e-PGD'sini yönlendiren **yüksek performanslı bir insan gücü** kazanır.





Funded by
the European Union

10 FARKINDALIK ARTIRMA VE PAYDAŞ İŞ BİRLİĞİ (6. BİLEŞEN)

Bir e-PGD sistemi, kendi başına işleyen kapalı bir makine değildir. En güçlü hukuki çerçeve (1. Bileşen), karmaşık risk temelli metodoloji (3. Bileşen), en gelişmiş teknoloji (2. Bileşen), iyi koordine edilmiş kurumlar (4. Bileşen) ve yetenekli denetçiler (5. Bileşen) ile desteklendiğinde bile, tek başına başarılı olamaz.

E-PGD bir ekosistemidir. Etkinliği, tüm katılımcılarının (kamu otoriteleri, e-ticaret platformları, satıcılar, endüstri dernekleri, STK'lar ve tüketiciler) rollerini ne kadar iyi anladıklarına, sorumluluklarını yerine getirip getirmediğine ve iyi niyetle iş birliği yapıp yapmadıklarına bağlıdır. 6. Bileşen, bu ortak sorumluluk ekosistemini oluşturmak, düzenleyicilerin çalışmalarını güçlendiren ve etkisini artıran **bilgili, katılımcı paydaşlardan oluşan bir ağ oluşturmayı hedefler.**

10.1 E-PGD Zincirinde Farkındalık ve İş birliğinin Rolü

E-ticarete, güvenli olmayan bir ürünün yaşam döngüsü saatlere veya günlere sıkıştırılır. Boğulma tehlikesi yaratan bir oyuncak veya yalıtımı zayıf bir elektrikli cihaz sabah saatlerinde çevrimiçi olarak satışa sunulabilir, öğle saatlerinde yüzlerce tüketici tarafından satın alınabilir ve akşam saatlerinde farklı bir satıcı adı altında yeniden satışa sunulabilir. Bu hız, PGDK'ların uygunsuz ürünlerin arzını önleme ve kaldırma görevini tek başına üstlenmesinin imkansızlığını göstermektedir. Aşağıda belirtilen üç unsurun eş zamanlı gerçekleşmesi gerekir:

1. **Satıcılar, bir ürünü listelemeden önce kuralları bilmelidir.** Güvenlik gerekliliklerini ve uygunsuzluğun sonuçlarını anladıklarında, tehlikeleri proaktif olarak önleme olasılıkları artar.
2. **Platformlar, yalnızca pasif araçlar değil, operasyonel ortaklar olarak hareket etmeye hazır olmalı** ve güvenli olmayan ilanları kaldırmak ve yeniden ortaya çıkmalarını önlemek için hızlı önlemler almalıdır.
3. **Tüketiciler risklerin farkında olmalı ve sorunları bildirme yetkisine sahip olmalıdır,** sistem için ilave bir göz ve kulak görevi görmelidir.

Bu üç unsur olmadan, yetkililer her zaman bir "saklambaç" oyunu oynamak zorunda kalacaktır.

10.2 Satıcılar Arasında Uyum Kültürü Oluşturmak

Satıcılar, piyasaya arzın **ilk ve en doğrudan** kaynağıdır. Güvenliğin isteğe bağlı bir yük değil, iş yapmanın bir parçası olarak görüldüğü bir uyum kültürü, önleyici stratejinin temelini oluşturur.

6. Bileşen, farklı satıcı profillerine yönelik **çok katmanlı bir farkındalık programı** önermektedir:

- **Büyük satıcılar ve marka sahipleri** halihazırda uyum sistemlerine sahiptirler, ancak asgari yasal gerekliliklerin ötesine geçen gönüllü güvenlik kriterleri belirleyerek ve sektörleri için rol model olarak hareket ederek daha da ileri gitmeleri teşvik edilebilir.
- **Küçük ve orta ölçekli işletmeler (KOBİ'ler)** genellikle kurum içi uyum kapasitesinden yoksundurlar. Bu işletmeler için basit, görsel ve sektöre özgü rehberlik esastır. Bu rehberlik,



Funded by
the European Union

resimli kontrol listeleri, hızlı referans kartları ve yaygın ürün türleri için "En Önemli 10" güvenlik kuralı şeklinde olabilir.

- Sosyal medya veya küçük çevrimiçi mağazalar aracılığıyla satış yapanlar da dahil olmak üzere **mikro ve gayri resmi satıcılar**, fiilen kullandıkları kanallar aracılığıyla hedefe yönelik mesajlara ihtiyaç duymaktadır. Kısa videolar, infografikler ve platform içi bildirimler, uzun resmi kılavuzlardan daha etkili olabilir.
- **Sınır ötesi satıcılar**, satıcının bulunduğu yerden bağımsız olarak, Türk ürün güvenliği mevzuatının Türk piyasasına satılan tüm ürünlere uygulandığını açıklayan farklı dillerde bilgilere ihtiyaç duyar.

Bu yaklaşımın pratik ve ölçeklenebilir hale getirilmesi için:

- Ticaret Bakanlığı, sektörel PGDK'larla iş birliği içinde ve PGDKK'ya verilen rol kapsamında, her ürün kategorisine uyarlanmış, **sade bir dille yazılmış uyum kılavuzları** hazırlamalıdır.
- **Çevrimiçi uyum araç setleri** geliştirilmeli ve bir devlet portalında yayımlanma ve bu araç setleri öz değerlendirme araçları, Sık Sorulan Sorular (SSS'ler) ve ilgili mevzuata bağlantılar içermelidir.
- **Web seminerleri, sanal atölyeler ve oryantasyon oturumları** düzenli olarak planlanmalı ve sunulmalı, kayıtları daha sonra da izlenebilir olmalıdır.
- **Platform oryantasyon paketleri**, pazar yerleri ile ortaklaşa geliştirilmeli, böylece her yeni satıcı ürünlerini listelemeden önce uygunluk bilgilerini alabilmelidir.

Yaklaşımın dayanağı açıktır: Uygun olmayan ve/veya güvenli olmayan ürünlerin ilanlarını önlemek, uygulama yükünü azaltmak, tüketicileri daha erken aşamalarda korumak ve satıcılar ile yetkililer arasındaki güveni artırarak, mümkün olan en yüksek güvenlik seviyesini sağlamak.

10.3 Platformları Proaktif Ortaklara Dönüştürmek

E-ticaret platformları, dijital pazarın operasyonel merkezleridir. Uygulamada, ürünleri anında kaldırabildikleri, engelleyebildikleri veya işaretleyebildikleri için, düzenleyicilerden daha hızlı bir şekilde ürün ilanları üzerinde kontrole sahiptirler. Ancak, İhtiyaç Analizi değişken bir iş birliği olduğunu ortaya koymuştur: bazı platformlar oldukça duyarlıyken, diğerleri özel iletişim kanallarına sahip bulunmamakta, bu da yaptırımları daha yavaş ve zahmetli hale getirmektedir.

Bu sorunu çözmek için 6. Bileşen, aşağıdakiler yoluyla **iş birliğinin resmi bir zemine taşınmasını** talep etmektedir:

- Tüm büyük platformlarla **yasal dayanaklı Mutabakat Zaptı (MZ)** imzalanması ve aşağıdakilerin belirlenmesi:
 - Kaldırma işlemi için standart zaman çizelgeleri (örneğin, yüksek riskli durumlarda 24 saat içinde kaldırma).
 - Satıcı ve ürün verilerinin paylaşılması için mutabık kalınan formatlar.
 - Acil durumlarda izlenecek usuller.
- **Platform irtibat görevlileri** – her pazar yerinde, ulusal e-PGD koordinasyon birimi ile günlük iletişimi sağlamakla sorumlu olarak atanan kişiler.



