Kişisel Verilerin Korunması Kapsamında Uygulamada Göz Önünde Bulundurulması Planlanan Kriterler ve Adımlar

Kişisel verilerin korunması, KVKK, GDPR ve diğer ulusal/uluslararası veri koruma düzenlemeleri çerçevesinde büyük önem taşımaktadır. Bu kapsamda, uygulamamızda aşağıdaki kriterler ve adımlar dikkate alınarak gerekli önlemler planlanmıştır:

1. **Erişim Yetkileri ve Kullanıcı Rolleri:**

   Kullanıcıların sadece yetkilendirildikleri verilere erişebilmeleri sağlanacaktır. Rol tabanlı erişim kontrolü uygulanarak, yetkisiz erişimlerin önüne geçilecektir.

   Örnek: Kullanıcı tablosundaki (users) verilere erişimi yalnızca belirli yetkilere sahip kullanıcıların yapabilmesi için, **permissions** tablosunu kullanarak rol tabanlı erişim kontrolü sağlayacağız. Örneğin, sadece "admin" rolüne sahip kullanıcılar tüm kullanıcı verilerine erişim hakkına sahip olacak, diğer roller yalnızca kendi verilerini görebilecektir. Bu sayede, yetkisiz erişimlerin önüne geçilmiş olacaktır.

2. **Veri Maskeleme ve Şifreleme:**

   Hassas kullanıcı verileri (örn. parola, telefon numarası) şifrelenmiş bir şekilde saklanacaktır. Verilerin yetkisiz erişim durumunda korunmasını sağlamak amacıyla veri maskeleme teknikleri kullanılacaktır.

   Örnek: users tablosunda yer alan hassas veriler, özellikle şifreler (**password_hash**) ve telefon numaraları (**phone_number**), güvenlik açısından şifrelenmiş olarak saklanacaktır. Bu şifreleme işlemi, verilerin yetkisiz kişilerce okunamamasını sağlayacaktır. Ayrıca, veri maskeleme teknikleri kullanarak, sadece gerekli bilgilerin görünür olmasını temin edeceğiz.

3. **Loglama ve İzleme:**

   Kullanıcıların sisteme giriş ve çıkış zamanları, kullanılan cihaz bilgileri ve IP adresleri düzenli olarak loglanacaktır. Bu loglar, şüpheli aktivitelerin tespit edilmesi ve izlenmesi amacıyla periyodik olarak analiz edilecektir.

   Örnek: Kullanıcıların uygulamaya giriş ve çıkış zamanları, IP adresleri ve kullanılan cihaz bilgileri **login_history** tablosunda kayıt altına alınacaktır. Bu loglar, şüpheli aktivitelerin tespit edilmesi ve izlenmesi amacıyla düzenli olarak analiz edilecektir. Bu süreç, kullanıcıların sistem üzerindeki hareketlerinin izlenebilirliğini sağlayacaktır.

4. **İzinlerin Kısıtlanması ve Zaman Aşımı:**

   Veri erişim izinleri, belirli bir sürenin ardından otomatik olarak sona erecek şekilde yapılandırılacaktır. Gereksiz veri erişimlerinin önüne geçmek için izinlerin geçerlilik süreleri düzenli olarak gözden geçirilecektir.

Örnek: permissions tablosunda yer alan izinler, belirli bir sürenin ardından otomatik olarak sona erecek şekilde yapılandırılacaktır. Örneğin, bir kullanıcının geçici erişim izni varsa, **expires_at** sütunu kullanılarak bu izinler zamanla kısıtlanacak ve süresi dolduğunda erişimi engellenecektir. Bu, gereksiz veri erişimlerinin önüne geçmek için kritik bir adımdır.

5. **Veri Erişim Talepleri ve Denetimi:**

   Her veri erişim işlemi, iz bırakacak şekilde kaydedilecektir. Hangi kullanıcının, hangi verilere eriştiği ve hangi zamanlarda erişim sağladığı detaylı olarak loglanacak ve denetlenebilir olacaktır.

   Örnek: Her veri erişim işlemi, iz bırakacak şekilde kaydedilecektir. **login_history** tablosunda tutulan loglar, hangi kullanıcının hangi verilere eriştiğini ve hangi zamanlarda bu erişimi sağladığını detaylı olarak kaydedecektir. Bu loglar, denetim süreçlerinde kullanılmak üzere düzenli olarak incelenecektir.

6. **Veri Anonimleştirme ve Silme:**

   Kullanıcıların veri silme talepleri doğrultusunda kişisel bilgiler anonim hale getirilecek veya tamamen silinecektir. Bu süreç, KVKK ve GDPR kapsamında kullanıcılara tanınan haklara uygun olarak yönetilecektir.

   Örnek: Kullanıcıların veri silme talepleri doğrultusunda, **users** tablosundaki kişisel bilgiler anonim hale getirilecek veya tamamen silinecektir. Örneğin, bir kullanıcı uygulamadan ayrılmak istediğinde, kimlik bilgileri anonimleştirilerek sistemde herhangi bir iz bırakılmadan silinecektir. Bu işlem, KVKK ve GDPR kapsamındaki kullanıcı haklarını gözetmek adına yapılacaktır.

7. **Olağanüstü Durumlar ve Geri Alma Prosedürleri:**

   Sistemde güvenlik ihlali tespit edilmesi durumunda, verilerin korunmasını sağlamak amacıyla yedekleme ve geri alma prosedürleri devreye sokulacaktır.

   Örnek: Sistemde bir güvenlik ihlali tespit edilmesi durumunda, verilerin korunmasını sağlamak amacıyla düzenli olarak yapılan yedeklemelerden veri geri alma prosedürleri devreye sokulacaktır. Bu sayede, kullanıcı verilerinin güvenliğini sağlamak için en hızlı şekilde aksiyon alınacaktır.

8. **OTP ve 2FA (İki Faktörlü Kimlik Doğrulama):**

   Kullanıcıların güvenliğini artırmak amacıyla iki faktörlü kimlik doğrulama (2FA) ve tek kullanımlık şifre (OTP) uygulamaları entegre edilecektir. Bu doğrulama süreçleri, yetkisiz veri erişimlerini engelleyecek kritik bir güvenlik katmanı oluşturacaktır.

   Örnek: otp_verifications tablosu, kullanıcıların giriş sırasında doğrulama için kullandıkları tek kullanımlık şifreleri (OTP) saklayacaktır. Ayrıca, **users** tablosunda **is_2fa_enabled** alanı, iki faktörlü kimlik doğrulamanın etkinleştirildiğini belirtecektir. Bu doğrulama süreçleri, kullanıcıların hesaplarının güvenliğini artıracak ve yetkisiz veri erişimlerini engelleyecektir.

Bu kriterler ve adımlar, uygulamamızın güvenliğini artırmak ve kişisel verilerin korunmasını sağlamak amacıyla ekibimizle birlikte geliştirilecektir. Geliştirme sürecinde her adımda bu ilkeleri göz önünde bulundurarak, güvenli ve kullanıcı dostu bir uygulama oluşturmayı hedefliyoruz.