3rd Party Script Envanteri & GTM/Consent Planlama Şablonu — Yazılım / GTM (v1.0)

Asset Amaç: Bu şablon, web sitesindeki tüm üçüncü taraf (*3rd party*) script'leri tek bir envanterde toplar ve Google Tag Manager (GTM) altında kategori, kullanım amacı ve rıza (*consent*) eşlemesini standardize eder. Kullanıcı iznine bağlı tetikleme kurallarını şeffaf ve görünür kılar, redundant (gereksiz/yineleyen) script'leri temizlemek için teknik bir karar zemini sağlar. Otel ve B2B projelerinde denetlenebilirlik, sayfa yüklenme hızı ve veri minimizasyonu açısından tam netlik üretir.

Kim Kullanır?: Pazarlama Ekipleri, Ajans Performans Ekipleri, IT ve Yazılım Ekipleri (Otel ve B2B Sektörleri).

Nasıl Kullanılır?

1. Web sitesindeki tüm mevcut script'leri (kod içinde sabit tanımlı *hardcoded* olanlar ve GTM konteynerindekiler) tespit edip envanter tablosuna işleyin.
2. Her bir script'i kategori, kullanım amacı ve rıza kategorisiyle eşleştirerek özel tetikleme kurallarını (*triggering rules*) belirleyin.
3. Gereksiz veya güvenlik/KVKK riski taşıyan script'ler için eylem planı çıkarın: *Kaldır*, *Sınırla*, *Maskele* veya *Consent'e Bağla*.

TEMPLATE — 3rd Party Script Envanteri & GTM/Consent Planlama Matrisi

1) Script Envanteri Tablosu (Boş Planlama Şablonu)

Web varlıklarında çalışan tüm etiketin (tag) teknik, hukuki ve operasyonel veri kimlik kartı:

Envanter Alanı	Tanım / Girilecek Veri
Vendor / Script Adı	`_____` *(Örn: Google Analytics 4, Meta Pixel, Hotjar)*
Kategori	`[ ] Zorunlu` | `[ ] Analitik` | `[ ] Reklam/Pazarlama` | `[ ] UX/Performans`
Kullanım Amacı	`_____` *(Örn: Dönüşüm takibi, kullanıcı ısı haritası, retargeting)*
Sayfa Kapsamı	`[ ] Tüm Site` | `[ ] Belirli Sayfalar` *(Örn: Yalnızca /rezervasyon-basarili)*
Tetikleyici (Trigger)	`[ ] Pageview` | `[ ] Event` | `[ ] Scroll` | `[ ] Form Submit`

Consent Gereksinimi	`[ ] analytics_storage` | `[ ] ad_storage` | `[ ] ad_user_data` | `[ ] Zorunlu`
Veri Davranışı (Genel)	`[ ] Cookie` | `[ ] Pixel` | `[ ] Session Replay` | `[ ] Live Chat`
Masking / Privacy Ayarı	`[ ] Var (Maskeli)` | `[ ] Yok` *(Hassas veri gizleme aktif mi?)*
Script Sorumlusu (Owner)	`____________________` *(Örn: Dijital Pazarlama Ajansı / IT)*
GTM Konumu	`____________________` *(Konteyner ID / Klasör Adı / Tag İsmi)*
Son Değişiklik Tarihi	`____ / ____ / ________`
Son Audit Tarihi	`____ / ____ / ________`
Aksiyon / Eylem Planı	`[ ] Kalsın` | `[ ] Kaldır` | `[ ] Consent'e Bağla` | `[ ] Sayfa Kapsamını Daralt`

2) Consent Tetikleme Kural Şablonu

Rıza Yönetim Platformu (CMP / Cookie Banner) ile GTM arasındaki tetikleyici mantığı:

- **Consent Sinyali Kaynağı:** `____________________` *(Örn: CMP* `dataLayer` *anahtarı:* `cookie_consent_update`*)*
- **Kural Mantığı:**
  "Script Kategorisi = ***[Reklam / Analitik]*** *ise, yalnız* ***[ad_storage = granted / analytics_storage = granted]*** *sinyali alındığında etiketi çalıştır."*
- **Test Senaryosu & Doğrulama:**
  - *Kullanıcı Çerezleri Reddettiğinde:* Ağ (*Network*) sekmesinde ilgili vendor sunucusuna hiçbir HTTP isteği gitmemeli (`Blocked by Consent`).
  - *Kullanıcı Çerezleri Kabul Ettiğinde:* Etiket sıralı olarak tetiklenmeli ve veri iletimi başlamalı.

