SAKIZLI BEŞ AŞAMALI DANIŞMANLIK MODELİ

Aşağıda, etik soruları ve Governance ilkelerini ayrıntılı biçimde ele alan mevcut "Sakizli Modeli" üzerine kesintisiz biçimde inşa edilen "Sakizli Beş Aşamalı Danışmanlık Modeli"ni sunuyorum. Bu model, söz konusu temeli yapay zekâ kullanımının sözleşmesel, hukuki ve düzenleyici boyutlarını kapsayacak şekilde genişletir. Yapay zekâ danışmanlarının bu zorlukları sistematik ve disiplinlerarası bir yaklaşımla ele almasına yönelik, uygulamaya dönük bir çerçeve sunar. Sakizli Modeli ile bütünleşmesi sayesinde etik ve Governance konuları korunurken hukuki çerçeve güçlü biçimde merkeze alınır. Bu bütünleşik yaklaşım, kuruluşların yalnızca hukuki riskleri azaltmasına değil, hızla gelişen yapay zekâ ortamındaki fırsatlardan sorumlu biçimde yararlanmasına da yardımcı olur.

Aşama 1: Hazırlık ve Ön Değerlendirme

Hedeflerin netleştirilmesi:

- Sözleşmesel ve düzenleyici hedefleri tanımlayın: Yasal ve sözleşmesel hedefleri net bir şekilde tanımlayın; örneğin Compliance sağlama, sorumluluk risklerinin güvence altına alınması veya veri koruma optimizasyonu.

Bilgi toplama:

- Teknolojik bağlam: Kullanılan yapay zekâ teknolojileri, altyapı ve arayüzlerin analizi.
- Mevcut sözleşmeler: Mevcut anlaşmaların, lisans anlaşmalarının ve iş birliği anlaşmalarının gözden geçirilmesi.
- İlgili yasalar ve standartlar: Ulusal ve uluslararası mevzuatların, sektöre özgü standartların ve düzenleyici gerekliliklerin (örneğin General Data Protection Regulation (GDPR), ürün sorumluluğu) tanımlanması.

Çerçeve koşullarını tanımlayın:

- Proje planlaması: Zaman çizelgeleri, kilometre taşları ve kaynaklar belirlemek.
- Stakeholder analizi: Tüm iç ve dış aktörlerin (hukuk uzmanları, teknologlar, Compliance görevlileri vb.) tanımlanması.

Aşama 2: Analiz ve problem tanımı

İhtiyaç analizi:

- Temel zorlukların tanımlanması: Mevcut sözleşme düzenlemelerindeki boşluklar ve yasal belirsizlikler.
- Konular: veri koruma, sorumluluk meseleleri, fikri mülkiyet ve düzenleyici Compliance.

Risk ve fırsat değerlendirmesi:

- SWOT analizi:
  - Güçlü yönler: Mevcut Compliance mekanizmalar, kanıtlanmış iç süreçler.
  - Zayıf yönler: Mevcut sözleşmelerde hukuki netlik eksikliği, yeni teknolojik gelişmelere yetersiz uyum.
  - Fırsatlar: Yeni sözleşmesel düzenlemeler yoluyla optimizasyon potansiyeli, mevcut düzenleyici gelişmelerin proaktif entegrasyonu.
  - Riskler: Veri ihlali, sorumluluk riskleri veya belirsiz sorumluluklar nedeniyle gecikmeler.

Önceliklendirme:

- Aciliyet değerlendirmesi: Belirlenen sorunları, genel başarıya etkisi ve önemine göre sıralayarak odaklanmış bir danışmanlık süreci sağlanır.

Aşama 3: Danışmanlık ve Çözüm Geliştirme

Somut çözüm önerilerinin geliştirilmesi:

- Özel sözleşme taslağı: Sorumluluk konularını, veri koruma gereksinimlerini ve Compliance yönergelerini ele alan özel düzenlemelerin geliştirilmesi.
- Risk azaltma önlemleri: Belirlenen yasal ve düzenleyici riskleri en aza indirmek için stratejilerin oluşturulması.

En iyi uygulamaların entegrasyonu:

- Best-Practice yöntemleri: Mevcut Sakizli Modelinden kanıtlanmış prosedürlerin benimsenmesi ve uyarlanması, yasal kontrol listeleri ve Compliance-Framework'lerle desteklenir.
- Danışmanlık yaklaşımı: pratik ve sürdürülebilir çözümler geliştirmek için etkileşimli atölye çalışmaları ve vaka çalışmalarının kullanılması.

Disiplinlerarası işbirliği:

- Uzman ağı: Avukatların, teknologların, veri koruma görevlilerinin ve diğer uzman alanların danışmanlık sürecine katılımı için bütüncül bir bakış açısı sağlanır.

Aşama 4: Uygulama ve dokümantasyon

Eylem planı:

- Adım adım planlama: Açıkça atanan sorumluluklar, son tarihler ve kaynak tahsisi içeren ayrıntılı bir uygulama planı oluşturulması.
- Uygulama adımları: Somut görevlerin tanımlanması, sözleşme revizyonundan yeni Compliance süreçlerinin tanıtılmasına kadar.

Dokümantasyon:

- Rapor hazırlama: Tüm geliştirilmiş sözleşme düzenlemeleri, yasal tavsiyeler ve önlemlerin kapsamlı bir rapor veya sunumda özeti.
- Kanıt: İlgili kararları, risk değerlendirmelerini ve iletişim stratejilerini gelecekteki Audit süreçleri referans olarak arşivleme.

İletişim stratejisi:

- Şeffaflık: Sonuçların iç (örneğin atölye çalışmalarında, eğitimlerde) ve harici olarak (örneğin ortak toplantılarında veya kamuya açık açıklamalarda) nasıl iletildiğini belirlemek Stakeholder güvenini güçlendirmek.

Aşama 5: Değerlendirme ve takip

Geri Bildirim ve Review:

- Değerlendirme döngüleri: Önlemlerin etkinliğini izlemek ve erken aşamada uyum ihtiyacını belirlemek için düzenli Feedback döngüleri ve Review süreçleri uygulanır.

Özelleştirme:

- Dinamik güncelleme: Modelin değişen teknolojik, yasal veya düzenleyici çerçevelere sürekli uyarlanması.
- Lessons Learned: Sürekli gelişim için deneyimlerin ve başarı faktörlerinin belgelenmesi.

Uzun vadeli destek:

- Follow-up toplantılar: Compliance ile sürdürülebilir uyumu sağlamak ve yeni zorlukları proaktif şekilde ele almak için düzenli Monitoring ve optimizasyon toplantıları planlamak.
- Monitoring: Uygulanan önlemlerin başarısını ölçmek için KPIs ve metriklerin oluşturulması.

Sakizli Beş Aşamalı Danışmanlık Modeli - Ayrıntılı Sürüm

Aşama 1: Hazırlık ve Ön Değerlendirme - Ayrıntılı Açıklama

Bu ilk aşama, tüm ilgili hukuki perspektifleri sistematik olarak yakalayarak ve yapay zekâ uygulamalarının işlediği bağlamı kapsamlı şekilde analiz ederek danışmanlık modelinin tamamının temelini oluşturur. Aşağıda, bu aşamanın temel unsurları açıklanmakta, özellikle hukuki konular ve yürürlükteki yönerge ve mevzuata özel olarak odaklanılır.

1. Hedeflerin netleştirilmesi

Sözleşmesel ve düzenleyici amaçların tanımı:

- Compliance ve sorumluluk: Sorumluluk risklerini en aza indirmek için hangi Compliance hedeflerinininin (örneğin GDPR, EU AI Act) gerçekleştirileceğinin belirlenmesi.
- Yasal uyumun sağlanması: Hangi yasa ve yönergelerin (örneğin eIDAS, DSA, DMA) planlanan yapay zekâ kullanımı için geçerli olduğunu ve hangi alanlarda (medya hukuku, ceza hukuku, ticaret hukuku vb.) özel gerekliliklerin olduğunu belirlemek.
- Hassas bilgilerin korunması: Ticari sırların, telif haklarının ve veri korumasının korunmasına ilişkin hedeflerin belirlenmesi.
- İnsan hakları ve etik ilkeler: Hukuki hedeflerin insan hakları standartları ve etik yönergelerle uyumlanması, örneğin ayrımcılık veya mahremiyet ihlali önlemek.

2. Bilgi toplama

A. Teknolojik bağlam ve iş ortamı

- Teknoloji ve sistem analizi: Belirli hukuk alanlarıyla ilgili olan yapay zekâ teknolojileri, algoritmalar, veri kaynakları ve arayüzlerin kaydedilmesi (örneğin algoritmik kararlar ve bunların EU AI Act ışığında şeffaflığı).
- Şirkete özgü durumlar: İç düzenlemeler, önceki sözleşmeler ve iç veri koruma kavramlarının dikkate alınması; bunlar daha fazla düzenleme için bir başlangıç noktası olarak hizmet eder.

