Araba Kiralama Şirketi için Müşteri Migrasyonu ve Ehliyet Doğrulama

1. Giriş

Bu projede, bir araba kiralama firmasının hali hazırda kullandığı mevcut uygulamadan, 50.000 müşterinin yeni bir uygulamaya taşınması ve müşterilerin ehliyet bilgilerinin Emniyet Genel Müdürlüğü (EGM) sisteminden doğrulanması hedeflenmektedir. Proje, müşteri verilerinin güvenli bir şekilde yeni sisteme aktarılmasını ve aynı zamanda ilgili mevzuatlara uygun bir şekilde kimlik doğrulama işlemlerinin yapılmasını kapsamaktadır.

2. Proje Hedefleri

- 50.000 müşterinin mevcut sistemden yeni sisteme veri kaybı olmadan taşınması.
- EGM sisteminden entegrasyon sağlanarak müşterilerin ehliyet bilgilerinin doğrulanması.
- Veri güvenliği ve KVKK uyumluluğunun sağlanması.
- Kullanıcı deneyimini bozmadan hızlı ve sorunsuz bir geçiş sürecinin tamamlanması.

3. Aksiyon Planı ve Yöntemler

3.1 Mevcut Sistem ve Yeni Sistem Analizi

- **Mevcut Verilerin İncelenmesi:** Müşteri bilgileri, kiralama geçmişi, ödeme bilgileri ve ehliyet bilgileri analiz edilmiştir. Bu verilerin yeni sistemdeki karşılıkları tespit edilmiştir.
- **Yeni Sistem Tasarımı:** Veritabanı yapısı, kullanıcı arayüzü ve entegrasyon süreçleri, yeni sisteme uygun hale getirilmiştir.

3.2 Veri Migrasyonu Planı

3.2.1 Veri Temizliği

- **Eksik ve Hatalı Verilerin Belirlenmesi:** Migrasyon öncesinde tüm müşteri verileri analiz edilerek eksik veya hatalı bilgiler tespit edilmiştir. Eksik veriler tamamlanmış, hatalı veriler düzeltilmiştir.

3.2.2 Veri Transferi

- **Toplu İşleme Yöntemi:** Veri transferi, 10.000 müşteri olacak şekilde beş aşamalı toplu işleme yöntemiyle gerçekleştirilmiştir. Her bir grup transfer edildikten sonra doğrulama testleri yapılmıştır.

- **Veri Güvenliği:** Tüm veri aktarım süreçleri, şifrelenmiş bağlantılar (HTTPS) üzerinden gerçekleştirilmiş ve KVKK'ya uygun veri işleme prosedürleri uygulanmıştır.

3.2.3 Test ve Doğrulama

- **Doğrulama Testleri:** Her bir veri transferi sonrasında, yeni sistemdeki müşteri bilgileri eski sistemdeki verilerle karşılaştırılarak tutarlılığı kontrol edilmiştir.

3.3 Ehliyet Doğrulama Entegrasyonu

3.3.1 API Erişimi

- **EGM ile İletişim:** Emniyet Genel Müdürlüğü ile yapılan resmi prosedürler sonucunda, ehliyet doğrulama API erişim bilgileri temin edilmiştir.

3.3.2 API Kullanımı

- **Doğrulama Süreci:** Her müşterinin TC kimlik numarası ve ehliyet numarası üzerinden EGM sistemine sorgu gönderilerek doğrulama yapılmıştır. Bu süreç, müşteri kaydı sırasında ve veri migrasyonu sonrasında otomatik olarak gerçekleştirilmiştir.

3.4 Pilot Test ve Kullanıcı Eğitimi

- **Pilot Uygulama:** 1000 müşterilik bir grup üzerinde pilot testler yapılmış, müşterilerin yeni sisteme adaptasyonu ve ehliyet doğrulama entegrasyonu başarılı bir şekilde test edilmiştir.
- **Kullanıcı Eğitimi:** Yeni sisteme geçiş sonrasında, kullanıcıların uygulamayı sorunsuz kullanabilmeleri için rehber dokümanlar ve e-posta bilgilendirmeleri hazırlanmış ve gönderilmiştir.

4. Veri Güvenliği ve KVKK Uyumluluğu

- **KVKK Uyumluluğu:** Kullanıcıların tüm kişisel bilgileri, Kişisel Verilerin Korunması Kanunu'na uygun olarak işlenmiş, depolanmış ve taşınmıştır. Hassas verilerin güvenli bir şekilde saklanması için şifreleme ve erişim kontrol önlemleri uygulanmıştır.
- **Veri Güvenliği:** Tüm veriler şifrelenmiş kanallar üzerinden aktarılmış, yetkisiz erişimlere karşı güvenlik duvarları ve kimlik doğrulama yöntemleri kullanılmıştır.

