KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

Hedef Kitle: Bariyer Güvenlik tarafından kişisel verileri işlenen tüm gerçek kişiler

Hazırlayan: Bariyer Güvenlik Kişisel Verilerin Korunması Komitesi

Versiyon: 1.0

Onaylayan: Bariyer Güvenlik yetkilisi tarafından onaylanmıştır.

Bariyer Özel Güvenlik Hizmetleri A.Ş.
KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

1. GİRİŞ

Bariyer Özel Güvenlik Hizmetleri A.Ş. **("Bariyer Güvenlik")** olarak özel güvenlik hizmetleri faaliyetlerinde kişisel verilerin korunmasına önem vermekte ve iş ve işlemlerinde öncelikleri arasında kabul etmektedir. Bariyer Güvenlik Kişisel Verilerin Korunması ve İşlenmesi Politikası **("Politika"),** 6698 sayılı Kişisel Verilerin Korunması Kanunu'nca **("Kanun")** belirlenen kişisel veri işleme usul ve esaslarının Bariyer Güvenlik organizasyon ve iş süreçlerinin uyumuna yönelik temel düzenlemedir. Bariyer Güvenlik bu Politika prensipleri doğrultusunda, üst düzey sorumluluk ve bilinciyle kişisel verileri işlemekte ve korumakta, kişisel veri sahiplerini bilgilendirerek gerekli şeffaflığı sağlamaktadır.

1.1. Amaç

Bu Politikanın amacı, Kanun ve ilgili diğer mevzuat ile öngörülen usul ve esasları, Bariyer Güvenlik organizasyon ve süreçlerine uyumlulaştırılarak, faaliyetlerinde etkin bir şekilde uygulanmasını sağlamaktır. BARİYER GÜVENLİK kişisel verilerin işlenmesi ve korunması için bu Politika ile her türlü idari ve teknik önlemleri almakta, gerekli iç prosedürler oluşturmakta, farkındalığı arttırmakta, bilincin sağlanması için gerekli tüm eğitimleri yapmaktadır. Hissedarlar, yetkililer, çalışanlar ve iş ortaklarının Kanun süreçlerine uyumları için, gerekli tüm önlemler alınmakta, uygun ve etkin denetim mekanizmaları kurulmaktadır.

1.2. Kapsam

Politika, BARİYER GÜVENLİK iş süreçlerinde otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilen bütün kişisel verileri kapsamaktadır.

1.3 . Dayanak

Politika, Kanun ve ilgili mevzuata dayanmaktadır. Kişisel veriler, 5188 sayılı Kanun, 6502 sayılı Tüketicinin Korunması Hakkında Kanun, 1774 sayılı Kimlik Bildirme Kanununu, 4857 sayılı İş Kanunu, 6331 İş Sağlığı ve Güvenliği Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 4447 sayılı İşsizlik Sigortası Kanunu, 6102 sayılı Türk Ticaret Kanunu, 213 sayılı Vergi Usul Kanunu ve diğer ilgili mevzuattan kaynaklanan kaynaklanan yasal yükümlülükleri yerine getirmek için işlenmektedir.

Yürürlükteki mevzuat ve Politika arasında uyumsuzluk olduğu hallerde yürürlükteki mevzuat uygulanır. İlgili mevzuat tarafından öngörülen düzenlemeler, Politika ile BARİYER GÜVENLİK uygulamalarına dönüştürülmektedir.

1.4 . Tanımlar

Açık rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Başvuru Formu	Kişisel veri sahiplerinin haklarını kullanmak için yapacakları başvuruyu içeren, 6698 sayılı Kişisel Verilerin Korunması Kanununa ve Kişisel Verileri Koruma Kurumunun çıkardığı Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun olarak hazırlanmış, ilgili kişi (Kişisel Veri Sahibi) tarafından veri sorumlusuna yapılacak başvurulara ilişkin başvuru formu.
İlgili kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.

Kayıt ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel verilerin işlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kişisel verilerin anonim hale getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel veri sahibi	Kişisel verileri BARİYER GÜVENLİK tarafından veya adına işleme sokulan gerçek kişi.
Kişisel verilerin silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel verilerin yok edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
Özel nitelikli kişisel veri	Kişilerin sağlığı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik verileri.
Periyodik imha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri sahibi / İlgili kişi	Kişisel verisi işlenen gerçek kişi.
Veri sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Veri Temsilcisi	Kanun uyarınca Veri Sorumlusunun ilgili kanun maddeleri kapsamındaki görevlerini yerine getirmek üzere atanmış gerçek kişi.