B. İlgili yasal çerçeveler ve standartlar

- Avrupa mevzuatları:
  - EU AI Act: Yapay zekâ kullanımına uygulanan şeffaflık, risk değerlendirmesi ve sorumluluk konularına ilişkin gereksinimlerin analizi.
  - GDPR (General Data Protection Regulation (GDPR)): Veri koruma ilkeleri, ilgili kişilerin hakları ve veri işleme süreçlerinin incelenmesi.
  - DSA (Digital Services Act) ve DMA (Digital Markets Act): Çevrimiçi platformlarla ilgilenmedeki yükümlülüklerin, algoritmik karar vermenin ve rekabetçi yönlerin incelenmesi.
  - eIDAS (Electronic Identification, Authentication and Trust Services): Elektronik güven hizmetleri ve yasal gereksinimlerinin değerlendirilmesi.
- Ulusal mevzuat ve belirli hukuk alanları:
  - Telif hakkı ve medya hukuku: Telif hakkı koruma düzenlemelerinin ve medya hukuku hükümlerinin (örneğin basın hukuku) yapay zekâ kullanımını nasıl etkilediğinin incelenmesi.
  - Ceza hukuku yönleri: Potansiyel ceza hukuku risklerinin (örneğin yapay zekâ sistemlerinin kötüye kullanımı veya mahremiyette haksız müdahale) analizi.
  - Ticaret hukuku ve sözleşme hukuku: Hizmet sağlayıcıları veya ortaklarla yapılan sözleşmelerde tanımlanması gereken ticari hukuk çerçevelerinin incelenmesi.
  - Sorumluluk konuları: Sorumluluk düzenlemelerinin (örneğin ürün sorumluluğu, haksız fiil sorumluluğu) yapay zekâ uygulamaları açısından nasıl tasarlanması gerektiğinin belirlenmesi.
- Sektöre özgü standartlar ve sertifikalar: Yasal gerekliliklere ek olarak kullanılabilen ISO standartları veya özel sektör sertifikaları gibi ilgili sektör standartlarının toplanması.

C. İç ve dış belgelerin toplanması:

- Mevcut sözleşmeler ve politikalar: Mevcut sözleşmelerin, veri koruma politikalarının, Compliance düzenlemelerinin ve iç prosedürel belgelerin analizi.

- Dış görüşler ve yönergeler: Hukuki durumun değerlendirilmesine katkıda bulunan çalışmalar, düzenleyici yönergeler (örneğin veri koruma otoriteleri veya Avrupa kurumların) ve Best-Practice örneklerin dahil edilmesi.

3. Çerçeve koşullarını tanımlayın

A. Proje Organizasyonu ve Stakeholder Tanımlaması:

- İç aktörler: Hukuk departmanlarının, Compliance görevlilerinin, BT güvenlik uzmanlarının ve uzman departmanların rollerinin tanımı.
- Dış uzmanlar: Uzman avukatlar, veri koruma uzmanları, sektör danışmanları ve gerekirse devlet düzenleyicilerinin katılımı.
- İşbirliği ve iletişim: Disiplinlerarası iş birliğini sağlamak için iletişim kanalları ve düzenli koordinasyon süreçlerinin tanımlanması.

B. Zaman Çizelgeleri, Kaynaklar ve Bütçe:

- Proje dönemi: Bilgi toplama, analiz ve sonrasında uygulanan önlemler için ayrıntılı zaman çizelgesi, yasal gerekliliklere uyumu doğrulamak için kilometre taşları dahil.
- Kaynak tahsisi: Kapsamlı hukuki Review süreçleri için insan ve finansal kaynakların tahsis edilmesi (örneğin GDPR uyum hakkında dış görüşler).

C. Risk yönetimi ve yasal koruma:

- Erken risk belirleme: Sorumluluk sorunları veya veri koruma ihlalleri gibi potansiyel yasal engelleri tespit etmek için mekanizmaların uygulanması.
- Önlemler kataloğunun hazırlanması: Kritik hukuki eksiklikler analiz kapsamında tespit edilirse acil önlemlerin ve acil durum planlarının tanımlanması.

D. Dokümantasyon ve Reporting:

- Şeffaf toplama: Toplanan tüm bilgilerin, analizlerin ve tespit edilen hukuki sorunların tam dokümantasyonu; belirli yasa ve direktiflere (örneğin GDPR'nin belirli maddeleri, EU AI Act bölümleri vb.) çapraz referanslar dahil.
- Reporting yapıları: Yasal mevcut hukuki durumu ve tespit edilen tüm zorlukları hem iç hem de dış denetim organları karşısında anlaşılır bir şekilde sunmayı mümkün kılan yapılandırılmış bir Reporting sisteminin geliştirilmesi. Sakizli Legal Modeli'nin özet 1. Aşaması, yapay zekâ uygulamaları bağlamında tüm ilgili hukuki boyutları kapsayan sağlam bir başlangıç noktası oluşturacaktır. Hedeflerin netleştirildiğinden, teknik, sözleşmesel ve hukuki çerçeve koşullarının ayrıntılı toplanması ve analizine, açık proje ve iletişim yapılarının tanımlanmasına kadar, telif hakkı ve medya hukukundan AB düzenlemelerine, sorumluluk meselelerine ve veri korumasına kadar tüm yönler sistematik olarak dikkate alınmaktadır. Bu kapsamlı hazırlık, başarılı disiplinlerarası danışmanlık ve buna dayalı özel hukuki ve sözleşmesel önlemlerin geliştirilmesinin temelini oluşturur.

Aşama 2: Analiz ve problem tanımı - ayrıntılı açıklama

Bu aşamada, çözümün sonraki gelişimi için temel atılır. Mevcut mevcut durumu, mevcut zorlukları ve riskleri ile mevcut fırsatları sistematik olarak belirlemek önemlidir. Bunu yaparken, veri korumasından sorumluluk meselelerine ve özel düzenleyici gereksinimlere kadar tüm ilgili hukuki perspektiflerin kapsamlı bir şekilde analiz edilmesine özel özen gösterilmektedir.

1. İhtiyaç analizi

İlk durumun hedefli kaydı:

- Hukuki boşluklar ve zorluklar:
  - Mevcut sözleşmelerin ve veri koruma (GDPR, eIDAS) ile ilgili iç politikaların gözden geçirilmesi ve EU AI Act, DSA ve DMA gibi düzenleyici gerekliliklerle Compliance incelemesi.
  - Telif hakkı ve medya hukuku hükümlerinin (örneğin telif hakkı, basın hukuku) şu anda ne ölçüde dikkate alındığı veya gelecekte değişiklik gerektirdiği analizi.
  - Örneğin, yapay zekâ sistemlerinin kötüye kullanılmasından kaynaklanabilecek ceza hukuku risklerinin tanımlanması.
  - Özellikle ürün sorumluluğu ve yapay zekâ tabanlı kararlarda haksız fiil sorumluluğu bağlamında sorumluluk rejimlerindeki belirsizliklerin tanımlanması.

- İçsel ve dış etki faktörleri:
  - Teknolojik ortamın haritalanması ve hukuki değerlendirmeyi etkileyen yapay zekâ algoritmalarının haritalanması (örneğin EU AI Act'daki şeffaflık gereksinimleri).
  - Compliance politikaları, veri koruma kavramları, ticari sır koruması ve önceki Audit sonuçları gibi mevcut iç belgelerin toplanması.
  - Yasal gereklilikler için bir kıyaslama olarak hizmet eden dış uzman görüşleri, yönergeler ve sektöre özgü standartların (örneğin ISO standartları) dikkate alınması.
- Stakeholder bakış açıları:
  - Hukuk, Compliance, BT güvenliği ve diğer ilgili departmanlardan Feedback ve deneyimin dahil edilmesi.
  - Objektif bir envanter sağlamak için uzman avukatlar ve veri koruma danışmanları gibi dış uzmanlarla koordinasyon sağlanması.

2. Risk ve fırsat değerlendirmesi

Kapsamlı bir SWOT analizi yapmak:

- Güçlü yönler:
  - Veri koruma ve sözleşme yönetimi alanlarında mevcut Compliance önlemleri ve yerleşik süreçler.
  - Zaten Best-Practice standartları entegre etmiş ve disiplinlerarası iş birliğiyle başarı hikayelerini belgelemiştir.
- Zayıf yönler:
  - Mevcut sözleşmelerdeki potansiyel boşluklar, özellikle veri ihlali durumunda sorumluluk sorunları ve belirsiz sorumluluklar açısından.
  - İç süreçlerin yeni düzenleyici gereksinimlere yetersiz uyarlanması, örneğin EU AI Act veya DSA ve DMA'in yeni hükümleri nedeniyle.
  - Ticari sırlar ve fikri mülkiyet (telif hakkı) korunması konusunda şeffaflık ve belge eksikliği.
- Fırsatlar:
  - Sorumluluk konularını ve veri koruma risklerini açıkça ele alan yenilikçi sözleşme modellerinin tanıtılması yoluyla optimizasyon potansiyeli.
  - Mevcut ve gelecekteki düzenleyici gereksinimlere proaktif uyum sağlayarak rekabet avantajı, bu da ortakların ve müşterilerin güvenini güçlendirir.
  - Sertifikalar ve sektöre özgü standartlar (örneğin ISO sertifikaları) aracılığıyla piyasadaki konumunuzu pekiştirme fırsatı.
- Tehditler:
  - Veri koruma düzenlemelerine (GDPR) uymama veya EU AI Act dikkate alınmaması durumunda yüksek finansal ve itibar riskleri, bu da önemli para cezalarına yol açabilir.
  - YZ sistemlerinin kötüye kullanımına veya insan hakları ihlallerine karşı yetersiz korumanın cezai sonuçları.
  - Belirsiz sözleşme düzenlemeleri ve ticari ile sözleşme hukuku alanında koruma eksikliğinden kaynaklanan öngörülemeyen sorumluluk riskleri.
  - Ticari sırlar veya fikri mülkiyet yeterince korunmadığında dış ortaklar veya düzenleyicilerle olası çatışmalar.