3) Nasıl Doldurulur? (5 Kritik Entegrasyon Kuralı)

1. **Hardcoded Script'leri Envanterde İşaretleyin (Öncelik: GTM'e Taşıma):** Kaynak koda manuel eklenmiş script'leri tespit edin. Bu kodların kontrolü zor olduğu için ilk sprintte GTM konteynerine taşıyın.
2. **Her Script'e Net Bir Sorumlu (Owner) Atayın:** Sahibi, yöneticisi veya kullanım amacı doğrulanmayan script'leri anında "Kaldırılacak" statüsüne geçirin.
3. **Kategori ve Consent Alanlarını Boş Bırakmayın:** Script'lerin engellenmesini önlemek adına rastgele "Zorunlu / Essential" etiketi vermeyin; bu durum KVKK denetimlerinde ihlal sayılır.

4. **"Pageview" Tetikleyicilerini Daraltın:** Tüm sitede her sayfa yüklemesinde çalışan reklam ve pazarlama kodlarını sadece ilgili dönüşüm sayfalarına (`/teklif-tesekkur`, `/rezervasyon-onay`) kısıtlayın.
5. **Yıllık Script Temizlik Rutini (365 Gün kuralı):** Yılda en az bir kez tüm etiketi denetleyin; aktif kullanılmayan kampanyalara ait eski pikselleri sistemden silin.

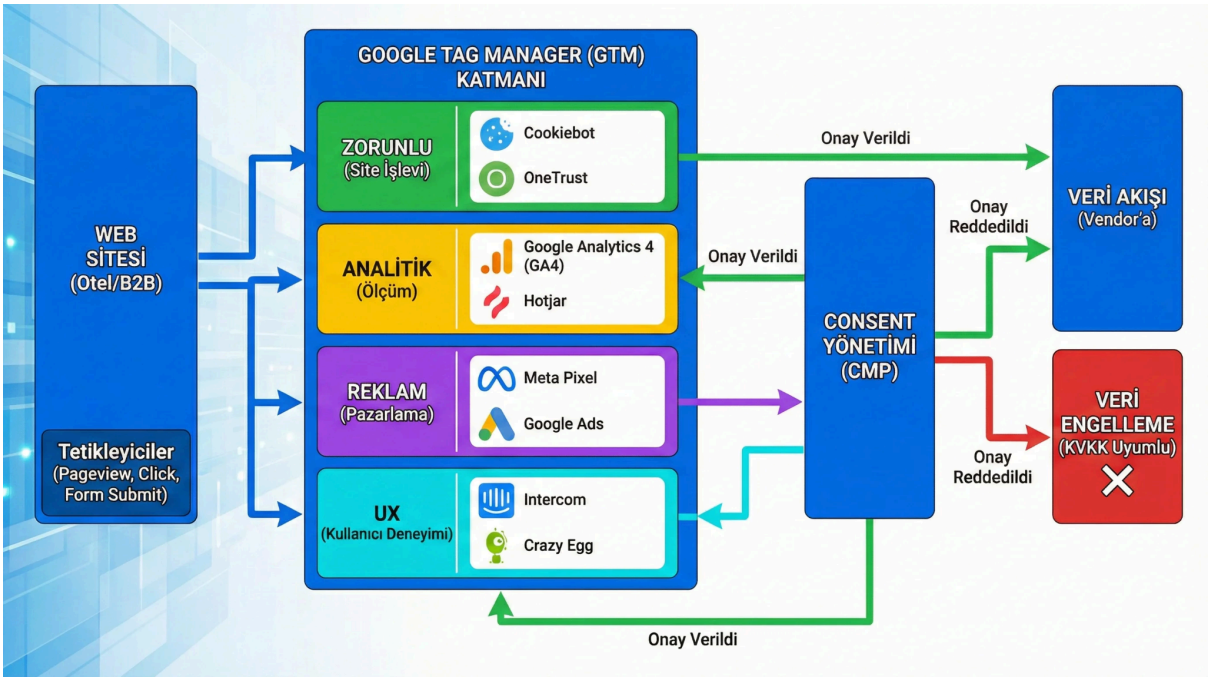
4) Denetim ve Kontrol Listesi (Checklist)