Yönetmelik	28 Ekim 2017 tarihinde Resmi Gazete' de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

2. KİŞİSEL VERİLERİN KORUNMASI KONULARI

2.1. Kişisel Verilerin Güvenliğinin Sağlanması

BARİYER GÜVENLİK , kişisel verilerin hukuka aykırı açıklanmasını, erişimini, aktarılmasını veya başka şekillerde oluşabilecek güvenlik sorunlarını önlemek için, kişisel verinin niteliğine göre, Kanun'un 12. maddesinde öngörülen gerekli önlemleri almaktadır. BARİYER GÜVENLİK , Kişisel Verileri Koruma Kurumu tarafından yayımlanmış olan rehberlere uygun olarak gerekli kişisel veri güvenlik seviyesini sağlamak için tedbirler almakta, denetimler gerçekleştirmektedir.

2.2. Özel Nitelikli Kişisel Verilerin Korunması

Özel nitelikte olan, kişilere ait sağlık, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili verilerin korunmasına yönelik alınan önlemler özenle uygulanmakta ve gerekli denetimler yapılmaktadır.

2.3. Kişisel Verilerin Korunması ve İşlenmesi Bilincinin Geliştirilmesi

BARİYER GÜVENLİK , kişisel verilerin hukuka uygun işlenmesini, erişilmesini, verilerin muhafazası ve hakları kullanmaya yönelik bilincin geliştirilmesi için ilgililere gerekli eğitimleri verir.

Çalışanların kişisel verileri koruma bilincini arttırmak için, BARİYER GÜVENLİK gerekli iş süreçlerini oluşturur, ihtiyaç duyulması halinde uzman danışmanlardan destek alır. Uygulamada karşılaşılan eksiklikler ve eğitimlerin sonucu BARİYER GÜVENLİK yönetimi tarafından değerlendirilir. Yapılan bu değerlendirmeler ile ilgili mevzuattaki değişikliklere bağlı ihtiyaç duyulması halinde yeni eğitimler düzenlenir.

3. KİŞİSEL VERİLERİN İŞLENMESİ

Kişisel veriler aşağıda sayılan ilkeler doğrultusunda mevzuata uygun işlenir.

i. ***Hukuka ve Dürüstlük Kuralına Uygun İşleme***
Kişisel veriler, iş süreçlerinin gerektirdiği ölçüde, bunlarla sınırlı, kişilerin temel hak ve özgürlüklerine zarar vermeden, hukuka ve dürüstlük kuralına uygun olarak işlenir.

ii. ***Kişisel Verilerin Güncel ve Doğru ve Olmasını Sağlama***
İşlenen kişisel veriler, güncel ve doğru tutmak için gerekli önlemler alınmakta ve plan ve programlı çalışılmaktadır.

iii. ***Belirli, Açık ve Meşru Amaçlarla İşleme***
Kişisel veriler, yürütülen iş süreçlerinde belirlenen ve açıklanan meşru amaçlara bağlı işlenmektedir .

iv. ***İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma***
Kişisel veriler, iş süreçlerinin gerektirdiği nitelik ve ölçüde toplamakta, belirlenen amaçlara bağlı, sınırlı işlenmektedir.

v. ***Gerekli Olan Süre Kadar Muhafaza Etme***
Kişisel veriler, ilgili mevzuatta öngörülen ve kişisel verileri işleme amacı için gerekli olan en az süre kadar muhafaza edilmektedir. Öncelikle, ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülmüş ise bu süreye, öngörülmemiş ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar muhafaza edilmektedir. Kişisel veriler saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak, uygun yöntemlerle (silme, yok etme veya anonimleştirme) imha edilmektedir.