Funded by
the European Union

- **Ortak tatbikatlar ve simülasyonlar** – denetçiler ve platform personelinin, toplu geri çağırma veya tehlikeli bir ürün kategorisinin toplatılması gibi gerçek hayat senaryolarını prova ettikleri alıştırımlar.

Bu sadece tarafların niyetine bırakılacak bir konu olmayıp, gecikmeleri ve mükerrerlikleri önleyen öngörülebilir, verimli iş akışları oluşturmayı amaçlamaktadır. Bir platform ne kadar hızlı yanıt verirse, tüketicilerin maruz kalma süresi de o kadar kısılacaktır.

10.4 Tüketicileri Güvenlik Aktörleri Olarak Güçlendirmek

Tüketiciler çoğu zaman güvenli olmayan bir ürünle ilk karşılaşan ve bazen de bu üründen ilk zarar gören kişilerdir. Ancak çoğu durumda, endişelerini nasıl ve nereye bildireceklerini bilmezler veya bildirimlerinin bir sonuca varacağından şüphe duyarlar.

6. Bileşen, **tüketici bildirimlerini e-PGD sisteminin doğal, kolay ve değerli bir parçası** haline getirmeyi amaçlamaktadır. Bunun için:

- Ulusal IT sistemine bağlı, masaüstü ve mobil cihazlardan erişilebilen **merkezi bir çevrimiçi bildirim portalı oluşturulması**.
- Ürün resimleri ve satın alma ayrıntıları için fotoğraf yükleme seçenekleriyle desteklenen, sade bir dille yazılmış **basit bildirim formları hazırlanması**.
- Sosyal medya, tüketici örgütleri ağları ve kamu medyasında, uygun olmayan ve/veya güvenli olmayan ürünleri nasıl tanıyacaklarını ve bunları nasıl bildireceklerini açıklayan **farkındalık kampanyaları yayımlanması**.
- Tüketicilerden alınan bildirimlerin ne tür faaliyetlerle sonuçlandığını gösterecek **geri bildirim döngüleri** - güven oluşturmak ve katılımı güçlendirmek açısından faydalı olacaktır.

Bu yaklaşımın nedeni açıktır: tüketiciler en geniş izleme kaynağıdır ve uygun kanallarla resmi denetimin önemli bir tamamlayıcısı haline gelebileceklerdir.

10.5 Sektör Kuruluşları ve Sivil Toplum ile İşbirliğinden Yararlanma

Sektör dernekleri, ticaret odaları, tüketici örgütleri ve STK'lar, farkındalık çalışmalarında güçlü birer aktördür. Bu kuruluşlar, yaygın iletişim ağlarına ve toplulukları içindeki güvenilirlik ile belirli hedef gruplarına erişim konusunda, kamuoyu kampanyalarından daha etkili imkanlara sahiptir.

6. Bileşen şunları öngörmektedir:

- Bu grupların endişelerini paylaşabileceği, iyileştirme önerileri sunabileceği ve e-PGD reformları hakkında güncel bilgiler alabileceği **düzenli paydaş forumları** kurmak.
- **Sektöre özgü atölye çalışmalarının ortak ev sahipleri** olarak onları dahil ederek erişimi ve katılımı artırmak.
- Mesajların sektörün gerçeklerini yansıtmayı ve pratik zorlukları ele alması için **farkındalık materyallerinin tasarımına** onları da dahil etmek.

Bu çarpanlar kullanıldığında, farkındalık kampanyaları daha geniş bir erişime, daha yüksek ilgi düzeyine ve daha güçlü bir katılıma sahip olacaktır.



Funded by
the European Union

10.6 İş birliğini Sisteme Yerleştirme

Tekil kampanyalar veya düzensiz toplantılar tek başına yeterli bir yaklaşım olmayacaktır. İş birliği, e-PGD sisteminin **rutin çalışma kültürüne** entegre edilmelidir. Bunun için:

- Paydaş katılımını ulusal e-PGD koordinasyon biriminin **kalıcı çalışma programına** dahil etmek.
- İş birliği performansını değerlendirmek, engelleri gidermek ve en iyi uygulamaları paylaşmak için platformlarla **üç ayda bir değerlendirme toplantıları** düzenlemek.
- Performans göstergeleri, vaka çalışmaları ve iyileştirme planlarını içeren **yıllık iş birliği ve paydaş katılım raporları** yayınlamak.

Buradaki ilke süreklilik olmalıdır - farkındalık artırma ve iş birliği **tek seferlik etkinlikler değil, süregelen süreçlerdir**.

10.7 6. Bileşen'in Sistemik Faydaları

6. Bileşen tam olarak uygulandığında aşağıdaki hususları sağlayacaktır:

- Satıcıların güvenlik kurallarını **bilmemeleri için hiçbir mazeretleri** kalmayacaktır.
- Platformları, uygulamada **tutarlı ve öngörülebilir ortaklar** haline getirecektir.
- Tüketicilerin, güvenli olmayan ürünler için **erken uyarı sensörü** görevi görmelerini sağlayacaktır.
- Şeffaflık, geri bildirim ve ortak sorumluluk yoluyla **güven oluşturulacaktır**.
- Tüm e-ticaret ortamını **varsayılan olarak uyuma** yönltecek, böylece düzeltici önlemlerin gerekliliğini azaltacak ve düzenleyicilerin kaynaklarını en ciddi tehditlere yönlendirmesine olanak sağlayacaktır.

Özetle 6. Bileşen, e-PGD'yi **sadece kamu görevi modelinden çıkartarak**, önleme, tespit ve müdahalenin tüm piyasa genelinde paylaşıldığı, **çok paydaşlı bir güvenlik ekosistemine** dönüştürmektedir.





Funded by
the European Union

11 EYLEM PLANI

11.1 Eylem Planının Amacı ve Rolü

Eylem Planı, Strateji ve Eylem Planı Raporunu (SAPR) vizyoner bir belgeden, Türkiye'de modern, AB ile uyumlu bir e-PGD sistemi kurmak için **uygulanabilir bir yol haritasına** dönüştürmektedir. Bu kapsamda:

- Ticaret Bakanlığı, PGDK'lar, gümrük, çevrimiçi platformlar ve tüketici örgütleri gibi tüm aktörlerin aynı reform dizisini takip etmeleri için **ortak bir yol haritası** sağlamak.
- Hukuki, teknik ve operasyonel önlemlerin uyumlu bir şekilde ilerlemesi için bir **koordinasyon aracı** olarak hizmet etmek.
- İlerlemeyi ölçülebilir hale getiren ve gerçek zamanlı olarak yönlendirmelere olanak tanıyan bir **izleme aracı** olarak işlev görmek.

11.2 SAPR Bileşenleri ile Stratejik Entegrasyon

Plandaki her adım, SAPR'nin altı stratejik bileşeninden birine dayandırılmış olup, **bütünsel bir reformu** önermektedir:

1. Hukuki Uyum

- **Örnek önlemler:** Yetkililere çevrimiçi denetim yapma yetkisi veren mevzuat değişiklikleri taslağı; platform iş birliğini yasal olarak zorunlu kılması; e-PGD hükümlerini GÜGT ve DSA ile uyumlu hale getirmesi hedeflenmektedir.
- **Neden önemli:** Net yasal yetki ve bağlayıcı yükümlülükler olmadan hiçbir IT aracı, risk modeli veya denetim kampanyası sürdürülebilir olamaz.

2. IT Aracı Geliştirme ve Entegrasyon

- **Örnek önlemler:** Ulusal e-PGD platformunun tasarlanması; ETBIS, MERSIS, PGDBIS ve TAREKS ile entegre edilmesi; çevrimiçi platformlarla güvenli veri alışverişi protokolleri oluşturması hedeflenmektedir.
- **Neden önemli:** E-ticaretin ölçeği, ürünlerin otomatik izlenmesi, veriye dayalı risk puanlaması ve merkezi vaka yönetimi gerektirir.