Özel hukuki değerlendirmeler:

- Veri koruma ve eIDAS: Yanlış veri işleme risklerinin, ilgili kişi haklarının olası ihlallerinin ve elektronik güven hizmetleri gereksinimlerinin değerlendirilmesi.
- EU AI Act: Yapay zekâ uygulamaları için özel olarak geliştirilen şeffaflık gereksinimleri, risk sınıflandırmaları ve sorumluluk rejimlerinin analizi.
- DSA, DMA ve medya hukuku: Dijital hizmetler, rekabet düzenlemeleri ve medya hukuku gerekliliklerinin incelenmesi, kabul edilemez uygulamalardan kaçınmak.
- Sözleşme ve ticaret hukuku: Mevcut sözleşmelerin sorumluluk düzenlemelerindeki boşluklar ve ticaret bağlamında beklenmedik risklerle nasıl başa çıkılacağı açısından incelenmesi.

3. Önceliklendirme

Belirlenen zorlukların sistematik değerlendirmesi:

- Aciliyet matrisi:
  - Risklerin ve fırsatların etkilerine (yüksek, orta, düşük) ve gerçekleşme olasılıklarına göre değerlendirildiği bir matris oluşturulması.
  - Kritik alanlar (örneğin, veri ihlali, sorumluluk sorunları) önceliklendirilerek hemen harekete geçilmelidir.
- Değerlendirme Metrikleri:
  - Olası para cezaları, itibar zararı ve hukuki sonuçları göz önünde bulunduran nicel ve niteliksel kriterler geliştirin.
  - Stakeholder önceliklerinin entegrasyonu; böylece en acil sorunlar - örneğin GDPR veya EU AI Act alanında yetersiz Compliance - listenin başında yer almaktadır.
- Disiplinlerarası doğrulama:
  - Öncelikleri birlikte doğrulamak ve ayarlamak için iç ve dış uzmanlarla düzenli koordinasyon toplantıları.
  - Öncelikleri net bir raporda belgeleyin ve iletin; bu rapor Aşama 3'te çözüm geliştirme temelini oluşturur.

4. Analizin özeti ve dokümantasyonu

Detaylı bir analiz raporunun hazırlanması:

- Yapılandırılmış sunum:
  - İlgili hukuk alanlarına (GDPR, EU AI Act, telif hakkı, sorumluluk hukuku vb.) atıfta bulunarak belirlenen tüm zorluklar, boşluklar ve fırsatların özeti.
  - Her hukuk alanı için belirlenen belirli noktaları içeren SWOT analizinin ayrıntılı sunumu.
- Önceliklendirmenin belgelenmesi:
  - Önceliklendirilen riskler ve fırsatların net listesi, ek önlemler için temel oluşturur.
  - Bireysel risklerin aciliyetini ve potansiyel etkisini görselleştirmek için grafikler ve tabloların entegrasyonu.
- Bir Monitoring mekanizmasının kurulması:
  - Hukuki, teknolojik veya düzenleyici alandaki değişikliklerin erken tespit edilip gelecekteki analizlere dahil edilebilmesi için sürekli bir Monitoring sistemi geliştirmek. 2. Aşamaya İlişkin

Sonuç

Detaylı analiz ve problem tanım aşaması, sonraki çözüm yaklaşımlarının dayandığı sağlam bir temel oluşturur. Sistematik ihtiyaç analizi, farklılaştırılmış risk ve fırsat değerlendirmesi ve belirlenen tüm zorlukların net önceliklendirilmesi - veri koruma, sorumluluk, AB direktifleri ve diğer özel hukuk alanları gibi tüm hukuki yönlere özel odaklanarak - ilgili hukuki perspektifin göz ardı edilmemesini sağlar. Bu, Sakizli Legal Modeli'nin sonraki aşamalarında hedefli ve disiplinlerarası bir yaklaşımı mümkün kılar.

Aşama 3: Danışmanlık ve Çözüm Geliştirme - Detaylı Detaylandırma

Bu aşamada, somut ve pratik önlemlerin temeli atılır. Amaç, tüm tespit edilen hukuki zorlukları ele alan ve disiplinlerarası danışmanlık sürecine entegre edilmiş özel çözümler geliştirmektir. Hem yenilikçi sözleşme modelleri hem de kanıtlanmış Compliance yöntemleri içermektedir.

1. Somut çözüm önerilerinin geliştirilmesi

C. Özel hazırlanmış sözleşme taslağı ve yasal düzenlemeler:

- Sözleşme maddeleri:
  - Sorumluluk maddeleri: Hem ürün sorumluluğu hem de haksız fiil sorumluluk unsurlarını kapsayan kesin sorumluluk rejimlerinin geliştirilmesi. Bu maddeler, net sorumlulukları tanımlamayı ve risk azaltma mekanizmalarını içermeyi amaçlamaktadır.
  - Veri koruma ve Compliance: GDPR, eIDAS ve EU AI Act uyumu için veri işleme düzenlemeleri, ilgili kişilerin hakları ve veri ihlali durumunda Reporting yükümlülükleri gibi özel maddelerin entegrasyonu.

- Fikri mülkiyet ve ticari sırlar: İstenmeyen ifşaları ve rekabet dezavantajlarını önlemek amacıyla telif hakları, medya hakları ve iç ticari sırların korunması için düzenlemelerin geliştirilmesi.

- Düzenleyici koordinasyon:
  - En güncel düzenleyici gerekliliklerin (örneğin DSA, DMA) sözleşme anlaşmalarına gözden geçirilmesi ve entegre edilmesi.
  - İç düzenlemelerin dış rehberlik ve uzman görüşleriyle uyumlanması, böylece tüm düzenleyici değişiklikler ve sektöre özgü standartlar dikkate alınır.

B. Risk azaltma önlemlerinin geliştirilmesi:

- Risk yönetimi Framework:
  - Özellikle hukuki riskleri (örneğin veri koruma ihlalleri, sorumluluk belirsizlikleri) sistematik olarak kaydedip değerlendiren ayrıntılı bir risk yönetimi sürecinin oluşturulması.
  - Beklenmedik hukuki zorluklar veya düzenleyici değişiklikler durumunda acil durum ve yükseltme planları geliştirin.
- Eylem için özel öneriler:
  - Tespit edilen zafiyetlerle başa çıkma konusunda önerilerin hazırlanması; örneğin ek eğitim, yeni iç kontrol mekanizmalarının getirilmesi veya veri güvenliğini artırmak için teknik önlemlerin kullanılması.

2. En iyi uygulamaların entegrasyonu

C. Best-Practice Yöntemler ve Standartlar:

- Yönergeler ve kontrol listeleri:
  - Veri koruma (GDPR) ve EU AI Act telif hakkı ile medya hukukuna kadar tüm ilgili hukuk alanlarını kapsayan standart kontrol listelerinin kullanımı.
  - Yenilikçi sözleşme modellerinin ve Compliance mekanizmalarının en güncel standartlara uyduğundan emin olmak için Best-Practice dokümantasyonu kullanın.
- Sertifikalar ve standartlar:
  - Teknik ve yasal güvenliği sağlamak için uluslararası tanınmış sertifikaların (örneğin ISO standartları, BT güvenlik standartları) entegrasyonu.
  - Sektöre özgü sertifikalara referans, bunlar da kalite kanıtı olarak sözleşmelere ve iç süreçlere dayandırılabilir.

B. Metodolojik yaklaşım:

- Atölye çalışmaları ve vaka çalışmaları:
  - Uygulamadan vaka çalışmalarının analiz edildiği ve somut çözümlerin geliştirildiği etkileşimli atölyeler düzenlemek.
  - Senaryo analizini kullanarak belirli hukuki zorlukların (örneğin, sorumluluk davaları veya veri ihlali) farklı ortamlarda nasıl sonuçlanabileceğini belirleyin.
- Benchmarking:
  - İç prosedürleri sektör standartları ve rekabet uygulamalarıyla karşılaştırarak iyileştirme alanlarını belirleyin ve değerlendirin.

3. Disiplinlerarası iş birliği

A. Farklı uzman gruplarının katılımı:

- Hukuk uzmanları ve veri koruma görevlileri:
  - Tüm hukuki meseleleri - telif hakkından ceza hukukuna kadar - sağlam bir şekilde ele almak için iç avukatlar ve dış uzman avukatlarla sürekli koordinasyon.
  - Tüm düzenlemelerin GDPR uyumlu ve ileriye dönük olmasını sağlamak için veri koruma görevlilerinin katılımı.
- Teknolojik ve operasyonel uzmanlar:
  - BT güvenlik uzmanları ve teknologlarıyla iş birliği yaparak yasal önlemlerin teknik sonuçlarını (örneğin, veri depolama ve işlemede) değerlendirin ve optimize edin.
  - Geliştirilen çözümlerin operasyonel olarak uygulanabilir ve ekonomik olarak sürdürülebilir olmasını sağlamak için operasyonel ve yönetim temsilcilerinin katılımı.