Çalışan, çalışan adayı/stajyer/öğrencilerin: Kimlik Verileri (Ad-soyad, T.C. kimlik numarası, kimlik kartı bilgileri, doğum yeri/tarihi, anne-baba adı, nüfus kayıt bilgileri), İletişim Verileri (Adres, telefon, e-posta, acil durum kişisi bilgileri), Özlük Verileri (İşe giriş-çıkış belgeleri, bordro ve ücret bilgileri, disiplin süreçleri, performans değerlendirmeleri, izin kayıtları, sertifika bilgileri (5188 sertifikası dahil), eğitim kayıtları), Hukuki İşlem Verileri (Tebligat kayıtları, adli yazışmalar, iş kazası bildirimi, ihtar/cevap/müzekkere yazıları), Fiziksel Mekân Güvenliği Verileri (Kamera görüntüleri,

bina giriş-çıkış kayıtları, turnike verileri, ziyaretçi logları), İşlem Güvenliği Verileri (IP adresi, sistem erişim bilgileri, kullanıcı logları, şirket cihazlarının kullanım kayıtları), Finans ve Banka Bilgileri (IBAN, banka hesap bilgileri, ödeme kayıtları), Sağlık Verileri (Özel Nitelikli) (Periyodik sağlık raporları, iş göremezlik raporları, işe giriş sağlık muayenesi, engellilik durumu bilgileri), Ceza Mahkûmiyeti ve Güvenlik Tedbirleri Verileri (Özel Nitelikli) (Adli sicil kaydı, arşiv araştırması, güvenlik soruşturması sonuçları), Mesleki Deneyim Verileri (Diploma, sertifika, kurs bilgileri, hizmet içi eğitimler), Araç Bilgileri (görev aracı kullanan personel) (Plaka bilgisi, araç kullanım kayıtları), Görsel/İşitsel Kayıtlar (Fotoğraf, kamera görüntüleri, işe giriş dosyası fotoğrafları), Çalışma Verileri (Vardiya planları, görev yeri kayıtları, devriye raporları, risk alanı notları), Lokasyon Verileri (görev gereği) (GPS cihazı, devriye takip sistemi, mobil uygulama konum verileri) ve ek politikalarla belirlenecek kişisel veriler;

İş Sözleşmesinin Kurulması ve İfası (KVKK md. 5/2-c), Özlük dosyası oluşturulması, Ücret bordrolarının hazırlanması, SGK bildirimi, Vardiya düzenlemesi, Sertifika/doğrulama kontrolleri, Görev yerlerinin planlanması, Şirketin Hukuki Yükümlülüklerinin Yerine Getirilmesi (KVKK md. 5/2-ç), 5188 sayılı Kanun gereği güvenlik görevlisi sicil kontrolleri, Sağlık raporlarının alınması, SGK/İŞKUR bildirimleri, Vergi yükümlülükleri, İş sağlığı ve güvenliği zorunlulukları, Kanunda Açıkça Öngörülmesi (KVKK md. 5/2-a ve md. 6/3), Adli sicil kontrolü, Arşiv araştırması, Özel güvenlik kimlik yenileme işlemleri, İş kazası bildirimleri, Meşru Menfaat (KVKK md. 5/2-f), Kamera ile güvenlik denetimi, Bilgi işlem güvenliğinin sağlanması, İç denetim ve uyum süreçleri, Vardiya performans takibi, Görev sahası güvenliği, Bir Hakkın Tesisi, Kullanılması veya Korunması (KVKK md. 5/2-e), Hukuki süreçlerde delil sunulması, Sözleşmesel uyuşmazlıkların çözümü, İş kazası savunmalarının hazırlanması başta olmak üzere Politika'da belirlenen amaçlara bağlı, Kanun'un 5. ve 6. maddelerine uygun olarak işlenmektedir.

Veriler şu yöntemlerle toplanır: Fiziki formlar (işe giriş, özlük dosyası belgeleri); Kimlik fotokopileri, Kamera kayıtları, E-posta/telefon görüşmeleri, Devriye takip sistemi, Turnike – kart sistemi, Mobil uygulamalar, SGK ve e-Devlet entegrasyonları, Müşteri sahalarında kullanılan güvenlik sistemleri, müşteri – üst işveren tarafından aktarılan bilgi ve belgeler.