3. Risk Temelli Gözetim ve Analitik

- **Örnek önlemler:** Ulusal risk değerlendirme metodolojisinin geliştirilmesi; güvenli olmayan ürünlerin tespiti için yapay zeka kullanılması; sınır ötesi ürün güvenliği uyarı ağları ve tüketici şikayetlerinin denetimlerin hedeflenmesinde kullanılması.
- **Neden önemli:** Kaynaklar, rastgele kontroller yerine, güvensiz veya uygunsuz olma olasılığı en yüksek ürünlere odaklanmalıdır.

4. Kurumsal Kapasite Geliştirme

- **Örnek önlemler:** Sektörel PGDK'lar arasındaki rollerin tanımlanması; ortak denetim ekiplerinin oluşturulması; e-PGD'nin uygulanması için standart çalışma prosedürleri (SİP) geliştirilmesi.



Funded by
the European Union

- **Neden önemlidir:** Güçlü kurumsal düzenlemeler mükerrerliği önler, uygulama boşluklarını kapatır ve hızlı çok kurumlu müdahaleleri mümkün kılar.

5. İnsan Kaynakları ve Eğitim

- **Örnek önlemler:** Veri analistleri, e-PGD denetçileri ve IT yöneticileri için yeni iş tanımları oluşturulması; risk analizi ve çevrimiçi denetim yöntemleri konusunda uzmanlaşmış eğitimler verilmesi; kurum içi kapasiteyi geliştirmek için "eğiticilerin eğitimi" modelinin uygulanması.
- **Neden önemlidir:** Nitelikli insanlar, iyi hazırlanmış mevzuatlar ve araçlar kadar önemlidir — bunlar olmadan sistemler yeterince kullanılamaz.

6. Farkındalık Yaratma ve Paydaş İş birliği

- **Örnek önlemler:** Çevrimiçi satıcılar için farkındalık kampanyaları başlatılması; platformlarla resmi iş birliği anlaşmaları yapılması; güvenli olmayan ürünler için kullanımı kolay tüketici bildirim kanalları oluşturulması.
- **Neden önemlidir:** İktisadi işletmeciler ve tüketiciler kuralları, riskleri ve harekete geçme yollarını anladıklarında uyum oranı yükselir.

11.3 Sıralama ve Bağımlılıklar

Önlemler, birbirine bağlı adımların doğru sırada ilerlemesini sağlamak üzere yapılandırılmıştır:

- Hukuki yetkiler, IT geliştirme ve veri paylaşımından önce gelir.
- Kurumsal çerçeveler ve SİP'ler, ortak denetimler başlamadan önce kesinleştirilir.
- Kullanılacak sistemler ve metodolojiler hazır olduğunda eğitim verilir.
- Farkındalık kampanyaları, hukuki veya prosedürel yeni gerekliliklerin tanıtılmasıyla eş zamanlı olarak düzenlenir.

11.4 Aşamalı Uygulama

Plan, birbiriyle örtüşen üç aşamada uygulanır:

- **Aşama 1 – Kısa Vadeli (1–12. Aylar)**
Hukuki reformların yapılması, ilk IT platformu tasarımının geliştirilmesi, kurumsal rollerin netleştirilmesi ve risk metodolojisinin oluşturulması yoluyla temel hazırlıkları yapmak.
- **Aşama 2 – Orta Vadeli (13–36. aylar)**
E-PGD platformunun kullanıma sunulması, risk temelli denetimlerin başlatılması, AI destekli izlemenin pilot uygulaması ve platformlarla resmi iş birliğinin başlatılması.
- **Aşama 3 – Uzun Vadeli (36. Ay ve Sonrası)**
E-PGD faaliyetlerinin günlük çalışmalara entegre edilmesi, sonuçlara göre risk modelinin geliştirilmesi, farkındalık çalışmalarının genişletilmesi ve proje sonrası sürdürülebilirliğin sağlanması.

11.5 Sorumluluk Dağılımı

Planda yer alan her bir önlem için, bir **Öncü Kurum** ve uzmanlık, veri veya operasyonel kapasite sağlayan **Destekleyici Kurumlar** belirlenmiştir. Örneğin:





Funded by
the European Union

- Platform iş birliği maddelerinin hazırlanması → **Öncü: Ticaret Bakanlığı**, Destek: PGDK'lar, sektör dernekleri.
- AI tespit modüllerinin geliştirilmesi → **Öncü: Ticaret Bakanlığı IT Departmanı**. Destek: PGDK'lar, tüketici örgütleri, sektör dernekleri ve Gümrükler Genel Müdürlüğü
- KOBİ'leri hedefleyen ortak farkındalık kampanyası → **Öncü: Ticaret Bakanlığı**, Destek: PGDK'lar, e-platformlar, tüketici örgütleri.

Ek II – Önlemler Matrisi – önerilen eylemler ile SAPR bileşenlerinin, kurumsal sahiplikleri ve etkili uygulama için gerekli sıralama arasındaki bağlantıları vurgulamaktadır. **Ek III ise strateji, eylemler ve proje faaliyetlerinin** nasıl birbiriyle bağlantılı ve birbirini güçlendirici olarak tasarlandığını göstermektedir.

11.6 İzleme ve Uyarılama

Eylem Planı, **yaşayan bir belge** olarak aktif bir şekilde yönetilecektir:

- **Yılda iki kez yapılacak ilerleme değerlendirmeleri**, her önlemin durumunu takip edecek, gecikmeleri belirleyecek ve kapasite darboğazlarını tespit edecektir.
- **Yıllık performans raporları**, reformların somut iyileştirmeler sağlayıp sağlamadığını değerlendirecektir – örneğin, güvensiz ürünlerin tespitinde artış ve çevrimiçi pazar yerlerinden daha hızlı kaldırılması gibi.
- **Uyarlanabilir güncellemeler**, AB'deki yasal değişikliklere, pazar dinamiklerine veya ortaya çıkan ürün risklerine yanıt olarak önlemlerin sırasının yeniden düzenlenmesine veya yeni önlemlerin eklenmesine olanak tanıyacaktır.

11.7 Beklenen Sonuçlar

Eylem Planı uygulandığında Türkiye:

- Güçlü hukuki temellere dayanan, **AB ile uyumlu**, tam işlevsel bir **e-PGD çerçevesi** işletecektir.
- Çevrimiçi pazarlardan uygun olmayan ve/veya güvenli olmayan ürünlerin **hızlı ve sistematik bir şekilde** tespit edilerek kaldırılması sağlanacaktır.
- **Veriye dayalı, risk temelli bir yaklaşım** kullanarak kaynaklarını tahsis edebilecektir.
- Tüm PGDK'lar arasında kesintisiz **kurumlar arası koordinasyon** sağlayacaktır.
- Satıcıları, platformları ve tüketicileri **pazar güvenliği konusunda aktif ortaklar** olarak dahil edebilecektir.



Funded by
the European Union

12 RİSK YÖNETİMİ VE RİSKİN AZALTIMI

12.1 Risk Yönetimi SAPR için Neden Esastır?

Türkiye'nin e-PGD sisteminin dönüşümü, kapsamı açısından iddialı ve benzeri görülmemiş bir girişimdir. Bu dönüşüm, mevzuatı, kurumsal düzenlemeleri, teknoloji kullanımı, insan kaynağı kapasitesi ve paydaş katılımını kapsamaktadır. Üstelik tüm bunlar, ürünlerin, satıcıların ve hatta satış platformlarının bir gecede değişebildiği son derece dinamik bir pazarda gerçekleşmektedir.