5. Sonuç ve Değerlendirme

Bu proje kapsamında, 50.000 müşterinin verileri başarılı bir şekilde eski sistemden yeni sisteme taşınmıştır. EGM ile entegrasyon sağlanarak ehliyet doğrulama süreci etkili bir şekilde yürütülmüştür. Verilerin bütünlüğü ve güvenliği korunarak, kullanıcı memnuniyeti yüksek seviyede tutulmuş ve sistem sorunsuz bir şekilde devreye alınmıştır.

Migrasyon sürecinde, kullanıcıların sisteme adaptasyonu sağlanmış ve geçiş sonrası kullanıcı desteği sağlanmıştır. Tüm süreç boyunca veri güvenliği ve yasal uyumluluk gereksinimlerine uygun hareket edilmiştir.

Ek Bilgiler (Opsiyonel):

- **Projede Kullanılan Teknolojiler:** Veri tabanı (MySQL), API entegrasyonu (REST API), Güvenlik (SSL/TLS, KVKK uyumlu veri işleme).
- **İletişim Bilgileri:** Proje ile ilgili herhangi bir sorunuz için benimle iletişime geçebilirsiniz: [neslihankizilaslan@gmail.com].

EGM ile İletişime Geçme Süreci ve API Erişim İzni Detayları

Müşteri ehliyet bilgilerinin doğrulanabilmesi için Emniyet Genel Müdürlüğü (EGM) ile resmi bir entegrasyon sağlanması gerekmektedir. Bu süreç, aşağıdaki adımlar çerçevesinde yürütülmüştür:

1. Ön Hazırlık ve Gereksinimlerin Belirlenmesi

Öncelikle, EGM ile yapılacak entegrasyonun amacı, kapsamı ve teknik gereksinimleri belirlenmiştir:

- **Amaç**: Araba kiralama şirketinin müşterilerinin ehliyet bilgilerinin doğrulanması.
- **Kapsam**: Müşteri ehliyet bilgileri (ehliyet numarası, TC kimlik numarası, doğum tarihi) gibi kritik verilerin doğrulanması.
- **Teknik Gereksinimler**: API erişimi, güvenlik protokolleri (şifreleme, kimlik doğrulama), veri formatı (JSON, XML vb.).

2. EGM ile Resmi İletişim Kurulması

EGM ile resmi API erişimi sağlayabilmek için aşağıdaki adımlar izlenmiştir:

2.1. Başvuru Hazırlığı

Resmi bir kurumla iletişim kurmadan önce, başvuru için gerekli belgeler ve bilgilerin hazırlanması gerekir:

- **Kurumsal Bilgiler**: Şirketin vergi numarası, ticaret sicil bilgileri, adresi ve diğer yasal bilgiler.
- **Proje Bilgileri**: Ehliyet doğrulama projesinin amacı, hedefleri ve kapsamı.
- **Teknik Belgeler**: Uygulamanın nasıl çalıştığını açıklayan teknik dökümanlar ve API entegrasyonu ile ilgili teknik gereksinimler.

Bu hazırlık sürecinde, proje yöneticisi veya teknik lider sorumluluğunda gerekli belgeler derlenmiş ve doğruluğu kontrol edilmiştir.

2.2. İlgili Birimlerle İletişim

EGM bünyesinde ehliyet ve kimlik doğrulama işlemleri için kullanılan veri tabanı ve API hizmetleri, genellikle **Bilgi Teknolojileri Dairesi Başkanlığı** tarafından yönetilmektedir. Aşağıdaki yöntemlerle resmi iletişim başlatılmıştır:

- **Resmi Yazı ile Başvuru**: Kurumdan API erişimi talep etmek için yazılı bir başvuru yapılmıştır. Bu yazı, projenin detaylarını, entegrasyon gereksinimlerini ve şirket bilgilerini içermiştir.
- **Elektronik Başvuru**: EGM'nin elektronik başvuru sistemi (genellikle e-Devlet üzerinden veya EGM'nin resmi internet sitesi üzerinden) aracılığıyla entegrasyon talebinde bulunulmuştur. Bu başvuru sırasında, proje bilgileri ve teknik detaylar sunulmuştur.

2.3. Görüşmeler ve Onay Süreci

Başvurunun ardından, EGM yetkilileriyle çeşitli görüşmeler yapılmıştır. Bu görüşmelerde:

- **API Kullanım Amacı**: Müşterilerin ehliyet bilgilerinin doğrulanmasının neden gerektiği açıklanmıştır. Araba kiralama süreçlerinde ehliyet doğrulama ihtiyacı ve dolandırıcılıkları önleme amacı detaylandırılmıştır.
- **Veri Güvenliği Önlemleri**: Şirketin veri güvenliği politikaları ve KVKK uyumlu veri işleme prosedürleri hakkında bilgi verilmiştir. API entegrasyonunun güvenli bir şekilde yapılacağı ve kullanıcı verilerinin koruma altına alınacağı belirtilmiştir.