Çalışan, çalışan adayı/stajyer/öğrencilerin fotoğraf ve görüntüleri, Bariyer Güvenlik'in tanıtım, reklam, marka görünürlüğü ve kurumsal iletişim faaliyetleri kapsamında kullanılabilmektedir. Bu kapsamda işlenen kişisel verilerin niteliği, işlenme amaçları, hukuki sebepleri, aktarım süreçleri ve çalışan hakları aşağıda belirtilmiştir. Bu kapsamda aşağıdaki kişisel veriler işlenebilir: Fotoğraf, Video görüntüsü, Ad-soyad bilgisi, Ünvan, görev bilgisi, Görsel kayıt tarih ve konum bilgisi (çekim etkinliği sırasında oluşturulan meta veriler). Çalışana ait fotoğraf ve görüntüler aşağıdaki amaçlarla işlenebilir: Şirketin reklam ve tanıtım faaliyetleri, Kurumsal web sitesi, sosyal medya hesapları (Instagram, LinkedIn, X, Facebook vb.) üzerinden paylaşım ve tekrar paylaşım, Basın bülteni, kurumsal katalog, broşür, afiş, tanıtım filmi, kurumsal sunum ve dokümanlarda kullanım, İşveren markasının güçlendirilmesi ve yeni müşteri edinme süreçleri, Şirket içi – dışı organizasyonların duyurulması.Reklam ve pazarlama amaçlı görsel paylaşımı, hukuken açık rıza gerektiren bir veri işleme faaliyetidir. Bu nedenle kişisel veriler yalnızca çalışanın KVKK m.5/1 kapsamında verdiği "ayrı, özgür iradeye dayalı, belirli konuya ilişkin açık rızası" ile işlenecek ve paylaşılacaktır. Açık rızanın verilmemesi veya geri alınması, iş sözleşmesine, çalışma şartlarına veya çalışan haklarına hiçbir olumsuz sonuç doğurmaz. Açık rızanın verilmesi halinde fotoğraf ve görüntü verileri: Şirketin kurumsal sosyal medya hesapları (Instagram, LinkedIn, Facebook, X), Şirketin web sitesi, Basın-yayın kuruluşları, Reklam, medya ve tasarım ajansları, Kurumsal etkinlik organizatörleri, Şirket iş ortakları ve tedarikçiler ile tanıtım faaliyeti ile sınırlı olmak üzere paylaşılabilir. Fotoğraflar, video kayıtları ve işitsel veriler, tanıtım materyallerinin yayında bulunduğu süre boyunca veya çalışanın açık rızasını geri aldığı ana kadar saklanır. Açık rızanın geri alınmasından sonra veriler ileriye dönük olarak işlenmez, tüm dijital ortamlardan silinir ve yeni paylaşımlar durdurulur. Basılı materyallerin geri çağrılması teknik olarak mümkün olmadığı ölçüde yalnızca yeni baskılarda kullanım durdurulur.

Müşteri ve/ya iş ilişkisi sıfatıyla Şirketimizle sözleşme imzalayan, imzalayacak olan ve/ya ticari herhangi ilişkisi gerçek kişi müşteriler ile müşteri tüzel kişilerin yetkilisi, ortağı, çalışanı ve temsilcisi konumundaki gerçek kişilere ilişkin olarak; kimlik bilgileri (ad-soyad, T.C. kimlik numarası, imza örneği, unvan, görev/pozisyon), iletişim bilgileri (adres, iş/e-posta adresi, telefon numarası), müşteri şirket bilgileriyle bağlantılı ticari bilgiler (çalıştığı şirket, birim, organizasyon şeması içindeki konum, yetki ve temsil bilgileri), sözleşme sürecine ilişkin bilgiler (sözleşme metinleri, teklif, sipariş ve hizmet talep kayıtları, yazışmalar, tutanaklar, talimatlar), finans ve muhasebe verileri (fatura bilgileri, banka hesap bilgileri, tahsilat ve ödeme kayıtları) ile iş ilişkisi kapsamında ortaya çıkan hukuki işlem ve uyuşmazlık verileri Şirketimiz tarafından; özel güvenlik hizmeti ve sair hizmet sözleşmelerinin kurulması ve ifası, sözleşme öncesi tekliflendirme ve müşteri ilişkilerinin yönetimi, hizmetin planlanması ve sahada ifası, ziyaret ve iletişim süreçlerinin yürütülmesi, mali ve finansal kayıtların oluşturulması, saklanması ve denetlenmesi, hukuki ve ticari güvenliğin sağlanması, risk yönetimi, denetim ve raporlama faaliyetlerinin yürütülmesi, olası uyuşmazlık, dava ve idari süreçlerde delil elde edilmesi ve hakların tesisi, kullanılması veya korunması amaçlarıyla; 6698 sayılı Kanun'un 5/2-c bendinde düzenlenen "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması", 5/2-ç bendinde düzenlenen "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" ve 5/2-f bendinde düzenlenen "veri sorumlusunun meşru menfaati için veri işlemenin zorunlu olması" hukuki sebeplerine dayanılarak ve gerektiği ölçüde işlenmektedir.

