PASHA Bank

KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

Kişisel Veri Koruma Sisteminin Amaçları

Kişisel Veri Koruma Sisteminin amacı, Banka'nın kişisel verilerin yönetiminde kendi standartlarını oluşturmasının ve gerçekleştirmesinin sağlanması; organizasyonel hedef ve yükümlülüklerin belirlenmesi ve desteklenmesi, Banka'nın kabul edilebilir risk seviyesiyle uyumlu olarak kontrol mekanizmalarının tesis edilmesi; Banka'nın kişisel verilerin korunması alanındaki uluslararası sözleşmeler, Anayasa, kanunlar, sözleşmeler ve meslek kuralları uyarınca tabi olduğu yükümlülüklerin yerine getirilmesi ve bireylerin menfaatlerinin en iyi şekilde korunmasıdır.

Banka, kişisel verilerin korunması mevzuatı ve veri koruma ilkelerine uyar. Bankanın benimsediği veri koruma ilkeleri aşağıdaki gibidir:

a. Kişisel verileri yalnızca meşru kurumsal amaçlar bakımından açıkça gerekli olması halinde işlemek,
b. Bu amaçlar için gerekli asgari ölçekte kişisel veriyi işlemek ve gereğinden fazla veriyi işlememek,
c. Bireylere kişisel verilerinin kimler tarafından hangi amaçla ve ne şekilde kullanıldığı konusunda açık bilgi vermek,
d. Gerekli hallerde müşterilerinden özgür iradeyle açık rızalarını almak,
e. Yalnızca ilgili ve uygun kişisel verileri işlemek,
f. Kişisel verileri hakkaniyete ve hukuka uygun olarak işlemek,
g. Mevzuatta belirtildiği şekilde, kişisel veri envanteri tutmak,
h. Kişisel veri envanterinin doğruluğundan ve güncelliğinden emin olacak mekanizmalar kurmak,
i. Kişisel verileri Saklama ve İmha Politikasında belirtilen metodoloji ile belirlenmiş sürelere uyumlu olarak saklamak,
j. Kişisel verilerin saklanması ve imhası politikasını oluşturmak, süreçleri bu politika doğrultusunda yapılandırmak ve politikanın uygulamaya yansımasını sağlamak,
k. Bireylerin, erişim hakkı dahil olmak üzere, kişisel verileriyle ilgili haklarına saygılı olmak,
l. Tüm kişisel verileri güvenli tutmak,
m. Kişisel verileri yurtdışına (müşteri bilgileri / çalışan bilgileri vb.), yalnızca yeterli korumanın bulunması halinde, 4.8. maddesine uygun olarak transfer etmek,
n. Yalnızca KVK Kurumu tarafından belirlenen güvenli ülkeler veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri, Kurul'un izninin bulunması ve BDDK mevzuatına aykırılık olmaması halinde yurtdışına veri aktarmak,
o. Mevzuat uyarınca izin verilen istisnaları uygulamak,
p. Politikanın uygulanması için kişisel veri koruma sistemini tesis etmek ve uygulamak,
q. Gerektiğinde kişisel veri koruma sistemine taraf olan iç ve dış paydaşları ve bunların Banka'nın kişisel veri koruma sistemine ne ölçüde dahil olduklarını belirlemek,

r. Kişisel verilerin korunması sistemiyle ilgili özel yetki ve sorumluluklara sahip personelleri belirlemek.

Bildirim Yapma ve Erişim

Banka, veri sorumlusu olduğu ve bu sıfatla hangi kişisel veri kategorilerini işlediği konularında talep edilmesi durumunda, Kişisel Verilerin Korunması Kurulu'nu ("KVK Kurulu") bilgilendirir. Banka, kişisel veri envanterinde işlediği tüm kişisel veri kategorilerini belirler.

Bildirim KVK Kurulu'nca belirlenecek usul ve yöntem uyarınca yapılır ve yapılan bildirimin bir kopyası Banka'nın Kişisel Veri Koruma Komitesi (KVK Komitesi) tarafından saklanır.

İlgili mevzuat veya KVK Kurulu'nca gerekli görülmesi halinde bildirimler periyodik olarak tekrarlanır.