B. Disiplinlerarası iletişim ve koordinasyon süreçleri:

- Düzenli koordinasyon toplantıları:
  - Farklı disiplinler arasında düzenli değişimler kurarak bilgileri sürekli güncellemek ve ayarlamaları gerçek zamanlı tartışmak.
  - Belgeleri, analizleri ve Feedback girdilerii merkezi olarak toplamak ve şeffaf hale getirmek için modern iş birliği araçlarının kullanılması.
- Ortak hedef tanımı:
  - Yapay zekâ kullanımının genel stratejisini hizalamak için hukuki, teknik ve operasyonel gereksinimleri dikkate alan entegre hedef görüntünün formülasyonu.
  - Geliştirilen çözümlerin uygulanmasındaki ilerlemeyi ölçülebilir kılan KPIs (Key Performance Indicators) ve başarı kriterlerinin belirlenmesi. 3. Aşamaya İlişkin

Sonuç

Danışmanlık ve çözüm geliştirme aşamasında, yapay zekâ kullanımı için hukuki, sözleşmesel ve düzenleyici gereklilikleri karşılayan somut, pratik önlemler geliştirilir. Kişiye özel hazırlanmış sözleşme maddelerinin hedefe yönelik oluşturulması, güçlü bir risk yönetimi Framework uygulaması ve kanıtlanmış Best-Practice metodolojilerinin entegrasyonu ile yoğun disiplinlerarası iş birliği sayesinde, veri korumasından sorumluluk konularına ve özel AB düzenlemelerine kadar belirlenen tüm zorlukların kapsamlı ve sürdürülebilir şekilde ele alınması sağlanır. Bu prosedür, Sakizli Legal Modeli'nin sonraki aşamalarında uygulanan önlemlerin başarılı uygulanması ve sonrasında değerlendirilmesi için temel oluşturur.

4. Aşama: Uygulama ve dokümantasyon - ayrıntılı açıklama

Bu aşamada, önceden geliştirilen strateji somut, uygulanabilir önlemlere dönüştürülür. Geliştirilen yasal ve sözleşmesel düzenlemelerin uygulanmasının yanı sıra, tam dokümantasyon ve şeffaf iletişim çok önemlidir. Tüm adımlar sistematik olarak planlanır, uygulanır ve anlaşılır bir şekilde kaydedilir.

1. Eylem planı

C. Adım adım uygulama:

- Detaylı planlama:
  - Bir eylem planı oluşturun: Bireysel önlemleri (örneğin sözleşme revizyonu, yeni veri koruma süreçlerinin getirilmesi, sorumluluk düzenlemelerinin uygulanması) net tanımlanmış çalışma paketlerine dönüştürün.
  - Sorumlulukları ata: Uygulamadan hangi iç departmanların (örneğin, hukuk, BT, Compliance) veya dış ortakların (örneğin, uzman avukatlar, gizlilik uzmanları) sorumlu olduğunu belirleyin.
  - Zaman kilometre taşları: İlerlemeyi sürekli izleyebilmek için somut son tarihler ve ara hedefler belirleyin.
- Risk yönetimi ve yükseltme planları:
  - Risk tanımlama: Teknik entegrasyonlar veya yasal belirsizlikler (örneğin EU AI Act veya GDPR değişiklikleri nedeniyle) ilgili olası uygulama risklerinin ayrıntılı kaydedilmesi.
  - Acil durum stratejileri: Compliance ihlal veya gecikme durumunda yürürlüğe giren yükseltme ve acil durum planları geliştirin.
  - Sürekli Monitoring: Sapmalara erken tepki veren ve ayarlamalara olanak tanıyan Monitoring bir sistemin uygulanması.

B. Kaynak ve bütçe planlaması:

- Kaynak tahsisi:
  - Gerekli insani, finansal ve teknik kaynakların ayrıntılı listesi.
  - İlgili Stakeholder'larla koordinasyon, dar boğazları erken aşamada tespit etmek ve ortadan kaldırmak.
- Bütçeleme:
  - Dış danışmanlık hizmetleri, teknik uygulamalar ve eğitim dahil olmak üzere uygulama için bir bütçe oluşturun.

2. Dokümantasyon

C. Tüm önlemlerin kapsamlı kapsamı:

- Proje dokümantasyonu:
  - Tüm ilgili verileri, ilerlemeyi ve kararları belgeleyen merkezi bir proje Dashboard oluşturulması.
  - Toplantı tutanakları, kararlar ve iç ve dış ortaklarla önemli koordinasyon.
- Yasal izlenebilirlik:
  - Sözleşmeler ve iç politikalardaki tüm düzenlemelerin ilgili yasa ve standartlara (örneğin GDPR maddeleri, EU AI Act bölümlerine atıfta bulunarak) ayrıntılı dokümantasyonu.
  - Gelecekteki Compliance denetimleri için referans olarak risk analizlerini, Audit sonuçlarını ve değerlendirme raporlarını arşivleyin.

B. Reporting yapıları:

- İç raporlar:
  - İlerleme, belirlenen zorluklar ve uyum ihtiyacı hakkında bilgi veren düzenli durum raporları.
  - Uygulanan önlemlerin şeffaf şekilde takip edilmesini sağlayan bir Reporting sisteminin kurulması.
- Dış iletişim:
  - Sonuçların nihai uygulama raporunda belgelenmesi, bu rapor aynı zamanda düzenleyiciler veya ortaklar için kanıt olarak hizmet eder.

3. İletişim stratejisi

C. İç iletişim:

- Bilgi akışını sağlamak:
  - Tüm ilgili Stakeholderları sürekli bilgilendirmek için düzenli toplantılar ve güncellemeler (örneğin atölye çalışmaları veya dijital platformlar şeklinde) düzenlemek.
  - Değişiklikler ve ilerleme hakkında bilgi yaymak için iç iletişim kanallarının (intranet, bülten, iç eğitim) kullanılması.
- Eğitim ve farkındalık artırma:
  - Çalışanları yeni yasal düzenlemeler, veri koruma gereksinimleri ve sorumluluk düzenlemeleri hakkında bilgilendirmek için hedefli eğitim ve atölye çalışmaları düzenlemek.
  - Yeni süreçlerle başa çıkmayı kolaylaştıran rehberler ve FAQ belgeler oluşturulması.

B. Dış iletişim:

- Şeffaf ekran:
  - Alınan önlemlerle ilgili bilgilerin, örneğin basın bültenleri, Whitepapers veya kamu raporları şeklinde yayımlanması.
  - Alınan önlemlere olan güveni artırmak için dış ortaklar ve düzenleyicilerle koordinasyon.
- Stakeholder diyalog:
  - Süreçlerin sürekli optimizasyonuna dış Feedbacki dahil etmek için Feedback mekanizmalarının (örneğin Stakeholder turları, anketler) kurulması.

Sonuç

Sakizli Legal Modeli'nin 4. aşaması, geliştirilen hukuki ve sözleşmesel

ve düzenleyici önlemler. Detaylı bir eylem planı, şeffaf ve kapsamlı dokümantasyon ile net bir iletişim stratejisi, sadece uygulamayı kontrol edip anlaşılır kılmakla kalmaz, aynı zamanda iç ve dış Stakeholder güvenini de güçlendirir. Bu yaklaşım, dinamik bir yasal ortamda gereksinimleri her zaman karşılamak için alınan önlemlerin sürdürülebilir bir uygulaması ve ardından değerlendirilmesi için temel oluşturur.

Aşama 5: Değerlendirme ve takip - detaylı açıklama

Bu son aşamada, uygulanan önlemlerin sürdürülebilir bir etki yaratması ve değişen hukuki, düzenleyici ve teknolojik çerçevelere sürekli olarak uyarlanması sağlanmaktadır. Tüm ilgili hukuki perspektifleri (örneğin GDPR, EU AI Act, telif hakkı, sorumluluk hukuku vb.) dikkate alan sistematik bir değerlendirme ve sürekli iyileştirme süreci oluşturulacaktır.

1. Geri Bildirim ve Review

A. Düzenli değerlendirme döngülerinin oluşturulması:

- Sabit denetim aralıkları:
  - Yeni sözleşme düzenlemelerinin ve Compliance önlemlerinin etkinliğini Monitoring amacıyla üç aylık veya iki yılda bir yapılan gözden geçirmelerin uygulanması.
  - Başarıyı ölçmek için belirli KPIs tanımlayın (örneğin, veri koruma olay sayısı, sözleşme maddesi güncelleme oranı Audit sonuçlar).

B. İç ve dış Stakeholder entegrasyonu:

- İç Review süreçleri:
  - Hukuk departmanı, Compliance yöneticileri, BT güvenliği ve diğer ilgili departmanlarla düzenli toplantılar yapılarak mevcut zorluklar ve iyileştirme potansiyeli görüşülür.
  - Yasal gerekliliklere (örneğin, GDPR, EU AI Act) uyumu doğrulamak için iç Audit süreçleri yürütmek.
- Dış uzman görüşleri ve Audit süreçleri:
  - Alınan önlemlerin objektif değerlendirilmesi için dış uzmanlarla (örneğin veri koruma görevlileri, uzman avukatlar) iş birliği.
  - İç değerlendirmeyi doğrulamak ve optimizasyon fırsatlarını belirlemek için harici Audit süreçleri kullanımı.

C. Sonuçların belgelenmesi ve iletimi:

- Detaylı değerlendirme raporlarının hazırlanması:
  - Tüm Feedback girdileriin, Audit sonuçların ve belirlenen iyileştirme alanlarının tam dokümantasyonu.
  - Bu raporların denetime uygun şekilde arşivlendiğinden ve gelecekteki Compliance denetimler için erişilebilir tutulduğundan emin olun.
- Şeffaf iletişim:
  - Yönetime düzenli iç raporlar ve ilgili dış Stakeholder'larla (örneğin düzenleyici otoritelere) bilgi alışverişi.

2. Özelleştirme ve sürekli optimizasyon

A. Modelin dinamik güncellemesi:

- Yasal değişikliklere duyarlılık:
  - Hukuki durumun ve düzenleyici gelişmelerin (örneğin GDPR değişiklikleri, EU AI Act güncellemeleri veya yeni gereksinimlerin sürekli izlenmesi

DSA/DMA).

- Güncel kalmak için hemen mevzuat değişikliklerini modele dahil edin.