Böylesine değişken ve çok paydaşlı bir ortamda, soru risklerin ortaya çıkıp çıkmayacağı değil, bunları ne kadar iyi öngörebileceğimiz, izleyebileceğimiz ve bunlara nasıl yanıt verebileceğimizdir. Proaktif risk yönetimi olmadan, yasal reformlar aylarca veya yıllarca durma noktasına gelebilir ve buna bağlı tüm önlemler gecikebilir; pahalı IT araçları geliştirilebilir ancak personel becerilerinin veya kurumsal taahhüdün eksikliği nedeniyle yeterince kullanılamayabilir; koordinasyon eksiklikleri, güvensiz ürünlerin denetimden kaçmasına izin vererek tüketicilerin güvenliğini zedeleyebilir ve Türkiye'nin AB ile uyum sürecini baltalayabilir. Bu nedenlerle, SAPR'a sonradan eklenmiş bir unsur değil, **en başından itibaren sistemin ayrılmaz bir parçası** olarak tasarlanmıştır.

12.2 Risk Türleri ve e-PGD Reformu ile İlgili Önemi

Yasal ve Düzenleyici Riskler

Neden önemli: Çevrimiçi denetimler, platformlardan veri talebi ve sınır ötesi yaptırım iş birliği için açık yetki veren yasal hükümler olmadan, diğer reformların uygulanabilir bir temeli olmayacaktır.

Olası sonuç: Platformlar iş birliğini reddedebilir, verilere erişim engellenebilir ve güvenli olmayan ürünler süresiz olarak çevrimiçi kalabilir.

Riskin Azaltımı için önlemler: Değişiklik taslaklarının erken hazırlanması, AB GÜGT ve DSA ile uyum sağlanması ve Parlamento'ya sunulmadan önce bakanlıklar arası desteğin sağlanması.

Kurumsal Koordinasyon Riskleri

Neden önemli: e-PGD, birbiriyle örtüşen yetki alanlarına sahip birden fazla kuruluşu içerir. Net bir rol dağılımı olmadan, yaptırımlar tutarsız veya mükerrer olabilir.

Olası sonuç: Çelişkili kararlar, kaynak israfı ve platformlar ile satıcılar nezdinde güvenilirliğin azalması.

Riskin Azaltımı için önlemler: Sorumlulukları tanımlayan mutabakat zaptları, kurumlar arası düzenli koordinasyon toplantıları ve ortak SİP'ler kullanılarak ortak denetim planlaması.

Teknik ve IT Riskleri

Neden önemli: e-PGD platformu, halihazırda mevcut olan birçok sistemle arayüz oluşturmalıdır. Entegrasyon zorlukları yaygındır.

Olası sonuç: Sistem gecikebilir, kısmi işlevsellikle çalışabilir veya maliyetli bir yeniden yapılandırma gerektirebilir.

Riskin Azaltımı için önlemler: Erken fizibilite çalışmaları, sanal test ortamları (sandbox) ve kademeli uygulamalar ile sorunlar tüm sistemi durdurmadan çözülebilir.



Funded by
the European Union

İnsan Kaynakları Riskleri

Neden önemli: E-PGD, özellikle veri analizi ve dijital soruşturma alanlarında yeni beceri setleri gerektirir.

Olası sonuç: İşlevsel bir IT platformu olsa bile, personel verileri yorumlayamazsa güvenli olmayan ürünler hızlı veya doğru bir şekilde tespit edilemeyebilir.

Riskin Azaltımı için önlemler: Erken aşamada yetkin personelin işe alınması veya yeniden görevlendirilmesi, gerçek araçlarla bağlantılı hedefli eğitimler verilmesi, kurum iç eğitim kapasitesinin oluşturulması.

Paydaş Katılımı Riskleri

Neden önemli: Platformlar, satıcılar ve tüketici grupları ürün güvenliğinin aktif katılımcıdır. İş birliği olmadan, yaptırımlar reaktif ve eksik kalacaktır.

Olası sonuç: Platformlar veri paylaşımını geciktirebilir veya sınırlayabilir, satıcılar yükümlülüklerini göz ardı edebilir ve tüketiciler güvenli olmayan ürünleri bildirmeyebilir.

Riskin Azaltımı için önlemler: Raporlama gerekliliklerinin sadeleştirilmesi, uyumun itibar açısından faydalarının gösterilmesi ve hedefli bilgilendirme kampanyalarının başlatılması.

Dış Çevre Riskleri

Neden önemli: E-ticaret, AB/küresel kurallar, yeni teknolojiler ve gelişen iş modelleri tarafından şekillenmektedir. Ani değişiklikler planları bozabilir.

Olası sonuç: Araç ve süreçlerin uygulama sırasında hızlı bir şekilde revize edilmesi gerekebilir, bu da gecikmelere ve bütçe aşımına yol açabilir.

Riskin Azaltımı için önlemler: AB'deki gelişmelerin sürekli izlenmesi, esnek sistem tasarımı ve hızlı ayarlamalara olanak tanıyan yönetim yapılarının kurulması.

12.3 SAPR Risk Matrisi

Ek I'de sunulan Risk Matrisi, belirlenen temel riskleri, bunların olasılık ve etki düzeylerini, üzerinde mutabık kalınan azaltım önlemlerini ve her bir riskin yönetiminden sorumlu kurumu özetlemektedir.

12.4 Risk Yönetiminin Eylem Planıyla İlişkisi

SAPR Eylem Planındaki 53 önlem birbiriyle bağlantılıdır. Temel bir önlemden yaşanacak gecikme, ona bağlı önlemlerde de gecikme yaratacaktır. Risk yönetimi süreci, önlemler arasındaki bağımlılıkları haritalandırarak, "baskı noktaları"nı (başarısızlığı en geniş dalga etkisi yaratacak önlemler) belirler ve azaltım çabalarının öncelikle bu noktalara odaklanmasını sağlar.

Örneğin: Platform iş birliği için yasal değişikliklerin gecikmesi, IT veri entegrasyonunu, SİP geliştirmeyi ve satıcılar için farkındalık kampanyalarını etkiler. Risk metodolojisinin kesinleşmesinin gecikmesi, ilgili eğitimleri, analitik araçlarının devreye alınmasını ve hedeflenen denetimleri erteler.

12.5 Risk Azaltımı için Rehber İlkeler

1. Önlemek, düzeltmekten daha iyidir - riskleri önceden tahmin etmek için önceden çalışma yürütmek.



Funded by
the European Union

2. Eş zamanlı çözümler - bir alanda yaşanan gecikmelerin diğer alanlardaki ilerlemeyi durdurmasını için birden fazla alanda destekleyici önlemler almak.
3. Yerleşik esneklik - tamamen yeniden bir tasarlama gerektirmeden gelecekteki değişikliklere uyum sağlayacak araçlar, yasalar ve prosedürler tasarlamak.
4. Şeffaflık - güveni ve ortak problem çözmeyi teşvik etmek için risk bilgilerini tüm paydaşlarla açık bir şekilde paylaşmak.
5. Kanıta dayalı uyum – riski, azaltım önlemlerini izleme ve değerlendirmeden elde edilen gerçek verilere dayandırmak.

12.6 Etkili Risk Yönetiminin Faydaları

Bu ilkelerin tutarlı bir şekilde uygulanması, kaçınılmaz aksaklıklara rağmen SAPR'nin zamanında uygulanmasını sağlayacak, IT sistemleri ve eğitime yapılan yatırımın getirisini koruyacak, paydaşların güvenini sürdürecektir ve Türkiye'nin AB kural değişikliklerine, yeni teknolojilere ve değişen pazar modellerine hızlı bir şekilde yanıt vermesini sağlayacaktır.