3. Teknik Detaylar ve Test Ortamı Sağlanması

EGM, başvuruyu onayladığında, teknik belgeler ve entegrasyon dokümanları sağlanmıştır. Bu aşamada:

- **API Dökümanları**: EGM tarafından verilen API dökümanları incelenmiş ve gerekli parametreler belirlenmiştir. Bu dokümanlar, API uç noktaları, istek/yanıt formatları, kimlik doğrulama yöntemleri (örneğin OAuth 2.0 gibi) ve kullanım limitleri hakkında bilgi içermektedir.
- **Test Ortamı (Sandbox)**: EGM, genellikle entegrasyon öncesinde geliştiricilerin test yapabilmesi için bir test ortamı (sandbox) sunar. Bu ortam, gerçek verilere erişmeden API'yi test etmek ve entegrasyonun düzgün çalıştığından emin olmak için kullanılmıştır.

4. Güvenlik ve Uyum Protokolleri

API entegrasyon sürecinde, EGM'nin güvenlik gereksinimlerine uygun olarak aşağıdaki önlemler alınmıştır:

- **SSL/TLS Şifrelemesi**: Tüm API talepleri ve yanıtları SSL/TLS şifrelemesi ile korunmuştur.
- **Kimlik Doğrulama**: EGM'nin sunduğu API'yi kullanabilmek için kimlik doğrulama anahtarları (API Key veya OAuth) kullanılmıştır. Bu anahtarlar, yalnızca yetkilendirilmiş uygulamalara erişim izni vermektedir.

- **Veri Gizliliği**: Kullanıcıların ehliyet bilgileri yalnızca doğrulama amacıyla kullanılmış ve üçüncü taraflarla paylaşılmamıştır. Verilerin sadece gerekli olan kısımları işlenmiş, hassas bilgiler korunmuştur.

5. Entegrasyon ve Canlıya Alma

Tüm testler başarıyla tamamlandıktan sonra, EGM'nin API'si canlı sisteme entegre edilmiştir:

- **Gerçek Ehliyet Doğrulama İşlemleri**: Artık sistem, müşteri kayıtları sırasında girilen ehliyet bilgilerini EGM'nin sisteminden doğrulamakta ve kiralama işlemleri sırasında müşterilerin ehliyet geçerliliğini kontrol etmektedir.
- **Sürekli İzleme**: API entegrasyonunun doğru çalıştığından emin olmak için izleme araçları kullanılmış ve EGM ile iletişim halinde kalarak herhangi bir kesinti veya sorun anında çözülmüştür.

KVKK Kapsamında Müşteri Verilerine Erişim ve Güvenlik Alternatifleri

1. Rol Tabanlı Erişim Kontrolü (RBAC)

1.1. Kişi Bazlı Erişim Yetkisi

Tanım: Kullanıcıların veriye erişim yetkilerini belirli roller üzerinden kontrol etme yöntemidir.

Uygulama Adımları:

- Kullanıcıları, uygulama içindeki rollerine göre gruplandırın.
- Her rol için veri erişim yetkileri tanımlayın.
- Yalnızca yetkili rol sahiplerinin belirli verilere erişmesini sağlayın.

Notlar:

- Erişim yetkilerinin düzenli olarak gözden geçirilmesi ve güncellenmesi önemlidir.

1.2. Yetki Seviyeleri

Tanım: Kullanıcıların veri üzerinde gerçekleştirebileceği işlemleri sınırlandıran erişim seviyeleridir.

Uygulama Adımları:

- Erişim seviyelerini belirleyin (okuma, yazma, düzenleme vb.).
- Bu seviyeleri kullanıcının görevleri ile ilişkilendirin.

- Gereksiz erişimleri engelleyin.

Notlar:

- Erişim seviyeleri belirli aralıklarla güncellenmelidir.

2. Loglama ve İzleme

2.1. Erişim Logları

Tanım: Verilere kimlerin, ne zaman ve hangi işlemleri gerçekleştirdiğini kaydeden sistemlerdir.

Uygulama Adımları:

- Erişim ve işlem loglarını düzenli olarak oluşturun ve saklayın.
- Logları düzenli olarak gözden geçirin ve şüpheli aktiviteleri tespit edin.

Notlar:

- Logların düzenli olarak yedeklenmesi önerilir.