- İçsel süreçlerin uyarlanması:
  - Değerlendirme sonuçlarına göre sözleşmelerin ve iç politikaların revize edilmesi ve optimize edilmesi.
  - Tüm etkilenen çalışanları yeni süreçler ve yasal gereklilikler hakkında bilgilendirmek için atölye çalışmaları ve eğitimler düzenleyin.

B. Lessons Learned Uygulaması:

- Ampirik değerlerin kaydı:
  - Tekrarlayan zorlukları ve başarılı önlemleri belirlemek için değerlendirme raporlarının sistematik analizi.
  - Bu bulguların modelde gelecekteki ayarlamalara entegre edilmesi.
- Risk yönetimi stratejilerinin optimizasyonu:
  - Yeni tespit edilen risklere (örneğin, sorumluluk veya veri koruma olayları) daha hızlı ve etkili yanıt vermek için acil durum planlarını ve yükseltme stratejilerini uyarlayın.

3. Uzun vadeli destek ve Monitoring

A. Sürekli Monitoring sisteminin kurulması:

- Gerçek zamanlı Monitoring:
  - İlgili KPIs ve düzenleyici değişikliklerin sürekli izlenmesi için bir Dashboard geliştirilmesi.
  - Olası Compliance ihlalleri veya düzenleyici uyum ihtiyaçları hakkında erken uyarı sağlamak için Monitoring araçları kullanın.

B. Düzenli Follow-up randevuları:

- Kontrol toplantılarının planlanması ve yürütülmesi:
  - Uygulanan önlemlerin uzun vadeli etkinliğini kontrol etmek için disiplinlerarası ekiplerle düzenli toplantılar.
  - Yasal gerekliliklere sürekli uyumu sağlamak için sorumluluklar belirleyin.

C. Şirkete sürdürülebilir entegrasyon:

- Uzun vadeli destek:
  - Yeni zorluklara sürekli uyum sağlayan ve düzenli güncellemeler yapan kalıcı bir Compliance yönetim sisteminin kurulması.
  - Modelin kurumsal stratejiye entegre edilmesini ve uzun vadeli operasyonlara sabitlenmesini sağlamak.

4. Belgeleme ve Reporting

A. Arşivleme ve revizyon güvenliği:

- Kapsamlı dokümantasyon:
  - Tüm değerlendirme raporları, uyarlama önlemleri ve eğitim belgeleri denetime dayanıklı bir şekilde arşivlenir ve iç ve dış denetimler için kullanılabilir.
- Her döngü için nihai raporun hazırlanması:
  - Tüm sonuçların ve ayarlamaların özeti, gelecekteki değerlendirme döngüleri için referans olarak hizmet eder.

B. Stakeholder'ye iletişim:

- İç Reporting:
  - Önlemlerin ilerlemesi ve etkinliği hakkında şeffaflık sağlamak için düzenli iç güncellemeler ve yönetime raporlar sunulması.
- Dış raporlar:
  - Dış ortakların ve düzenleyicilerin güvenini artırmak için gerekli sonuçlar ve ayarlamalar yayımlanın.

Sonuç

Sakizli Legal Modeli'nin 5. aşaması, uygulanan modelin sürdürülebilir etkinliğini garanti eder

yapılandırılmış ve sürekli bir değerlendirme ve uyum süreciyle ölçülür. Düzenli Feedback, sistematik Review süreçleri, dinamik ayarlamalar ve uzun vadeli destek, değişen ortamda bile tüm hukuki, sözleşmesel ve düzenleyici gerekliliklerin yerine getirilmesini sağlar. Bu, şirketin değişikliklere proaktif şekilde tepki vermesini, riskleri erken aşamada tespit etmesini ve uzun vadede Stakeholder güvenini sağlamasını sağlar.

Uygulama örneği:

Senaryo: Instagram entegrasyonlu RunwyML tabanlı bir yapay zekâ çözümü için danışmanlık

İlk durum:

Müşteriniz, Instagram için sosyal medya stratejisini optimize etmek amacıyla bir yapay zekâ çözümü kullanmayı planlıyor. Çözüm, RunwyML kullanarak veri tabanlı analizler yapmak üzere - örneğin hedef grup adresleme, Content optimizasyonu ve trend tahmini için. Aynı zamanda, veri koruma, sorumluluk, telif hakkı ve düzenleyici Compliance (örneğin GDPR, EU AI Act) açısından yüksek gereksinimler vardır.

Aşama 1: Hazırlık ve Ön Değerlendirme

1. Hedeflerin netleştirilmesi:

- Sözleşmesel ve düzenleyici hedefleri tanımlayın: Müşteriyle birlikte, projede hangi yasal çerçeve koşullarının (örneğin veri koruma, sorumluluk meseleleri, platform APIs kullanımı) uyulması gerektiğini netleştirirsiniz.
- Özel hedefler: Müşteri, yapay zekâ çözümünün sadece teknik olarak verimli olmasını değil, aynı zamanda özellikle Instagram verilerini işlerken, tüm düzenleyici gereksinimlere (GDPR, EU AI Act, eIDAS vb.) uyduğundan emin olmak ister.

2.Bilgi toplama:

- Teknolojik bağlam: RunwyML'nin nasıl çalıştığını analiz edecek ve bu platformun Instagram verilerini nasıl işlediğini açıklayacaksınız.
- Yasal temel: Tüm ilgili yasa ve standartların toplanması ve gözden geçirilmesi: veri koruması (GDPR, eIDAS), telif hakkı (Instagram içeriğiyle ilgili), medya hukuku, sorumluluk düzenlemeleri ve sektöre özgü gereksinimler (EU AI Act, DSA, DMA).
- Stakeholder ve kaynaklar: İç yetkinliklerin (örneğin hukuk departmanınız, BT güvenliği) ve dış uzmanların (veri koruma danışmanları, uzman avukatlar) değerlendirilmesi.

3. Çerçeve koşullarını tanımlayın:

- Proje organizasyonu: Sorumlulukların net atanması (örneğin, teknik entegrasyonu kim denetler, kim hukuki Compliance denetler).
- Zaman ve bütçe planlaması: Tüm gerekli hukuki Review süreçleri ve teknik düzenlemeleri uygulamak için gerçekçi kilometre taşları ve bütçeler belirlemek.

Aşama 2: Analiz ve problem tanımı

1.İhtiyaç analizi:

- Hukuki boşlukların tanımlanması: Instagram ile mevcut sözleşmelerin ve RunwyML kullanımının tüm ilgili yasal gereklilikleri ne kadar kapsadığının analizi.
- Teknik ve hukuki zorluklar: Örneğin, veri işleme süreçlerinin GDPR uyumlu olup olmadığının veya yapay zekâ çözümünün yanlış tahminleri durumunda sorumluluk sorunlarının ortaya çıkıp çıkmayabileceğinin değerlendirilmesi.

2.Risk ve fırsat değerlendirmesi:

- SWOT analiz: Güçlü yönleri (örneğin son teknoloji yapay zekâ teknolojisi), zayıf yönleri (veri güvenliğinde olası boşluklar), fırsatları (erken Compliance kadar rekabet avantajları) ve riskleri (veri ihlali için yüksek para cezaları) belirler.
- Hukuki odak alanları: Veri koruma, telif hakkı, sorumluluk ve EU AI Act'ın özel gereksinimleri gibi konulara özel önem verilir.

3. Önceliklendirme:

- Aciliyet matrisi: Belirlenen riskler (örneğin, yapay zekâ değerlendirmesinde hata durumunda belirsiz sorumluluk kuralları) ilgileri ve gerçekleşme olasılıklarına göre önceliklendirilir; böylece en acil sorunlar (örneğin veri koruma) hemen ele alınır.

Aşama 3: Danışmanlık ve Çözüm Geliştirme

1. Somut çözüm önerilerinin geliştirilmesi:

- Sözleşme taslağı: Sorumluluk meselelerini, veri korumasını (GDPR uyumlu veri işleme) ve telif hakkı meselelerini (Instagram içeriği kullanıldığında) net bir şekilde düzenleyen özel hazırlanmış sözleşme maddelerinin geliştirilmesi.
- Risk azaltma önlemleri: Olası Compliance ihlallerini önlemek için düzenli Audit süreçleri, yükseltme planları ve teknik kontroller gibi önlemleri tanımlayın.

2.En iyi uygulamaların entegrasyonu:

- Best-Practice yöntemler: Tüm ilgili hukuk alanlarını kapsayan standart kontrol listelerinin kullanımı.
- Atölye çalışmaları ve vaka çalışmaları: Somut vaka çalışmalarındaki çözüm ve olası riskler üzerinde pratik ışık tutmak amacıyla disiplinlerarası atölyelerin uygulanması (örneğin Instagram'dan veri ihracası).

3. Disiplinlerarası işbirliği:

- Uzman panelleri: Avukatlar, veri koruma görevlileri ve teknik uzmanların katılımı ile hem hukuki hem de teknik yönlerin en iyi şekilde değerlendirilmesi.

Aşama 4: Uygulama ve dokümantasyon

1.Ma eylem planı:

- Adım adım uygulama: Örneğin Instagram ile sözleşme yapmayı, RunwyML arayüzünü entegre etmeyi ve dahili veri koruma süreçlerini uyarlamayı içeren ayrıntılı bir plan oluşturun.
- Sorumluluklar: Görevlerin iç ekiplere ve dış ortaklara (örneğin, uzmanlaşmış gizlilik avukatları) net şekilde atanması.