Sonuç olarak, etkili risk yönetimi, Eylem Planını statik bir belgeden, e-ticaret ortamının belirsizliklerini yönetirken tüketici güvenliği ve AB uyumu için vaat edilen sonuçları sunan, dayanıklı ve uyarlanabilir bir stratejiye dönüştürür.





Funded by
the European Union

13 SONUÇ

Strateji ve Eylem Planı Raporu (SAPR), Türkiye'nin e-PGD sistemini AB ürün güvenliği gerekliliklerine uygun olarak geliştirmek için kapsamlı bir çerçeve önermektedir. İhtiyaç Analizi, paydaş istişareleri ve hukuki boşluk analizlerine dayanan SAPR, altı stratejik bileşen belirlemektedir:

1. Hukuki Uyum
2. IT Aracı Geliştirme ve Entegrasyon
3. Risk Temelli Gözetim ve Analitik
4. Kurumsal Kapasite Geliştirme
5. İnsan Kaynakları ve Eğitim
6. Farkındalık Artırma ve Paydaş İş birliği

Bu temel bileşenler, mantıksal sıralama ve bağlantılı ilişkilerin yönetimini sağlamak için üç aşamaya (kısa vadeli, orta vadeli ve uzun vadeli) ayrılmış 53 somut önlemlerle Eylem Planına dönüştürülmüştür. Eşlik eden Risk Yönetimi Çerçevesi, yasal, kurumsal, teknik, insan kaynakları, paydaşlar ve dış ortam risklerini belirler ve her biri için risk azaltma önlemleri ve sorumlu kurumları tanımlar.

Tasarlanan şekilde uygulanması halinde, SAPR şunları vaat etmektedir:

- E-PGD faaliyetlerinin yasal dayanağını güçlendirmek.
- Çevrimiçi pazar yerlerinden uygun olmayan ve/veya güvenli olmayan ürünlerin teknoloji destekli olarak tespit edilmesini ve kaldırılmasını sağlamak.
- Kurumsal koordinasyonu ve kaynak tahsisini iyileştirmek.
- Çevrimiçi satıcılar ve platformlar arasında farkındalığı ve uyumu artırmak.
- Tüketici korumasını güçlendirmek ve Türkiye'nin AB ürün güvenliği düzenlemelerine uyum sürecini hızlandırmak.

SAPR, bu nedenle hem stratejik bir vizyon hem de pratik bir uygulama aracı olup, reformların sürdürülebilir ve gelişen e-ticaret zorluklarına uyarlanabilir olmasını sağlamaktadır.





Funded by
the European Union

EKLER

EK I: RİSK MATRİSİ

EK II: ÖNLEMLER MATRİSİ

EK III: STRATEJİ, EYLEMLER VE PROJE FAALİYETLERİ

EK IV: EĞİTİM VE FARKINDALIK ARTIRMA FAALİYETLERİ

EK V: TAKSONOMİ TABLOSU





Funded by
the European Union

Ek I Risk Matrisi

Risk Kategorisi	Açıklama	Olasılık	Etki	Azaltma	Risk Sorumlusu
Yasal ve Düzenleyici	E-PGD kuruluşları ve platform iş birliği için yasal değişikliklerin kabul edilmesindeki gecikmeler	Yüksek	Yüksek	Parlamento'ya sunulmadan önce erken taslak hazırlama, paydaşlarla istişare, siyasi sahiplenme/dahil etme	Ticaret Bakanlığı ÜGDGM ve Hukuk Müşavirliği
Kurumsal Koordinasyon	Uygulama rollerinde PGDK'lar arasında çakışma/çatışma	Orta	Yüksek	Bağlayıcı mutabakat zaptları, ortak planlama toplantıları, entegre vaka yönetimi protokolleri	TB ÜGDGM (PGDKK Sekreteryası)
Teknik ve IT	e-PGD platformu ile mevcut sistemler (ETBIS, MERSIS, PGDBIS, TAREKS) arasındaki entegrasyon sorunları	Orta	Yüksek	Fizibilite çalışmaları, sandbox testleri, yedek seçeneklerle aşamalı uygulamaya geçme	TB ÜGDGM ve IT Departmanı
İnsan Kaynakları	Risk temelli gözetim için yetersiz veri analizi becerileri	Yüksek	Orta	Uzmanların erken işe alınması, uyumlu eğitim, eğitimcilerin eğitimi programları	Ticaret Bakanlığı Personel Genel Müdürlüğü ve PGDK'ların İK Departmanları
Paydaş Katılımı	Algılanan yük nedeniyle e-platformlar veya satıcıların düşük iş birliği	Orta	Orta	Açık yasal yükümlülükler, e-platformlarla diyalog, basitleştirilmiş raporlama formatları	TB ÜGDGM (PGDKK)
Dış Ortam	AB mevzuatında veya küresel e-ticaret uygulamalarında ani değişiklikler	Düşük	Yüksek	Sürekli izleme, esnek yönetim, önlemleri değiştirmeye hazır olma	Ticaret Bakanlığı ÜGDGM ve AB Genel Müdürlüğü



Funded by
the European Union

Ek II Önlemler Matrisi

	Önem	Kurumlar	Öncelik
Bileşen 1: Yasal Uyumlaştırma			
1	E-ticarete ürün güvenliği ve PGD bağlamında tam yasal uyum sağlamak için mevcut boşlukların tespit edilmesi gerekmektedir.	Ticaret Bakanlığı ve Piyasa Gözetim ve Denetim Kuruluşları (PGDK'lar), Proje Ekibi desteği ile	 Kısa
2	Öncelikle iş birliği açısından, e-PGD'nin çalışma ilkeleri ve uygulama kılavuzları geliştirilmelidir.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Kısa Vadeli
3	"Uzaktan İletişim Araçları Yoluyla Piyasaya Arz Edilen Ürünlerin PGDs'i Hakkında Yönetmelik" e-PGD'nin ihtiyaçları dikkate alınarak güncellenmeli ve etkin bir şekilde uygulanmalıdır.	Ticaret Bakanlığı	 Orta Vadeli
4	PGDK'lar, kurumsal iş birliği için gerekli ikincil mevzuatı hazırlamalıdır.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Orta Vadeli
5	E-ticaret platformlarının izlenebilirliği sağlamasını ve yapılandırılmış verilere erişim sağlamasını zorunlu kılan bir düzenleyici yükümlülük getirilmelidir.	Ticaret Bakanlığı	 Orta Vadeli
6	Satış ilanlarına savunmasız grupları hedefleyen bilgilerin dahil edilmesini zorunlu kılan bir düzenleyici yükümlülük getirilmelidir.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
7	E-PGD ve gizli satın alma yöntemlerine ilişkin açık ve net hükümler, birincil mevzuat düzeyinde düzenlenmelidir.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
8	PGD çerçevesinde hangi eylemlerin hangi yaptırımlara tabi olduğu konusundaki belirsizlikleri ortadan kaldırmak için mevzuat netleştirilmelidir.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
9	E-platformların ürün ilanlarında marka, model, ruhsat ve kayıt numarası gibi bilgileri zorunlu olarak belirtmeleri sağlanmalıdır.	Ticaret Bakanlığı PGDK'lar	 Orta
10	Yükümlülükler, e-platformun büyüklüğüne (büyük-küçük) göre farklılaştırılmalı ve bu ayırım mevzuatta açıkça belirtilmelidir.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
11	Satıcıların Türkiye'de bir irtibat noktası belirlemeleri de zorunlu kılınmalıdır.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
12	Platformların iç kontrol prosedürlerini uygulamalarını teşvik etmek için yasal bir çerçeve oluşturulmalıdır.	Ticaret Bakanlığı PGDK'lar Dışişleri Bakanlığı-AB Başkanlığı	 Orta Vadeli
13	Denetim ilkeleri mevzuatta açık ve uygulanabilir bir şekilde tanımlanmalıdır.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli



Funded by
the European Union

14	Riskli ürünlerin ve satıcıların e-ticaret platformları tarafından izlenmesini sağlamak için bir bilgi mekanizması ve ilgili mevzuat geliştirilmelidir.	Ticaret Bakanlığı	Orta Vadeli
15	E-PGD bağlamında, "gizli satın alma" yoluyla numune temini, takma ad kullanımı veya alternatif teslimat adreslerinin beyanı gibi uygulamalar için açık bir yasal dayanak gereklidir.	Ticaret Bakanlığı	Uzun Vadeli
16	Gizli satın alma sürecinde kişisel verilerin korunmasını sağlayacak şekilde takma adların ve teslimat adreslerinin kullanımı için yasal bir dayanak oluşturulmalıdır.	Ticaret Bakanlığı PGDK'lar	Uzun Vadeli
17	Oyuncak-kırtasiye ürünleri ve gıda ile temas eden malzemeler gibi çok kategorili ürünlerin sorumluluklarının dağılımına ilişkin gri alanları ele almak için özel düzenlemeler getirilmelidir.	Ticaret Bakanlığı PGDK'lar	Uzun vadeli
18	Bütçeyle ilgili engelleri ortadan kaldırmak için yasal değişiklikler yapılmalıdır.	Ticaret Bakanlığı PGDK Maliye Bakanlığı ile koordineli olarak	Uzun vadeli
19	Safety-Gate, ICSMS gibi sistemlerden bilgiye erişimi sağlamak için bir düzenleyici çerçeve oluşturulmalıdır.	Ticaret Bakanlığı	Uzun vadeli
20	Sayıştay tarafından yürütülen denetimler kapsamında gizli satın alma faaliyetleri için yasal güvenceler sağlanmalıdır.	Ticaret Bakanlığı PGDK Sayıştay ile koordineli olarak	Uzun vadeli
2. Bileşen: IT Aracı Geliştirme ve Entegrasyon			
21	Türkiye'de uygulanan piyasa gözetim uygulamalarıyla uyumlu e-PGD yazılımı geliştirilmesi gerekmektedir.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	Kısa Vadeli
22	Kullanıcı ve organizasyonel ihtiyaçları yansıtan teknik özellikler ve sistem gereksinimleri geliştirmek önemlidir.	Ticaret Bakanlığı Proje Ekibi desteği ile	Kısa Vadeli
23	Ulusal veri tabanları (ETBIS, MERSIS, PGDBIS, TAREKS vb.) ile etkileşimli çalışmanın fizibilitesi konusunda teknik ve idari bir değerlendirme yapılmalıdır.	Ticaret Bakanlığı Proje Ekibi desteği ile	Kısa Vadeli
24	Ürün güvenliği bilgilerinin tüm e-ticaret sayfalarında anlamsal olarak kolayca erişilebilir konumlarda görünmesini sağlamak için bir yazılım tasarımı geliştirilmelidir.	Ticaret Bakanlığı E-Ticaret Platformları PGDK'lar Proje Ekibi desteği ile	Kısa Vadeli
25	Görüntü çözünürlüğü ve etiket görünürlüğü gibi minimum kriterler belirlenmeli ve güvenlik	Ticaret Bakanlığı E-Ticaret Platformları PGDK'lar	Kısa Vadeli



Funded by
the European Union

	işaretleri, uyarılar ve etiketler ürün görüntülerinde açıkça okunabilir olmalıdır. Görüntüler, satıcının ürün reklam sayfalarında doğrudan görünmelidir.	Proje Ekibi desteği ile	
26	Sistem, PGDK'lar ve e-ticaret platformları arasında otomatik hafif mesajlar gönderip alabilmelidir.	Ticaret Bakanlığı Proje Ekibi desteği ile	 Kısa Vadeli
27	Türkiye'de uygulanan piyasa gözetim uygulamalarıyla uyumlu e-PGD yazılımı geliştirilmesi gerekmektedir.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Kısa Vadeli
28	PGDBIS'e veri girişi basitleştirilmeli ve TAREKS ve diğer piyasa gözetim veritabanlarıyla entegrasyon sağlanmalıdır. (Veriler her denetim için PGDBIS'e manuel olarak girilmelidir.)	Ticaret Bakanlığı	 Orta Vadeli
29	E-PGD yazılımı, kamu kurumlarının EBYS (Elektronik Belge Yönetim Sistemleri) ile entegre bir şekilde çalışacak şekilde tasarlanmalıdır.	Ticaret Bakanlığı PGDK'lar	 Orta Vadeli
30	Karar algoritmaları , denetimsiz makine öğrenimi ile çalışan AI tabanlı yapılara dönüştürülmelidir. Bu algoritmalar ayrıca çeşitli bağlamlarda ve kataloqlarda ürün aramayı basitleştirmelidir.	Ticaret Bakanlığı	 Orta Vadeli
31	Sosyal medya satışlarını ve fiyat karşılaştırma web sitelerini taramak için yazılım modülleri geliştirilmelidir.	PGDK'lar	 Orta Vadeli
32	Güvenlik işaretleri , ürün resimlerinde görünür şekilde yer almalı ve açıkça okunabilir olmasını sağlayan bir çözünürlükte olmalıdır.	E-Ticaret Platformları Ticaret Bakanlığı PGDK'lar	Orta  Orta Vadeli
3. Bileşen: Risk Temelli Gözetim ve Analitik			
33	Piyasa gözetim ve denetim otoriteleri tarafından kullanılacak ortak ve standartlaştırılmış bir risk değerlendirme metodolojisine ihtiyaç vardır. Özellikle risk sınıflandırması, uygunluk değerlendirmesi ve denetim süreci için karar verme aşamalarında.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Kısa Vadeli
34	Trend analizi, verimli sohbet ve risk değerlendirmesinde yapay zeka ve makine öğrenimi gibi ileri teknolojilerin kullanımı için teknik ve kurumsal kapasitenin geliştirilmesi gerekmektedir.	Ticaret Bakanlığı PGDK'lar	 Orta
35	E-ticaret platformlarından trend ve mevsimsellik analizinde kullanılmak üzere veri elde etmek için gerekli teknik ve yasal düzenlemeler hazırlanmalıdır.	Ticaret Bakanlığı	 Orta Vadeli