Bilgi Güvenliği Yönetimi Komitesi (BGY Komitesi), KVK Kuruluna yapılan bildirimde meydana gelebilecek potansiyel değişiklikleri tespit etmek amacıyla Banka'nın veri işleme faaliyetlerini ve bunlardaki değişiklikleri yıllık olarak gözden geçirir ve gerekmesi halinde KVK Kurulu'nu bilgilendirir.

Bu politika Banka'nın tüm birimlerini, çalışanlarını, destek hizmeti veren firma çalışanlarını, stajyer ve sözleşmeli personeli kapsamaktadır. KVKK veya bu politikayı ihlal edici her türlü eyleme Banka'nın disiplin mevzuatı uygulanacak ve söz konusu ihlalin suç veya kabahat oluşturması halinde durum en kısa süre içerinde ilgili makamlara bildirilir.

Banka'nın kişisel verilere erişimi veya erişme ihtimali bulunan çözüm ortakları ve Banka ile birlikte çalışan tüm üçüncü taraflar bu politikayı okumaya ve politikaya uymaya davet edilir. Hiçbir üçüncü taraf, kişisel verilerin korunması konusunda en az Banka'nınki kadar güçlü standartlara sahip yükümlülükleri ve bunlara ilişkin Banka'nın denetim hakkını içeren yazılı bir gizlilik anlaşması yapılmaksızın Banka tarafından işlenen kişisel verilere erişim sağlayamaz.

Risk Değerlendirme

Risk değerlendirmenin amacı, Banka'nın belirli kişisel veri türlerinin işlenmesiyle bağlantılı risklerin farkında olmasıdır.

Banka, kişisel bilgilerinin işlenmesinin bireyler üzerinde doğurabileceği riskleri değerlendirmek üzere yöntemler belirler. Bu değerlendirme, Banka adına verileri işleyen üçüncü kişiler de dikkate alınarak gerçekleştirilir. Banka, değerlendirme sonucu tespit edilen, riskleri bu politikayla uyumsuzluk oluşturmayacak şekilde yönetir.

Belirli bir türdeki veri işleme faaliyetinin, yapısı, bağlamı ve amaçları doğrultusunda kişisel hak ve özgürlükler üzerinde yüksek risk doğurması muhtemel ise, Banka veri işleme faaliyeti öncesinde faaliyet ile ilgili birim, Risk Yönetimi'nin uygunluğunu alarak bir etki analizi gerçekleştirir ve potansiyel riskleri yönetir. Benzer riskler içeren birden fazla veri işleme faaliyeti için tek bir değerlendirmeye dayanılabilir.

Etki analizi sonunda Banka'nın kişisel hak ve özgürlükler üzerinde yüksek risk doğurabilecek bir veri işleme faaliyetine başlamak üzere olduğu anlaşılırsa, bu konuyla ilgili BGY Komitesi onayı aranır. BGY Komitesi gerekli görmesi halinde KVK Kurulundan konuyla ilgili görüş alır.

Risk yönetiminde Banka'nın hali hazırda Bilgi Güvenliği Politikası uyarınca benimsemiş olduğu, Operasyonel Risk Prosedürü uyarınca uygulanan sistem ve kontroller uygulanır.

Veri Koruma İlkeleri

Tüm kişisel veri işleme faaliyetlerinin aşağıdaki veri koruma ilkeleriyle uyumlu olarak gerçekleştirilmesi esastır. Banka'nın politika ve prosedürleri bu ilkelerle uyumluluğu sağlamayı amaçlar:

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlar için işlenme.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme. Kişisel veriler hukuka ve dürüstlük kuralına uygun ve şeffaf bir şekilde işlenir. Bu doğrultuda Banka, gerçekleştirdiği kişisel veri işleme faaliyetlerine ilişkin, veri toplama kanallarında ve ilgili formlarda gizlilik bildirimlerine yer verir. Banka tarafından kimlere ilişkin hangi verilerin hangi amaçlarla işlendiğine ilişkin açık ve anlaşılabilir bilgilerin yer aldığı bu bildirimlerin yer alacağı ve ilan edileceği alanlar BGY Komitesi tarafından belirlenir. Bu bildirimlerde şu hususlara yer verilir:

- Banka'nın veri sorumlusu olarak kimliği ve iletişim bilgileri,
- BGY Komitesi ve iletişim bilgileri,
- İşlenen kişisel veri türleri (Kişisel veri veya Özel Nitelikli Kişisel Veri),
- Kişisel veri olarak değerlendirilen veri türleri basılı ve elektronik olarak ayrıştırılmaktadır,
- Kişisel verinin işlenme amaçları,
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Kişisel verinin öngörülen saklama süresi,
- Veri sahibinin hakları,
- Verinin paylaşılabileceği üçüncü taraflar.