2.Dokümantasyon:

- Şeffaf takip: Tüm değişiklikler, toplantılar ve kararlar ayrıntılı şekilde belgelenir - sözleşme düzenlemelerinden teknik uygulama detaylarına kadar.
- Reporting: Uygulamanın ilerlemesini ve herhangi bir zorluku şeffaf kılan yönetime ve ilgili Stakeholder düzenli raporlar.

3.İletişim stratejisi:

- İç iletişim: Tüm etkilenen çalışanlara yeni süreçler ve yasal gereklilikleri iletmek için düzenli güncellemeler ve eğitimler.
- Dış iletişim: ortakları ve uygun olduğunda halkı tüm ilgili gerekliliklere uyum konusunda bilgilendirerek güven inşa etmek.

Aşama 5: Değerlendirme ve takip

1. Geri Bildirim ve Review:

- Düzenli değerlendirme döngüleri: Uygulamadan sonra, tüm önlemlerin (örneğin GDPR uyumu, sorumluluk rejimleri) işe yaradığından emin olmak için, örneğin üç aylık Audit süreçleri boyunca sürekli Monitoring yapılır.
- Stakeholder'ların katılımı: İç ekiplerden ve dış danışmanlardan gelen Feedback girdileri sistematik olarak toplanır ve değerlendirilir.

2. Özelleştirme:

- Dinamik güncelleme: Model sürekli olarak yeni düzenleyici gereksinimlere (örneğin EU AI Act ayarlamaları veya Instagram kullanım şartlarındaki değişiklikler) uyarlanır.
- Lessons Learned: Optimizasyonlar, süreci uzun vadede iyileştirmek için değerlendirme döngülerinden türetilir.

3. Uzun vadeli destek:

- Monitoring: Kalıcı bir Monitoring sistemi, tüm yasal gerekliliklere uyumu sürekli izler ve uyum ihtiyacını erken aşamada belirler.
- Follow-up Randevular: Düzenli toplantılar, çözümün uzun vadeli başarısını ve sürekli gelişimini sağlar.

Sonuç Bu senaryo, "Sakizli Beş Aşamalı Modeli"nin karmaşık bir proje için hukuki, sözleşmesel ve

düzenleyici koruma sağlamak amacıyla bir danışma sürecinde yapılandırılmış bir rehber olarak nasıl kullanıldığını gösteriyor - bu durumda RunwyML ve Instagram entegre eden bir yapay zekâ çözümü. Beş aşamanın tamamını sistematik olarak uygulayarak, müşterinin sadece teknik olarak yenilikçi bir çözüm almasını değil, aynı zamanda tüm ilgili yasal gereklilikleri karşılamasını ve böylece uzun vadede başarılı ve uyumlu şekilde işletilmesini sağlarsınız.

SADECE GEÇERLI HUKUKI SORULARA ŞU ŞEKILDE ATIRILMIŞTIR SENARYOYA GÖRE MODEL OLUN VE GEREKSIZLERI ORTADAN KALDIRIN YÖNLER (MÜŞTERININ DANIŞMANLIK PROJE FIKRINE BAĞLI OLARAK)

DIKKATE ALınmadi. GERÇEKÇI UYGULAMA KESINLIKLE

ODAK EDIN VE MODELIN ÇALIŞTIRILMASININ DERINLIĞINI BELIRLER

Senaryo: "Alex Meier - Bağımsız Influencer" Alex Meier, veriye dayalı Insights kullanarak erişimini ve içeriğinin ek değerini artırmak isteyen yükselen bir Instagram influencer. RunwyML platformunda çalışan ve Instagram hesabıyla doğrudan etkileşime giren bir yapay zekâ çözümü uygulamayı planlıyor. Amacı, Content stratejilerini optimize etmek, trendleri erken belirlemek ve böylece Engagement Rate değerini geliştirmek. Alex, şahıs işletmesi sahibi olarak faaliyet gösterdiği için, GDPR, EU AI Act ve telif hakkı ile medya yasaları gibi tüm yasal ve düzenleyici gerekliliklerin de yerine getirilmesini sağlamalıdır. Tüm proje için bütçesi 15.000 €'dur.

Aşama 1: Hazırlık ve Ön Değerlendirme

1. Hedeflerin netleştirilmesi

- Antlaşma ve düzenleyici hedefler:
  - Alex, Instagram Hizmet Şartlarını ihlal etmeden Instagram aktivitelerini optimize etmek istiyor.
  - Yapay zekâ çözümü, verileri GDPR uyumlu bir şekilde işlemelidir ki uyarı veya para cezası riski çekmez.
  - Sorumluluk konularını - örneğin yanlış eğilim tahminleri durumunda - sözleşmelerde ve iç yönergelerde erken aşamada ele almak istiyor.
- Özel hedefler:
  - 6 ay içinde Engagement Rate %15 artırın.
  - Ayda en az 3 ilgili Content konuyu belirleyen otomatik trend analizi.
  - Tüm veri işlemenin (örneğin Instagram'den) EU AI Act ve GDPR gereksinimlerine uygun olmasını sağlamak.

2. Bilgi toplama

- Teknolojik bağlam:
  - RunwyML platformunun Instagram arayüzleri ve sosyal medya verilerinin işlenmesi açısından analizi.
  - Teknik gereksinimleri kontrol etmek: Alex, entegrasyonu iyi uygulayabilen modern bir akıllı telefon ve dizüstü bilgisayar kullanıyor.
- Hukuki çerçeve:
  - GDPR & eIDAS: Kişisel verilerin (örneğin yorumlar, beğeniler) veri koruma düzenlemelerine uygun şekilde nasıl işlenebileceğinin incelenmesi.
  - EU AI Act: Yapay zekâ çözümünün şeffaflık gereksinimleri ve risk sınıflandırmasının değerlendirilmesi.
  - Telif hakkı ve medya hukuku: Platform üzerinden analiz edilen görüntü ve videoların yasal olarak da kullanılabileceğini garanti etmek.
  - Sorumluluk hukuku: Alex'i olası sorumluluk risklerinden koruyan düzenlemelerin geliştirilmesi (örneğin yanlış analizler durumunda).
- Stakeholder ve kaynaklar:
  - Alex tek işletmeci olarak hareket ettiği için ana sorumluluğu üstlenir.
  - Bir dış veri koruma danışmanı (yaklaşık €2.000) ve teknik entegrasyon için bir Freelancer (yaklaşık €4.000) işe alır - her ikisi de bütçe dahilinde.

3. Çerçeve koşullarını tanımlayın

- Proje organizasyonu:
  - Alex birincil temas noktası olarak kalıyor. Teknik Freelancer ve hukuk danışmanıyla düzenli olarak koordinasyon sağlar.
- Zaman ve bütçe planlaması:
  - Toplam proje süresi: 3 ay.
  - Bütçe tahsisi: dış danışmanlık (veri koruma ve hukuki Review) için yaklaşık €6.000, teknik uygulama için €4.000, atölye çalışmaları ve iç eğitim için €2.000, beklenmedik maliyetler için tampon olarak €3.000.
- Risk yönetimi:

- Yükseltme planının oluşturulması: Veri koruması endişeleri durumunda, dış danışmanla derhal iletişime geçilir.
- Compliance ihlalleri erken aşamada tespit etmek için Monitoring bir sistem (örneğin, düzenli iç Review süreçleri) kurmak.

Aşama 2: Analiz ve problem tanımı

1. İhtiyaç analizi

- Hukuki boşluklar ve zorluklar:
  - Mevcut sözleşmeler: Alex şimdiye kadar sadece iş birliği ortaklarıyla gayri resmi anlaşmalar yaptı - özellikle sorumluluk ve veri koruması konusunda burada yetişmesi gereken çok şey var.
  - Teknik yönler: RunwyML'nin Instagram API kullanımı, askıya alınma veya yasal işlemlerden kaçınmak için mevcut Kullanım Şartlarına uygun olmalıdır.
- Teknik ve hukuki zorluklar:
  - Gizlilik: Tüm kişisel verilerin (takipçi etkileşimlerinin) anonimleştirilmesini veya yeterince korunan şekilde işlenmesini sağlamak.
  - Sorumluluk konuları: Bir hata durumunda kimin sorumlu olduğuna dair net düzenlemeler - Alex son kullanıcı olarak mı yoksa yapay zekâ yanlış önerilerde bulunursa hizmet sağlayıcısı olarak mı seçebilir.
- Stakeholder bakış açıları:
  - Dış veri koruma danışmanı, sosyal medya kanallarından veri toplamada özel risk görür.
  - Teknik Freelancer, olası API sınırlamalarını ve bunların veri kalitesi üzerindeki etkilerini vurgular.

2. Risk ve fırsat değerlendirmesi

- SWOT analizi:
  - Güçlü yönler:
    - Modern teknolojiyle yenilikçi yapay zekâ çözümü (RunwyML).
    - Tek şirket işletmecisi için esneklik ve hızlı karar alma süreçleri.
  - Zayıf yönler:
    - Sınırlı bütçe ve sadece hedefe yönelik risk yönetimine izin verir.
    - Kurum içi hukuk departmanının olmaması, dış danışmanlığı vazgeçilmez kılıyor.
  - Fırsatlar:
    - Veri odaklı Insights ile ulaşım ve etkileşimi artırın.
    - Düzenleyici gereksinimlerin erken uyarlanması yoluyla rekabet avantajları.
  - Riskler:
    - Veri koruma ihlalleri para cezalarına yol açabilir.
    - API yanlış kullanımı nedeniyle Instagram Kullanım Şartlarının olası ihlalleri.
- Önceliklendirme:
  - En öncelikli: veri koruma ve GDPR uyumu (kişisel veriler için kritik).
  - İkinci öncelik: Instagram'ın API spesifikasyonlarına net sorumluluk düzenlemeleri ve teknik Compliance.
  - Düşük öncelik: Yalnızca kamuya açık içerik kullanıldığı sürece telif hakkı sorunları genişletilir.