Funded by
the European Union

4. Bileşen: Kurumsal Kapasite Geliştirme			
36	Gizli satın alma faaliyetlerinin e-PGD süreçlerinde kanıt olarak kullanılabilmesi için uygulama ilkeleri ve uygun araçlar tanımlanmalıdır.	Ticaret Bakanlığı PGDK'lar	Orta Vadeli
37	E-PGD faaliyetlerine ilişkin görev tanımları, PGDK'ların taşra teşkilatlarında oluşturulmalı ve bu görevleri yerine getirmek için yeterli sayıda personel görevlendirilmelidir.	Ticaret Bakanlığı PGDK'lar	Orta vadeli
38	Her PGDK, e-PGD faaliyetleriyle ilgili iç düzenlemeler ve koordinasyon protokolleri oluşturmalıdır.	Ticaret Bakanlığı PGDK'lar	Orta vadeli
39	E-ticaret platformlarıyla iş birliğini düzenleyen yapılandırılmış protokollerin (MZ) oluşturulması teşvik edilmelidir.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları	Orta vadeli
40	E-ticarete gizli satın alma uygulamalarının hayata geçirilebilmesi için bütçe ve operasyonel eksikliklerin giderilmesi gerekmektedir.	Ticaret Bakanlığı PGDK'lar	Uzun vadeli
41	Gizli satın alma uygulamalarının etkin bir şekilde yürütülmesi için, her bir PGDK için sanal tüketici profilleri oluşturulmalı ve sanal ödeme sistemleriyle entegrasyon sağlanmalıdır.	Ticaret Bakanlığı PGDK'lar	Uzun vadeli
5. Bileşen: İnsan Kaynakları ve Eğitim			
42	E-PGD yazılımını kullanacak personele IT sistemleri eğitimi desteği sağlanmalı ve yazılımın kullanımı için gerekli teknik altyapı kurulmalıdır.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	Kısa Vadeli
43	Takma ad kullanılarak yapılan dijital alışverişlerde kişisel verilerin korunması konusunda eğitimler düzenlenmelidir.	Ticaret Bakanlığı PGDK'lar Tüketici Örgütleri E-Ticaret Platformları Sektörel Dernekler Proje Ekibi desteği ile	Kısa Vadeli
44	İnsan kaynakları planlaması, IT analistleri, risk değerlendiricileri ve dijital denetçiler için gelecekteki ihtiyaçları da içermelidir. Veri bilimi alanında uzmanlaşmaya özel bir ihtiyaç vardır.	Ticaret Bakanlığı PGDK'lar	Orta vadeli
45	Gelişmiş PGD sistemlerini desteklemek için veri analistleri ve risk modelleme uzmanları istihdam edilmelidir.	Ticaret Bakanlığı PGDK'lar	Orta
46	Eğitim programları, işlevsel rollere (IT, hukuk, saha denetimi) göre farklılaştırılmalıdır.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları Tüketici Örgütleri Sektörel Kuruluşlar	Orta vadeli



Funded by
the European Union

47	Eğitimcilerin eğitimi modelleri veya bölgesel düzeyde genişletilebilen ölçeklenebilir yapılar geliştirilmelidir.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları Tüketici Örgütleri Proje Ekibi desteği ile Sektörel Kuruluşlar	 Orta vadeli
48	PGDK'lar arasında bilgi ve veri paylaşımını sağlayacak bir iş birliği portalının kullanımı konusunda eğitim verilmesi.	Ticaret Bakanlığı PGDK'lar	 Orta
6. Bileşen: Farkındalık Artırma ve Paydaş İş birliği			
49	Tüketicileri hedefleyen bilgilendirme kampanyaları, güncel ve çevrimiçi kanallara uygun şekilde tasarlanmalıdır.	Ticaret Bakanlığı PGDK'lar Tüketici Örgütleri E-Ticaret Platformları Proje Ekibi desteği ile Sektörel Dernekler	 Kısa Vadeli
50	E-ticaret platformları, yüksek riskli satıcılarla ilgili uyarı mekanizmaları hakkında bilgilendirilmelidir.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Kısa vadeli
51	E-ticaret platformlarına, yasal yükümlülükler, risk göstergeleri ve sistem üzerinden çevrimiçi iletişim konusunda özel eğitim verilmelidir.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları Proje Ekibi desteği ile	 Kısa vadeli
52	Sosyal medya satıcıları ve çevrimiçi tüketiciler için farkındalık projeleri geliştirilmeli ve hedefli iletişim çalışmaları yürütülmelidir.	Ticaret Bakanlığı PGDK'lar Proje Ekibi desteği ile	 Kısa vadeli
53	Çevrimiçi satış ilanlarında güvenlik işaretlerinin görünürlüğü konusunda tüketici bilinci artırılmalıdır.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları Proje Ekibi desteği ile Tüketici Örgütleri	 Kısa vadeli
54	Tüketicilerin gönüllü olarak katkıda bulunduğu "Gönüllü Denetçi" kavramı geliştirilmelidir.	Ticaret Bakanlığı PGDK'lar E-Ticaret Platformları Tüketici Örgütleri	 Orta



Funded by
the European Union

Ek III Strateji, eylemler ve proje faaliyetleri

Eylem		Strateji				
		Yasal Uyumlaştırma	Kurumsal Kapasite Geliştirme	İnsan kaynakları geliştirme	Farkındalık Artırma	Etkili İş birliği Mekanizması (ECM)
IT Aracı Geliştirme ve Entegrasyonu	Risk Temelli Gözetim ve Analitik		x			
	Pazar yerleri entegrasyonu		x			
	PGDK'lar entegrasyonu		x		x	x
Eğitim/Seminerler	Tüketiciler	x		x	x	
	Çevrimiçi satıcılar ve e-pazar yerleri	x		x	x	
	Tüketici örgütleri	x		x	x	
	PGDK'lar	x	x	x		x
Kısa Filmler					x	
Sosyal medya uygulamaları					x	
Yayınlar					x	
Proje Kapanış Konferansı ve Paneli			x		x	x



Funded by
the European Union

EK IV Eğitim ve Farkındalık Artırma Faaliyetleri

EĞİTİM FAALİYETLERİ

No	Eğitim Konusu	Hedef Kitle	Odak Alanı	Süre*	Sıralama	Eğitim Formatı
1	Yasal ve Düzenleyici Çerçeve	PGDK'lar Türkiye Barolar Birliği veya Ankara Barosu'na kayıtlı avukatlar Tüketici Örgütleri E-Ticaret Platformları	- AB düzenlemelerini anlama (GÜGT, DSA, 2019/1020 sayılı Yönetmelik), - Türk mevzuatına yansımaları ve kalan boşlukları anlamak.	1 gün / düzenleme – toplam 3 gün		Bilgilendirici (mevcut mevzuat için)
2	Yasal ve Düzenleyici Çerçeve	PGDK'lar Türkiye Barolar Birliği veya Ankara Barosu'na kayıtlı avukatlar Tüketici Örgütleri E-Ticaret Platformları	- Türkiye'nin e-PGD Yönetmeliği'nde yansıtılacak değişiklikler. - Taraflar için yeni yükümlülükler - Daha iyi koordine edilmiş ve iş birliğine dayalı bir e-PGD uygulamasının hayata geçirilmesi için yeni kurallar.	2 gün – farklı illerde tekrarlanabilir veya çevrimiçi olarak sunulabilir	Güncellenmiş e-PGD Yönetmeliği taslağının hazırlanmasından sonra	Tüketiciler ve E-Platformlar için Bilgilendirici PGDK'lar için "Eğiticilerin Eğitimi"
3	Dijital Araçlar ve Risk Temelli Denetim	PGD Denetçileri	- Dijital risk modellerinin uygulanmasını anlama, - Platformlardan toplanan verilerin analizi, - LLM sistemlerini kullanarak veri analizini anlamak. - Karar Destek Sistemlerini Anlamak, - Trend önceliklendirme yöntemlerini anlamak.	1 gün/Ankara	Pilot Uygulama Sonrası	Eğiticilerin Eğitimi
4	Dijital Araçların Yönetimi ve Risk Temelli Denetim	PGDK'ların IT Birimleri	- Kullanıcı hesabı yönetimi ve faaliyetlerin izlenmesinin anlaşılması. - E-PGD süreci ve veri tarama/kazıma yöntemlerini anlama. - Veri Analizi yöntemleri. Kazınan verilerin verimli analizi için LLM sisteminin kullanımı. - Kullanıcı erişim kontrolleri.	1 gün /Ankara	Pilot Uygulama Sonrası	Doğrudan uygulama yönetimi eğitimi