Kişisel veriler yalnızca belirli, açık ve meşru amaçlarla işlenebilir.

Kişisel veri envanterinde kişisel verilerin işlenme gerekçeleri/amaçları belirlenir ve kişisel veriler başka bir hukuki gerekçe veya veri sahibinin açık rızası olmaksızın belirtilen amaç dışında kullanılamaz.

Bir kişisel verinin kişisel veri envanterinde belirtilmiş amaçlar dışında kullanılmasını gerektiren koşulların doğması halinde, bu durum ilgili personel/birim tarafından BGY Komitesi'ne bildirilir. BGY Komitesi yeni amacın uygunluğunu denetler ve gerekliyse veri sahibinin yeni amaçla ve yeni veri işleme faaliyeti konusunda bilgilendirilmesini sağlar.

Kişisel verileri işleme faaliyeti, amacına uygun, ilgili ve sınırlı olarak gerçekleştirilmelidir.

BGY Komitesi işleme amacı için açıkça gerekli olmayan kişisel verilerin toplanmadığını ve işlenmediğini sağlamakla yükümlüdür.

Envanterde belirtilenin haricinde yeni bir kişisel veri işleme sürecinde BGY Komitesi onayı alınır.

BGY Komitesi minimum altı ayda bir gözden geçirilen kişisel veri envanteri üzerinden, işlenen verilerin uygun ve ilgili olduğunu denetler.

BGY Komitesi yıllık bazda yapacağı/yaptıracağı iç denetim/ dış denetim ile tüm veri işleme yöntemlerinin uygun ve ilgili olduğunu denetler.

BGY Komitesi, uygun ya da ilgili olmadığı ya da işleme amacı bakımından gereğinden fazla olduğunu tespit ettiği kişisel veriler bakımından, ilgili olabilecek mevzuat hükümlerini de esas alarak veri işleme faaliyetinin durdurulmasından ve işlenmiş verilerin Saklama ve imha politikasına uygun olarak işlenmesini sağlamaktan sorumludur.
Kişisel veriler doğru ve güncel olmalıdır.

İnsan Kaynakları ve İdari İşler Birimi, tüm personel verilerinin doğru ve güncel olarak toplanması ve tutulması konusunda farkındalığın oluşturulması ve KVKK ile ilgili eğitimin koordine edilmesinden sorumludur.

Personele ilişkin tutulan verilerin doğruluğu ve güncelliği ilgili personelin kendi sorumluluğundadır.

Çalışanlar/ müşteriler ve diğer ilgili kişiler işlenen kişisel verilerin güncellenmesi için Banka'yı bilgilendirmelidirler. Bu şekilde bir bildirim yapılması üzerine söz konusu kaydın düzeltilmesi / güncellenmesi ile veri kategorilerindeki değişikliklerin veri envanteri üzerinde güncellenmesi ilgili birimin sorumluluğundadır.

BGY Komitesi veri envanteri üzerinden, ilgili olabilecek mevzuat hükümlerini de esas alarak yapacağı işlenen verinin türü, saklama süresi ve miktarı üzerinde değerlendirme ile belirli verilerin doğruluğunun veya güncelliğinin gözden geçirilmesi için ilgili birime talimat verebilir.

1. Kişisel veriler, ilgili kişi yalnızca veri işleme amacı bakımından gerekliyse teşhis edilebilecek şekilde işlenmelidir.

1.1 Kişisel verilerin yedekleme vb. gereklilikler nedeniyle gerekli sürenin ötesinde saklanması durumunda veri güvenliği zafiyeti durumlarında bireylerin hal ve özgürlüklerinin korunması için kişisel verilerin Saklama ve İmha Politikası gereğince işleme tabi tutulması esastır. Gerekli görülen hallerde BGY Komitesinin onayı alınır.