3. Risklerin önceliklendirilmesi:

- Veri koruma Compliance (GDPR, EU AI Act) en önemli kabul edilir.
- Teknik uygulama sorunları (API Compliance) paralel olarak ele alınır, ancak bütçe yoğunluğu daha düşüktür.

Aşama 3: Danışmanlık ve Çözüm Geliştirme

1. Somut çözüm önerilerinin geliştirilmesi

- Sözleşme taslağı ve yasal düzenlemeler:
  - Veri koruma maddeleri: Instagram verilerinin işlenmesini yöneten ve anonimleştirme ile güvenli depolama garantisi veren özel ifadelerin entegrasyonu.

    - Feragatnameler: Yapay zekâ tarafından yanlış analizler yapıldığında sorumluluğun hariç tutulduğunu veya sınırlandırıldığını belirten maddelerin hazırlanması - düzenli güncellemelere rağmen.
    - API Kullanım Şartları: Instagram API kullanımının Platform Yönergelerine uygun olduğundan emin olmak için teknik Freelancer ile danışma.
- Risk azaltma önlemleri:
    - Teknik önlemler: Veri işlemedeki anormallikleri bildiren otomatik Monitoring aracının uygulanması.
    - Eğitim ve farkındalık: Alex'i tüm ilgili GDPR gereksinimlerine duyarlı hale getirmek için veri koruma danışmanıyla birlikte küçük bir atölye (yaklaşık €500) düzenlemek.

2. En iyi uygulamaların entegrasyonu:

- Kontrol listeleri: Tüm kritik noktaları (GDPR, EU AI Act, Instagram API) kapsayan bir kontrol listesinin oluşturulması.
- Best-Practice belgeleri: Diğer influencerlar veya küçük işletmeler tarafından başarıyla kullanılan şablonlar ve rehberler kullanın.

3. Disiplinlerarası işbirliği:

- Dış uzmanlar:
    - Bir veri koruma danışmanı (bütçe yaklaşık €2.000) nihai veri koruma maddelerini inceler.
    - Teknik Freelancer (bütçe yaklaşık €4,000) kurallara uygun API entegrasyonu sağlar.
- Düzenli oylama:
    - Alex, teknik Freelancer ve veri koruma danışmanı arasında haftalık görüşmeler (Zoom aracılığıyla) ilerlemeyi takip etmek ve değişikliklere kısa sürede tepki vermek için yapılır.

Aşama 4: Uygulama ve dokümantasyon

1. Eylem planı ve uygulama:

- Adım adım plan:
    - 1-2. haftalar: Detaylı planlama, sözleşme taslağı ve gerekli tüm bilgilerin toplanması.
    - 3-6. Hafta: RunwyML arayüzünün teknik entegrasyonu ve Instagram ile veri iletiminin ilk testleri.
    - 7-10. hafta: İlk test sonuçlarına göre sözleşmeler ve iç süreçlerin ayarlanması.
    - 11-12. Hafta: Son Go-live ve Alex'e devr.
- Sorumluluklar:
    - Alex projeyi koordine eder ve nihai kararları verir.
    - Teknik Freelancer arayüzleri uygularken, veri koruma danışmanı hukuki yönleri kontrol eder.

2. Dokümantasyon:

- Proje Dashboard:
    - Tüm dönüm noktaları, kararlar ve değişiklikler merkezi bir Dashboard (örneğin Trello veya Asana) kaydedilir.
    - Haftalık görüşmelerin dakikaları arşivlenir.
- Yasal belgeler:
    - Sözleşmeler ve veri koruma yönergeleri, ilgili hukuki maddelere (örneğin GDPR madde 5, EU AI Act gereksinimlerine çapraz referanslar dahil) denetlenmeye dayanıklı bir şekilde saklanır.

3. İletişim stratejisi:

- İç iletişim:
    - Alex, ilerleme ve herhangi bir sorun hakkında bilgilendirilmek için haftalık güncellemeleri e-posta ve kısa video toplantılarla alır.
- Dış iletişim:
    - Kamuya açık sorgular varsa (örneğin iş birliği ortakları veya takipçilerden), tüm yasal gerekliliklere uyumu doğrulayan hazırlanmış açıklamalar vardır.

Aşama 5: Değerlendirme ve takip

1. Geri Bildirim ve Review:

- Düzenli değerlendirme döngüleri:
  - Yapay zekâ çözümünün işleyişini, GDPR uyumunu ve sözleşme maddelerinin etkinliğini kontrol etmek için tüm taraflarla birlikte aylık Review süreçleri (video görüşme şeklinde).
- Ölçülebilir KPIs:
  - Engagement Rate: Amaç, ilk 6 ay içinde %15 artmaktır.
  - Veri koruma olaylarının sayısı: Amaç sıfır olay.
  - Teknik performans: %99 sistem kullanılabilirliği ve sorunsuz API entegrasyonu.

2. Uyum ve sürekli optimizasyon:

- Dinamik Güncelleme:
  - Instagram Kullanım Şartlarında değişiklikler veya yeni yasal gereklilikler (örneğin EU AI Act kapsamındaki değişiklikler) durumunda, sözleşmeler ve süreçler derhal ayarlanacaktır.
  - Aylık Review süreçleriden Lessons Learned tüm ayarlamaların izlenebilir olmasını sağlayan bir güncelleme belgesine dahil edilir.

3. Uzun vadeli destek:

- Monitoring sistemi:
  - Tüm ilgili KPIs gerçek zamanlı Monitoring amacıyla kalıcı bir Monitoring Dashboard kurulmuştur.
- Follow-up tarihleri:
  - Proje tamamlandıktan sonra (3 ay sonra), yasal gerekliliklere uzun vadeli uyumu sağlamak ve çözümün daha da geliştirilmesini sağlamak için üç aylık Follow-up toplantıları düzenlenir. Senaryo Özeti Alex Meier, serbest çalışan bir influencer, sosyal medya stratejisini RunwyML ve Instagram tabanlı bir yapay zekâ çözümüyle optimize etmek istiyor. "Sakizli Beş Aşamalı Modeli" yardımıyla

aşağıdaki kurgusal cevapları ve kıyaslamaları içeren bir proje planı geliştirmiştir:

1. Aşama 1 - Hazırlık ve Ön Değerlendirme:

- Net hedef tanımı: Katılımı %15 artırın, GDPR uyumlu veri işleme ve sorumluluk risklerinin güvence altına alınması.
- Instagram, GDPR, EU AI Act, telif hakkı ve sorumluluk konularını dikkate alarak tüm ilgili teknik ve hukuki temellerin toplanması.
- Net bütçe ve zaman planlaması ile proje organizasyonu (3 ay, €15.000).

2. Aşama 2 - Analiz ve problem tanımı:

- Önceki sözleşmelerdeki boşlukların ve API kullanımındaki belirsizliklerin tespit edilmesi.
- Veri koruması ve sorumluluğu en yüksek riskler olarak sınıflandıran SWOT bir analiz yapmak.
- Riskleri önceliklendirin ki veri koruması (GDPR, EU AI Act) önce ele alınsın.

3. Aşama 3 - Danışmanlık ve Çözüm Geliştirme:

- Sorumluluk ve veri işlemeyi korumak için somut sözleşme maddeleri ve veri koruma yönergelerinin geliştirilmesi.
- Instagram API yönergelerine uymak ve RunwyML'yi entegre etmek için teknik önlemler.
- Alex, teknik Freelancer ve dış veri koruma danışmanı arasında düzenli koordinasyon.

4. Aşama 4 - Uygulama ve dokümantasyon:

- 12 haftalık bir zaman diliminde, net kilometre taşları ve sorumluluklarla uygulama.
- Tüm proje adımlarının ayrıntılı dokümantasyonu ve haftalık güncellemelerle şeffaf iletişim.
- Bir proje panosu oluşturulması ve tüm yasal belgelerin denetim amaçlı arşivlenmesi.

5. Aşama 5 - Değerlendirme ve takip:

- Aylık Review süreçleri ve ölçülebilir KPIs (etkileşim, sistem kullanılabilirliği, gizlilik olayları).
- Yeni yasal gereksinimlere ve değerlendirme döngülerinden Lessons Learned sürekli uyum sağlama.

- Uzun vadeli bir Monitoring ve üç aylık Follow-up toplantısı kuruldu. Bu senaryo, Alex Meier'in sınırlı bütçeye ve tek işletme olarak yapay zekâ çözümünü yasal uyumlu bir şekilde başarıyla uygulamak için "Sakizli Beş Aşamalı Modeli"ni nasıl kullandığını gösteriyor. Bu, teknik yeniliğin gerekli yasal korumayla el ele gitmesini ve elde ettiği verilerden sürdürülebilir şekilde faydalanmasını Insights sağlar.

PRATIK KULLANIM IÇIN ÖRNEK CEVAPLARLA BIRLIKTE ANKET OF MODEL:

Aşama 1: Hazırlık ve Ön Değerlendirme

Sorular

1. Proje ve hedef netleştirme:

- Soru: Planlanan yapay zekâ çözümüyle ilgili birincil hedefleriniz nelerdir? Örnek cevap: "Instagram Engagement Rate değerimi %15 artırmak ve Content stratejimi optimize etmek için veri odaklı Insights almak istiyorum."
- Soru: Hangi sözleşmesel ve düzenleyici hedeflere ulaşılacak? Örnek cevap: "Çözüm GDPR uyumlu olmalı, sorumluluk konularını net bir şekilde düzenlemeli ve Instagram verilerin yasal olarak güvenli şekilde kullanılmasını mümkün kılmalıdır."