Funded by
the European Union

No	Eğitim Konusu	Hedef Kitle	Odak Alanı	Süre*	Sıralama	Eğitim Formatı
			- PGDK'lar arasında bilgi paylaşımı için portal eğitimi. - Veri aktarım kontrolleri ve günlük analizi. - Risk analizi modellerinin başarısı için AI sistemi eğitimi. - Güvenli olmayan ürünleri izlemek için web kazıma, meta veri ve kapalı grup izleme kullanımı, - Dijital ortamlarda kanıtların işlenmesi. - Yararlanıcı DGIT için e-PGD sistemi yönetimi. - Sistem verimliliğinin ve etkinliğinin periyodik olarak değerlendirilmesi ve bunun sonucunda düzeltmeler ve düzeltici önlemler (eğitim dahil) alınması			
5	Platform Katılım ve İş Birliği Mekanizmaları	E-Ticaret Platformları (Uyum Ekipleri) PGDK'lar	- Revize edilmiş e-PGD Yönetmeliği kapsamında e-platformun sorumluluklarının netleştirilmesi, - Veri paylaşım mekanizmaları (MZ'ler, yapılandırılmış iletişim formatları) geliştirme olasılığı, - AB iyi uygulamalarına dayalı iş birliğinin teşvik edilmesi, - Platformlar tarafından paylaşılacak minimum veri setleri (satıcı bilgileri, satış eğilimleri, listeden çıkarmalar), - E-platformların satıcılarına yönelik sistematik ve etkili farkındalık artırma faaliyetleri.	2 gün – 1 gün İstanbul, 1 gün Ankara	Güncellenmiş e-PGD Yönetmeliği taslağının hazırlanmasından sonra	Bilgilendirici
6	Elektronik ticaret hizmet sağlayıcıları	Elektronik ticaret hizmet sağlayıcıları	- Ürün güvenliği ve geri çağırma,	1 gün/ürün kategorisi	Mevcut mevzuat kapsamında ve ayrıca revize	Bilgilendirici ve



Funded by
the European Union

No	Eğitim Konusu	Hedef Kitle	Odak Alanı	Süre*	Sıralama	Eğitim Formatı
	(bağımsız e-ticaret şirketleri) için ürün güvenliği konusunda farkındalık artırma ²	Ticaret Odası Yetkilileri	- Belirli düzenlemelere tabi ürün kategorileri (ilaçlar, gıda, oyuncaklar, elektrikli ürünler vb.) hakkında eğitim, - Belgeleme ve kayıt tutma, - Şikayetlerin, iadelerin ve geri ödemelerin ele alınması, - Ürün işaretleri, etiketleri ve ambalaj sorumluluklarını anlama.		edilmiş e-PGD mevzuatı sonrasında	"Eğiticileri Eğitim" programı
7	AI Destekli PGD	PGD Denetmenleri BİT Birimleri Hukuk Görevlileri	- Ürün analizi ve risk belirleme için AI destekli araçların kullanılması, - GDPR ve DSA kapsamında yasal sınırların değerlendirilmesi.	2 gün		Bilgilendirici
8	Birlikte çalışabilirlik (Gümrük ve MS)	PGDK'lar Gümrük Memurları Risk Analistleri DGIT	- TAREKS ve PGDBIS sistemlerinin entegrasyonu (iletişim sistemleri) - Sınır ötesi zorlukların ele alınması (Şubat ayı "Toolbox" raporunda yansıtılan AB öncelik alanları ile uyumlu olarak)	2 gün	Pilot Uygulama Sonrası	Resmi
9	E-Ticarette Uygun Olmayan ve/veya Güvenli Olmayan Ürünlerin Etkileri	PGDK'lar E-ticaret Platformları	- Uygun olmayan ve/veya güvenli olmayan ürünlerin maliyetleri, - İşletmelerin itibar kaybının analizi. - Gizli satın alma, senaryo alıştırmaları ve ortak simülasyonlar dahil olmak üzere vaka temelli, uygulamalı yöntemlerin uygulanması.	1 gün		
10	Pratik ve Etkileşimli Eğitim Yöntemleri	Tüm Paydaşlar		1 gün		

* Süre, görev tanımı gerekliliklerine göre revize edilebilir veya değişiklik önerileri sunulabilir.

² Bu eğitim, Ticaret Odaları ve İl Ticaret Müdürlükleri ile koordineli olarak belirlenen illerde gerçekleştirilmelidir. İlleri seçerken 'e-ticaret komitesi'nin varlığı dikkate alınmalıdır.



Funded by
the European Union

SEMİNERLER VE ÇALIŞMA GRUPLARI

Hayır	Seminer/Çalıştay Konusu	Hedef Kitle	Odak Alanı	Süre	Seminer/Çalıştay Formatı
1	Platform Katılımı ve İş birliği Mekanizmaları	E-Ticaret Platformları (Uyum Ekipleri) PGDK'lar	- E-platformların satıcılarına yönelik sistematik ve etkili farkındalık artırma faaliyetleri.	1 gün. Farklı yerlerde tekrarlamamız gerekiyor.	Bilgilendirici
2	Kurumsal Kapasite ve Koordinasyon	PGDK'lar (Yüksek düzeyde farkındalık artırma) Koordinasyon Kuruluşları (ÜGDGM) Politika Yapıcılar (yıllık planlar ve programlar düzenleyen kurumlar)	- Kurumsal rollerin gözden geçirilmesi ve netleştirilmesi, - PGDK'lar arasındaki "gri alanlar" için sorumluluk paylaşımının tartışılması, - Kurumlar arası koordinasyon ve ortak denetimler hakkında tartışmalar, - PGD için tek bir kurumun kurulması da dahil olmak üzere merkezi koordinasyon mekanizmalarının araştırılması, - Kurumlar arası veri alışverişini teşvik etmek.	1 gün	Bilgilendirici
3	Üçüncü Ülkelerle Yaptırım Diplomasisi	PGDK'lar Ticaret Müşavirleri Koordinasyon Birimleri (ÜGDGM)	- İkili iş birliği araçlarının oluşturulması, - AB'nin üçüncü ülkelerle yürüttüğü diyaloglarla uyum sağlanması, - Türkiye'nin uluslararası uygulama profilini oluşturmak.	1 gün	Bilgilendirici
4	Tüketici Bilinci ve Şikayet Mekanizmaları ³	Tüketici Örgütleri Öğretmenler	- Uygun olmayan ve/veya güvenli olmayan ürünler konusunda farkındalık yaratmak, - Ürün güvenliği ile ürün kalitesi arasındaki farkı anlamak, - Ürün işaretleri, etiketleri ve ambalajları anlamak, - Satın alma sonrası (kullanım öncesi) güvenlik kontrolleri ve uygunsuzluk durumunda alınacak önlemler, - Uygun olmayan ürünleri nasıl ve nereye bildireceği ve uyuşmazlıkların nasıl ele alınacağı,	1 gün	Bilgilendirici

³ Ankara, İstanbul, İzmir, Bursa, Diyarbakır, Gaziantep, Erzurum ve Antalya başta olmak üzere yedi coğrafi bölgeyi temsil eden şehirlerde, İl Ticaret Müdürlükleri, İl Millî Eğitim Müdürlükleri ve Ticaret Odalarının desteğiyle öğretmenler ve tüketici örgütleri için bilgilendirme toplantıları düzenlenmelidir.



Funded by
the European Union

			- Şikayet sistemlerinin optimize edilmesi (ALO Bakanlık Hatları, CIMER, Tahkim mekanizması), - Tüketici odaklı uyarılar tasarlamak (daha dikkat çekici, daha anlaşılır ve etkili mesajlar), - Halkın katılımını artırma stratejilerinin geliştirilmesi.		
--	--	--	---	--	--





"Bu belge, Avrupa Birlięi'nin mali desteęi ile hazırlanmıřtır. Bu yayının ięerięi, WEglobal Consultancy Inc. liderlięindeki konsorsiyumun sorumluluęundadır ve hiębir řekilde Avrupa Birlięi'nin grřlerini yansıtmamaktadır."