Envanterin canlıya alınması öncesinde tamamlanması gereken teknik adımlar:

- [ ] **Tüm Script'ler Envantere İşlendi:** Kaynak kod ve GTM üzerindeki istisnasız tüm etiketler listelendi mi?
- [ ] **Kategori ve Consent Eşleşmesi Tamamlandı:** Her script için CMP rıza parametresi (`ad_storage`, `analytics_storage` vb.) atandı mı?
- [ ] **Çerez Reddi Durumunda Network Bloklaması Doğrulandı:** Kullanıcı izni olmadığında tarayıcı ağ çağrılarının tamamen durduğu test edildi mi?
- [ ] **GTM Versiyonlama ve Değişiklik Notları Açıldı:** Yapılan her değişiklik öncesi GTM'de yeni versiyon oluşturulup değişiklik notları yazıldı mı?
- [ ] **Redundant (Mükerrer) Script Temizliği Yapıldı:** Aynı amaca hizmet eden birden fazla analitik veya ısı haritası aracından gereksiz olanlar kaldırıldı mı?
- [ ] **Session Replay / Isı Haritası Maskelemesi Aktif:** Ekran kaydı alan araçlarda kredi kartı, şifre, isim gibi hassas veri alanları (*input masking*) kapatıldı mı?
- [ ] **GTM Yayın Yetkisi Sınırlandırıldı:** Konteyneri canlıya alma (*Publish*) yetkisi yetkisiz kişilerden alınarak IT veya veri lideriyle sınırlandırıldı mı?

Deliverables (Teslim Edilecek Çıktılar)

- **3rd Party Script Envanter Tablosu (v1.0):** Sitedeki tüm dış kodların sahipliğini, teknik detaylarını ve durumunu gösteren güncel döküman.
- **GTM Consent Mode V2 Mimarisi:** İzin durumlarına göre tetiklenen etiketlerin ve değişkenlerin yer aldığı hazır GTM konteyner mimarisi planı.
- **Script Temizlik ve Güvenlik Runbook'u:** Yetkisiz script'lerin kaldırılması, veri maskeleme ayarlarının yapılması ve yıllık denetimlerin yürütülmesi için adım adım rehber.



[Diagram / Flow]

Bir otel veya B2B web sitesine gelen kullanıcının çerez tercihlerine göre GTM üzerinden 3rd party script'lerin tetiklenme veya bloklanma mantığını gösteren, 1920x1080px (16:9) Full HD çözünürlükte mimari süreç diyagramı. Koyu gece mavisi zemin üzerinde, en soldaki "Kullanıcı Sayfa Ziyareti & CMP Çerez Tercihi (DataLayer Event)" düğümünden çıkan oklar, ortadaki "GTM Consent Mode V2 Karar Katmanı"na ulaşıyor. Kullanıcı reddettiyse kırmızı kesikli hatlarla "Kritik Ağ İletimi Engellendi (Network Blocked)", onay verdiyse yeşil ve mor hatlarla "İlgili İzin Kategorisindeki Script'ler Tetiklendi (Analytics / Ads / UX)" uç noktalarına bağlanarak "clarity at a glance" felsefesiyle görselleştiriliyor.

[Checklist / Framework Card]

Pazarlama ekipleri, ajans performans uzmanları ve IT yöneticilerinin web sitelerindeki üçüncü taraf script'lerin KVKK uyumunu ve GTM tetikleme kurallarını denetlemeleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir kontrol kartı. Koyu karbon gri ve siber mavi tonlarındaki teknolojik arka plan üzerinde parlayan neon yeşili ve uyarı sarısı veri güvenliği simgeleri yer alıyor. Kartın üzerinde; "Tam Script Envanter Tespiti", "Consent Mode V2 Tetikleyici Eşleşmesi", "Çerez Reddi Ağ Çağrısı Bloklama Testi" ve "Session Replay Input Maskeleme Doğrulaması" maddeleri, yanlarında parlak check ikonlarıyla scannable ve kurumsal bir checklist formatında sergileniyor.