2.2. Olay İzleme

Tanım: Güvenlik olaylarını gerçek zamanlı olarak izleme yöntemidir.

Uygulama Adımları:

- Olay izleme sistemleri kurarak güvenlik tehditlerini ve anormal aktiviteleri tespit edin.
- Uyarı sistemleri oluşturarak hızlı müdahaleyi sağlayın.

Notlar:

- Olay izleme sistemlerinin sürekli güncellenmesi gerekir.

3. Veri Şifreleme

3.1. Veri Dinamik Şifreleme

Tanım: Verinin hem saklama hem de iletim aşamalarında şifrelenmesidir.

Uygulama Adımları:

- Hem veri at rest (saklama) hem de veri in transit (iletim) sırasında şifreleme yöntemlerini kullanın.
- Şifreleme anahtarlarını güvenli bir şekilde yönetin.

Notlar:

- Şifreleme anahtarlarının yönetimi çok önemlidir.

3.2. Şifreleme Anahtarları

Tanım: Şifreleme işlemleri için kullanılan anahtarların yönetimi ve korunmasıdır.

Uygulama Adımları:

- Şifreleme anahtarlarını güvenli bir ortamda saklayın.
- Anahtar erişimini sıkı bir şekilde kontrol edin.

Notlar:

- Anahtar yönetimi için düzenli denetimler yapılmalıdır.

4. Güvenli Veri Erişim Araçları

4.1. VPN ve Güvenli Bağlantılar

Tanım: Verilere erişim sağlanırken kullanılan güvenli bağlantı yöntemleridir.

Uygulama Adımları:

- VPN kullanarak veri erişimini güvenli hale getirin.
- Veri iletiminde güvenli protokoller (örneğin, HTTPS) kullanın.

Notlar:

- VPN bağlantılarının sürekli izlenmesi ve güncellenmesi gereklidir.

4.2. Kimlik Doğrulama ve Yetkilendirme

Tanım: Kullanıcıların kimliklerini doğrulama ve erişim yetkilerini kontrol etme yöntemidir.

Uygulama Adımları:

- Çok faktörlü kimlik doğrulama (MFA) kullanarak erişim güvenliğini artırın.
- Yetkilendirme politikalarını düzenli olarak gözden geçirin.

Notlar:

- MFA sistemlerinin sürekli güncellenmesi önemlidir.

5. Veri Maskelenmesi ve Anonimleştirme

5.1. Veri Maskelenmesi

Tanım: Hassas verilerin anonimleştirilmiş verilerle değiştirilmesidir.

Uygulama Adımları:

- Test ve geliştirme ortamlarında veri maskelenmesi uygulayın.
- Gerçek verilerin yerine anonimleştirilmiş veriler kullanın.

Notlar:

- Veri maskelenmesi sürecinin düzenli olarak gözden geçirilmesi gerekir.

5.2. Anonimleştirme

Tanım: Veriyi anonimleştirerek kişisel bilgilerin tanımlanabilirliğini azaltma yöntemidir.

Uygulama Adımları:

- Kişisel verilerin anonimleştirilmesi için teknik ve organizasyonel önlemler alın.

Notlar:

- Anonimleştirilmiş verilerin de güvenliğinin sağlanması önemlidir.

6. Erişim Politikaları ve Eğitim

6.1. Güvenlik Politikaları

Tanım: Kullanıcılar için veri erişim ve güvenlik kurallarının belirlenmesidir.

Uygulama Adımları:

- Erişim ve güvenlik politikalarını açıkça tanımlayın.
- Politikaları düzenli olarak gözden geçirin ve güncelleyin.

Notlar:

- Politikaların tüm kullanıcılar tarafından anlaşılması sağlanmalıdır.

6.2. Eğitim

Tanım: Kullanıcıların güvenlik protokolleri ve en iyi uygulamalar konusunda bilgilendirilmesidir.

Uygulama Adımları:

- Kullanıcılara düzenli güvenlik eğitimi verin.
- Eğitim materyallerini güncel tutun ve erişim sağlanabilir hale getirin.

Notlar:

- Eğitimlerin etkili olması için düzenli aralıklarla yapılması gerekir.

7. İzinsiz Erişim Tespit Sistemleri

7.1. IDS/IPS Sistemleri

Tanım: İzinsiz girişleri tespit eden ve engelleyen sistemlerdir.

Uygulama Adımları:

- Ağda IDS (Intrusion Detection System) ve IPS (Intrusion Prevention System) kullanarak güvenliği artırın.
- Güvenlik tehditlerini hızlı bir şekilde tespit edin ve müdahale edin.

Notlar:

- IDS/IPS sistemlerinin etkinliği düzenli olarak gözden geçirilmelidir.