Kişisel Verilerin İşlenme Genel Şartları

Kişisel veri, sahibinin açık rıza vermesi veya aşağıda belirtilen diğer bir veya birden fazla şarta dayanarak işlenir.

i. **Kişisel Veri Sahibinin Açık Rızasının Bulunması**
Kişisel verilerin işlenmesi veri sahibinin açık rızasıyla yapılır. Kişisel veri sahibinin açık rızası: belirli bir konuda bilgilendirilerek ve özgür iradesi alınarak gerçekleşir.

ii. **Kişisel Veri Sahibinin Açık Rızasının Bulunmaması**
Aşağıda sıralanan şartlarından herhangi birinin bulunması durumunda veri sahibinin açık rızasına gerek kalmaksızın kişisel veriler işlenebilir.

a. **Kanunlarda Açıkça Düzenlenmesi**
Kanunlarda kişisel verilerin işlenmesine ilişkin açık bir düzenleme bulunması halinde kişisel veriler, veri sahibinin rızası alınmadan işlenebilir.

b. **Fiili İmkânsızlık Sebebiyle İlgilinin Açık Rızasının Alınamaması**
Fiili imkânsızlık nedeniyle, rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınamayacak olan kişinin, kendisinin ya da başka bir kişinin hayatı veya beden bütünlüğünü korumak için, kişisel verisinin işlenmesi zorunlu olması durumunda veri sahibinin kişisel verileri işlenebilir.

c. **Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması**
Kişisel verilerin işlenmesi, veri sahibinin taraf olduğu bir sözleşmenin kurulması veya ifasıyla doğrudan ilgiliyse veri sahibinin kişisel verileri işlenebilir.

d. **Hukuki Yükümlülüğün Yerine Getirilmesi**
BARİYER GÜVENLİK hukuki yükümlülükleri yerine getirirken, kişisel veri işleme zorunlu olması halinde veri sahibinin kişisel verileri işlenebilir.

e. **Kişisel Veri Sahibinin Kişisel Verisini Alenileştirmesi**
Kişisel verisini alenileştiren veri sahiplerine ait kişisel veriler, alenileştirme amacıyla sınırlı olarak, kişisel verileri işlenebilir.

f. **Bir Hakkın Tesisi veya Korunması için Zorunlu Veri İşleme**
Veri işleme bir hakkın tesisi, kullanılması veya korunması için zorunlu ise veri sahibinin kişisel verileri işlenebilir.

g. **Meşru Menfaat için Zorunlu Veri İşleme**
Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek koşuluyla, BARİYER GÜVENLİK meşru menfaatleri için veri işlemenin zorunlu olması durumunda veri sahibinin kişisel verileri işlenebilir.

Özel Nitelikli Kişisel Verilerin İşlenmesi

BARİYER GÜVENLİK özel nitelikli kişisel verileri, Kanun ve Politika'da belirlenen ilkelere uygun, Kurul'un belirlediği yöntemlerle gerekli her türlü idari ve teknik önlemleri alarak, aşağıdaki usul ve esaslarla işler: Çalışan, çalışan adayı/stajyer/öğrencilerin özel güvenlik mevzuatından doğan hizmetlerin yerine getirilmesi ve iş kanunundan doğan yükümlülüklerin yerine getirilebilmesi için sağlık ve ceza ve güvenlik tedbiri kayıtları ölçülülük ilkesi kapsamında ve amacına uygun şekilde diğer verilerden ayrı şekilde işlenir, diğer verilerden ayrı şekilde muhafaza edilir.