2. Bilgi toplama (teknik ve hukuki bağlam):

- Soru: Hangi teknik sistemler ve platformlar kullanılır (örneğin RunwyML, Instagram)? Örnek cevap: "Yapay zekâ çözümünü RunwyML platformu üzerinden uygulamayı planlıyorum, doğrudan Instagram hesabıma bağlanacak şekilde."
- Soru: Projeniz için hangi yasal gereklilikler geçerli? Örnek cevap: "GDPR, EU AI Act, eIDAS, telif hakkı ve medya hukuku ile API kullanımlarla ilgili sorumluluk konuları önemlidir."
- Soru: Mevcut hangi sözleşmeler, yönergeler veya iç düzenlemeler zaten yürürlükte bulunuyor? Örnek cevap: "Tek işletmeci olarak, şimdiye kadar iş birliği ortaklarıyla gayri resmi anlaşmalar yaptım ancak resmi olarak güvence altına alınan sözleşme olmadı."

3. Çerçeve koşullarını tanımlayın:

- Soru: İç ve dış Stakeholder kimler (örneğin teknik Freelancer, veri koruma danışmanları)? Örnek cevap: "Tek işletme sahibi olarak çalışıyorum ve dış bir veri koruma danışmanı ile teknik bir Freelancer işe alıyorum."
- Soru: Bütçeniz nedir ve zaman dilimi nedir? Örnek cevap: "Toplam bütçem yaklaşık 15.000 € ve bunu 3 ay boyunca uygulamayı planlıyorum."
- Soru: Dahili olarak hangi kaynaklar mevcut? Örnek cevap: "Modern bir akıllı telefonum ve dizüstü bilgisayarım var, ama başka türlü dış uzmanlar kullanıyorum."

Aşama 2: Analiz ve problem tanımı

Sorular

1. İhtiyaç analizi ve eksikliklerin tanımlanması:

- Soru: Şu anda mevcut sözleşmelerinizde ve süreçlerinizde hangi hukuki boşlukları veya zorlukları görüyorsunuz? Örnek cevap: "Sorumluluk rejiminde boşluklar var ve Instagram verilerinin kullanımıyla ilgili net gizlilik maddeleri eksikliği var."
- Soru: RunwyML platformunu Instagram ile entegre ederken hangi teknik zorluklarla karşılaşmayı bekliyorsunuz? Örnek cevap: "Instagram API kullanımı mevcut politikalara uygun olmalı ve veri tutarsızlıkları riski vardır."

2.Risk ve fırsat değerlendirmesi:

- Soru: Hangi riskleri (örneğin veri koruma ihlalleri, sorumluluk riskleri) özellikle yüksek olarak görüyorsunuz? Örnek cevap: "En büyük risk, özellikle takipçilerin kişisel verilerinin işlenmesinde veri koruma alanındadır."
- Soru: YZ çözümünün uygulanması işletmeniz için hangi fırsatlar sunuyor? Örnek cevap: "Veri odaklı Insights sayesinde, ulaşımda önemli bir artış ve bana rekabet avantajı sağlayan gelişmiş Content stratejileri bekliyorum."
- Soru: Bu riskleri ve fırsatları nasıl önceliklendirirsiniz? Örnek cevap: "Gizlilik ve sorumluluk konuları önceliklidir, ardından teknik API gereksinimleri gelir."

3.Stakeholder bakış açıları:

- Soru: Dış danışmanlarınızın (örneğin veri koruma uzmanları, teknik Freelancer) projeden beklentileri nelerdir? Örnek cevap: "Veri koruma danışmanım katı GDPR uyumlu önlemlerin gerekliliğini vurgularken, teknik Freelancer uyumlu API kullanımını işaret ediyor."

Aşama 3: Danışmanlık ve Çözüm Geliştirme

Sorular

1. Somut çözüm önerilerinin geliştirilmesi:

- Soru: Sorumluluk konularını ve veri korumasını korumak için hangi sözleşmesel düzenlemeler yapmayı planlıyorsunuz? Örnek cevap: "Instagram verilerinin işlenmesini düzenleyen özel veri koruma maddelerine ve yanlış analizler durumunda geçerli olan feragatnamelere ihtiyacım var."
- Soru: Platform politikalarına uyumu sağlamak için hangi teknik önlemler uygulanmalıdır? Örnek cevap: "Veri transferlerini izleyen ve API kullanım şartlarını dikkate alan otomatik bir Monitoring aracı kurulmalıdır."

2.En iyi uygulamaların entegrasyonu:

- Soru: Çözüm geliştirme sürecine hangi Best-Practice yöntemleri veya kontrol listelerini entegre etmek istiyorsunuz? Örnek cevap: "Tüm kritik alanları (GDPR, EU AI Act, Instagram API) kapsayan standart kontrol listeleri kullanmak istiyorum."
- Soru: Teknik ve hukuk uzmanları arasındaki disiplinlerarası değişimi nasıl öngörüyorsunuz? Örnek cevap: "Benim, teknik Freelancer ve veri koruma danışmanım arasındaki haftalık koordinasyon görüşmeleri, tüm yönlerin en iyi şekilde koordine edilmesini sağlamak için tasarlanmıştır."

Aşama 4: Uygulama ve dokümantasyon

Sorular

1.Ma Eylem Planı ve Uygulama:

- Soru: Uygulama zaman çizelgesi nasıl olmalı (örneğin, dönüm noktaları, son teslim tarihleri)? Örnek cevap: "12 haftalık bir dönem planlıyorum: 2 hafta planlama, 4 hafta teknik entegrasyon ve ilk test, 4 hafta özelleştirme ve 2 hafta son Go-live."
- Soru: Projede kim hangi sorumlulukları üstlenir? Örnek cevap: "Ben ana iletişim noktası olarak kalıyorum, teknik Freelancer API entegrasyonunu uygular ve veri koruma danışmanı hukuki Reviewyi yürütüyor."

2.Dokümantasyon:

- Soru: Proje yönetimi ve dokümantasyon için hangi araçları kullanmak istiyorsunuz? Örnek cevap: "Proje yönetimi için Trello veya Asana gibi araçları kullanıyorum ve tüm yasal belgeleri denetime dayanıklı bir şekilde bulutta saklıyorum."
- Soru: İlerleme ve uyum nasıl belgelenmeli? Örnek cevap: "Haftalık raporlar, koordinasyon toplantılarının tutanakları ve merkezi bir proje gösterge paneli, ilerlemeyi şeffaf şekilde izlenebilir hale getirir."

3.İletişim stratejisi:

- Soru: Uygulama sırasında iç ve dış iletişim nasıl organize edilmelidir? Örnek cevap: "İç güncellemeler haftalık olarak e-posta ve kısa video toplantılarla sağlanırken, hazırlanmış açıklamalar dış talepler için kullanılır."

Aşama 5: Değerlendirme ve takip

Sorular

1. Geri Bildirim ve Review:

- Soru: Değerlendirme ve Feedback toplantıları ne sıklıkla yapılmalı? Örnek cevap: "İlerleme kontrolünü kontrol etmek ve optimizasyon potansiyelini belirlemek için aylık Review süreçlerii video görüşmesiyle planlıyorum."
- Soru: Başarıyı ölçmek için hangi KPI'ların kritik olduğunu düşünüyorsunuz (örneğin Engagement Rate, sistem erişilebilirliği, veri koruma olayları)? Örnek cevap: "Temel KPI'lar Engagement Rate'de %15 artış, %99 sistem kullanılabilirliği ve sıfır veri ihlalidir."

2.Özelleştirme ve sürekli optimizasyon:

- Soru: Yeni düzenleyici değişikliklere veya teknik zorluklara nasıl yanıt vermeyi planlıyorsunuz? Örnek cevap: "Düzenli Review süreçleri ve Monitoring sisteminin kurulmasıyla ayarlamalar hızlıca uygulanır."
- Soru: Lessons Learned gelecekteki proje aşamalarına nasıl dahil edilecek? Örnek cevap: "gözden geçirmelerin sonuçları bir güncelleme belgesinde özetlenir ve sonraki proje aşamaları için temel

olarak kullanılır."

3. Uzun vadeli destek:

- Soru: Proje tamamlandıktan sonra hangi Follow-up önlemleri almayı planlıyorsunuz? Örnek cevap: "Go-live sonrası, uzun vadeli uyumu sağlamak için üç aylık Follow-up toplantıları düzenlenecektir."
- Soru: Çözümün Monitoring uzun vadede nasıl garanti edilecek? Örnek cevap: "Tüm ilgili KPIs gerçek zamanlı Monitoring amacıyla kalıcı bir Monitoring Dashboard kurulacak."

Özet Bu anket, hedef netleştirmeden risk analizine, çözüm geliştirmeye, uygulama ve değerlendirmeye kadar tüm ilgili konuları kapsar. Sakizli Legal Modeli'nde en iyi şekilde kullanabileceğiniz kapsamlı bilgileri müşterilerinizden (influencerlar, küçük işletmeler veya büyük kuruluşlar olsun) alabileceğiniz yapılandırılmış bir şablon sunar. Örnek cevaplar, tipik müşteri ihtiyaçlarının nasıl görünebileceğine dair gerçekçi bir fikir verir ve modelin bireysel olarak uyarlanmasına yardımcı olur.