1.2 Kişisel verilerin belirlenmiş sürelerin sonrasında işlenmesi BGY Komitesinin yazılı onayına bağlıdır.

Veri Sahiplerinin Hakları

Veri sahipleri haklarındaki Banka nezdindeki veri işleme faaliyetleri ve kayıtlara ilişkin olarak aşağıdaki haklara sahiptir:

- Kişisel verisinin bulunup bulunmadığı, bulunuyorsa hangi verilerinin bulunduğunu öğrenme,
- Kişisel verisinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Açık rıza verme/vermeme, vermiş olduğu açık rızayı geri çekme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilmeyi talep etme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- KVKK veya bu politika uyarınca işlenmesi için hukuka uygun bir gerekçe veya dayanak bulunmayan kişisel verilerin silinmesini veya yok edilmesini isteme,
- İsteği üzerine yapılan düzeltme veya silme işlemlerinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Veri sahipleri, kişisel verilerine erişme ve yukarıda sayılan haklarını kullanma talebinde bulunabilirler. Bu talepler 'İrtibat Sorumlusu'na iletilir. İrtibat Sorumlusu tarafından bilgilendirilen BGY Komitesi, en geç 30 gün içerisinde gerekli işlemlerin yerine getirilmesini sağlar. Veri sahipleri ile her türlü iletişim İrtibat Sorumlusu üzerinden sağlanır.

Taleplerin alınması, iletilmesi ve sonuçlandırılmasına ilişkin süreçler veri sahibi erişimi için tanımlanmış kurallar kapsamında gerçekleştirilir.

Veri sahiplerinin taleplerini yöneltebilmesi için gizlilik bildirimlerinde ve Banka'nın web adresinde veri sahiplerinin BGY Komitesi'ne erişim hakkına ve Komitenin iletişim bilgilerine yer verilir.

Banka'nın tüm personeli, görev tanımı ne olursa olsun kendisine yönelmiş veri sahibi erişim taleplerini Hukuk Birimine yönlendirmekle, Hukuk Birimi'de bu talepleri en kısa süre içeresinde BGY Komitesi'ne iletmekle yükümlüdür. Banka personeli, veri sahiplerinden gelecek talepler konusunda nasıl hareket etmeleri konusunda BGY Komitesince bilgilendirilmeli ve eğitilmelidir.

Açık Rıza Alınması

Banka, veri sahibi tarafından belirli veri işleme faaliyetlerine ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle, hakkında veri işlenmesine ilişkin iradeyi ortaya koyan, yazılı/sözlü beyan veya açık doğrulayıcı eylemle açıklanan, rızayı açık rıza olarak kabul etmektedir. Hassas veriler bakımından açık rıza mutlaka yazılı olarak alınır. Açık rıza veri sahibi tarafından her zaman geri alınabilir.

Açık rıza, açık rıza formu şablonu veri sahibine imzalatılarak veya veri sahibiyle yapılacak sözleşme veya elektronik formda bu şablonda yer alan unsurlara yer verilmesi suretiyle alınabilir. Çalışanlar, çalışan adayları ve müşterilere ilişkin rutin olarak işlenen kişisel veriler bakımından açık rıza, ilgili standart sözleşme veya formlar aracılığıyla alınır.

Açık rızaya dayanan veri işleme faaliyetinin süreklilik arz edecek veya tekrarlanacak olması halinde ilgili birimce tek bir liste halinde açık rızası alınmış kişilerin kayıtları tutulur. Bu

kayıtların güncelliği ve doğruluğu ilgili birimin sorumluluğundadır. Açık rızaya dayanan veri işleme faaliyetine ilişkin açık rıza formları veya diğer ilgili ispat araçları ilgili birimce saklanır.

Veri Güvenliği

Personel, Banka tarafından işlenen ve kendi sorumluluklarında olan verilerin güvenli olarak tutulmasını ve gizlilik sözleşmesi imzalamadıkça, hiçbir üçüncü tarafa açıklanmamasını sağlamakla yükümlüdür.

Kişisel verilere, yalnızca bunlara erişimi gerekli olanlar erişir. Erişimler, belirlenmiş kurallara uygun olarak sağlanır.

Veri güvenliği, Banka'nın Bilgi Güvenliği Politikası ve buna bağlı dokümanlar uyarınca sağlanır.

Veri güvenliği kapsamında veri sorumlusu;

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

Kanuni yükümlülük olarak, kişisel verilere ilişkin bilgi güvenliği olayları BGY Komitesi tarafından en kısa süre içerisinde KVK Kuruluna ve ilgili kişiye bildirilir.

Veri Paylaşımı

1. Kişisel veriler ancak hukuka ve hakkaniyete uygun olarak üçüncü kişilerle paylaşılabilir. Buna göre kişisel verilerin paylaşılabilmesi için aşağıdaki koşullardan birinin bulunması aranır:
    - Veri sahibin açık rızasının alınmış olması.
    - Kanunlarda açıkça öngörülmesi.
    - Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
    - Banka'nın taraf olduğu ya da olacağı bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

- Banka’nın hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Banka’nın haklarının tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Banka’nın meşru menfaatleri için veri işlenmesinin zorunlu olması.

2. Kişisel veriler, ancak yukarıdaki koşulların sağlanması, hedef ülkede yeterli korumanın bulunması ve veri sahibinin bu aktarım konusunda açık rızasının alınması koşuluyla yurtdışına aktarılabilir.

   Kişisel verilerin yurtdışına aktarılmasında KVK Kurulu tarafından belirlenen yeterli korumanın bulunduğu ülkeler listesi dikkate alınır.
   Kişisel verilerin yurtdışına aktarılması söz konusu olduğunda KVKK ve ilgili mevzuat uyarınca, BGY Komitesi KVK Kurulu nezdinde gerekli izin ve bildirimleri sağlar.

3. Kişisel verilerin paylaşımına ilişkin tüm işlemler gerekçeleriyle birlikte yazılı olarak kayıt altına alınmalıdır. Bu kayıtlar BGY Komitesince belirli periyotlarla denetlenir.

4. Yasal bir dayanak veya hukuki yükümlülük olmaksızın düzenli bir veri paylaşma ilişkisinin söz konusu olması halinde, söz konusu tarafla veri paylaşımının koşullarını belirleyen bir veri paylaşma sözleşmesi yapılır. Veri paylaşma sözleşmesi minimumda şunları içerir:
   - Paylaşımın amacı veya amaçları;
   - Potansiyel üçüncü kişi alıcılar veya alıcı türü ve erişim hakkı koşulları;
   - Paylaşılacak verilerin neler olduğu (bu amaçlarınız için gerekli minimum düzeyde tutulmalıdır);
   - Verinin işlenmesine ilişkin genel ilkeler;
   - Veri güvenliği tedbirleri bilgi varlığı gizlilik sınıfına göre değerlendirilir. Bilgi varlığı gizlilik sınıfları Gizli, Sınırlı Erişim, Kuruma Özel ve Umumi olarak belirlenmesi;
   - Paylaşılan verilerin tutulma süresi;
   - Veri sahibinin hakları, erişim talepleri, başvuru ve şikayetlere cevap verme prosedürleri;
   - Paylaşım sözleşmesinin yürürlüğünün sona erdirilmesinin gözden geçirilmesi ve Sözleşmeye uyulmaması veya personelin bireysel ihlalinden dolayı sorumluluk ve yaptırımlar
   - Veri paylaşma sözleşmeleri Hukuk Biriminin onayından sonra BGY Komitesi’nin onayına sunulur.

Kayıtların Yönetimi

Kişisel veriler, işlenme amaçları için gerekli süreden fazla tutulamaz. Kişisel veri içeren kayıtların sınıflandırılması ve bunlara ilişkin saklama süreleri, ilgili mevzuata uygun olarak hazırlanmış Varlık Belirleme ve Sınıflandırma Prosedürü uyarınca belirlenir.

İşlenme amaçları için gerekli süresi dolan veya veri sahibinin haklı talebi üzerine mevzuat kapsamında imha edilebilecek kişisel veriler, Saklama ve İmha Politikası uyarınca anonimleştirilir silinir veya yok edilir.

Denetim

KVK denetimleri, şirket içinde İç Denetim Birimi tarafından veya 3. taraf bir firma tarafından yapılır. İç ve dış denetim sonuçları BGY Komitesi tarafından periyodik olarak yapılan değerlendirme toplantılarında gözden geçirir.