Kişisel Veri Sahibinin Aydınlatılması

BARİYER GÜVENLİK , kişisel veri sahiplerini, hangi amaçlarla kişisel verilerinin işlendiği, hangi amaçlarla kimlerle paylaşıldığı, hangi yöntemlerle toplandığı, hukuki sebebi ve veri sahiplerinin kişisel verilerinin işlenmesinde sahip olduğu hakları konularında, ilgili mevzuata uygun şekilde bilgilendirir. Bu bakımdan kişisel verilerinin korunmasını, Politika'daki esaslar çerçevesinde hazırlanan diğer politika belgeleri ve aydınlatma metinlerine bağlı yürütülmektedir.

Kişisel Verilerin Aktarılması

BARİYER GÜVENLİK , kişisel veri işleme amaçları doğrultusunda, gerekli güvenlik önlemlerini alarak, kişisel verileri ve özel nitelikli kişisel verileri üçüncü kişilere (üçüncü kişi şirketlere, grup şirketlerine, üçüncü gerçek kişilere) hukuka uygun olarak aktarabilir. BARİYER GÜVENLİK aktarma işlemlerini, Kanun'un 8. maddesinde öngörülen düzenlemelere uygun şekilde işlemleri gerçekleştirir.

Kişisel verilerin akratılması için kişisel veri sahibinin açık rızası aranmakla birlikte, aşağıda belirtilen koşulların bir ya da birkaçına dayanılarak, Kurul tarafından öngörülen yöntemler de dahil gerekli tüm güvenlik önlemleri alınarak kişisel veriler üçüncü kişilere aktarılabilir.

a. Kanunlarda açıkça öngörülmesi,

b. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olması,

c. BARİYER GÜVENLİK 'ın hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

d. Veri sahibi tarafından kişisel verileri alenileştirilmiş olması şartıyla, alenileştirme amacıyla sınırlı,

e. BARİYER GÜVENLİK 'ın veya veri sahibinin veya üçüncü kişilerin haklarının tesisi, kullanılması veya korunması için zorunlu olması,

f. Veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla BARİYER GÜVENLİK meşru menfaatlerinin sağlanması içinzorunlu olması,

g. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünü koruması için zorunlu olması.

Özel nitelikli kişisel veriler, Politika'da belirlenen ilkelere uygun olarak, Kurul'un belirleyeceği yöntemler **de dahil olmak üzere, gerekli her türlü idari ve teknik tedbirler alınarak aşağıda belirlenen koşullarla aktarılabilir:**

a. **Sağlık dışındaki özel nitelikli kişisel veriler,** kanunlarda kişisel verilerin işlenmesine ilişkin açıkça bir hüküm olması halinde veri sahibinin açık rızası aranmaksızın, aksi halde veri sahibinin açık rızası alınması durumunda.

b. **Sağlığa ilişkin özel nitelikli kişisel veriler**, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza aranmaksızın, aksi halde veri sahibinin açık rızası alınması durumunda.

Çalışan, çalışan adayı/stajyer/öğrencilerin verileri aşağıdaki kişi ve kurumlara aktarılabilir; Yetkili Kamu Kurum ve Kuruluşları: Sosyal Güvenlik Kurumu, İŞKUR, Vergi Dairesi, Çalışma Bakanlığı, İçişleri Bakanlığı, Emniyet – Özel Güvenlik Şube, Adli Merciler; Hukuki Sebep: Kanuni zorunluluk; Müşteri Firmalar / Hizmet Verilen İşyerleri: Görev listeleri, kamera kayıtları, giriş-çıkış logları, isim-soyisim listesi, sözleşmeden doğan sorumluluk; Hukuki Sebep: Sözleşmenin ifası, 5188 sayılı Kanun gereği güvenlik kontrolü; Tedarikçiler – Hizmet Sağlayıcılar Bordro firması, yazılım firması, devriye takip sistemi firmaları; Hukuki Sebep: Meşru menfaat, sözleşmesel gereklilik; Grup Şirketleri / İş Ortakları: Personel görevlendirme süreçleri, raporlama; Avukatlar – Finansal Danışmanlar – Denetçiler: Hukuki süreçlerin yürütülmesi, raporlama; Sigorta Şirketleri: İş kazası, sağlık sigortası, BES süreçleri; Yargı Mercileri ve Arabulucular: Delil niteliğindeki kayıtlar, ödeme belgeleri, kamera görüntüleri. Personel verileri güvenli olmayan ülkelere aktarılmaz. Aktarım yapılacaksa KVKK md. 9 ve Kurul izni zorunludur.

Müşteri ve/ya iş ilişkisi sıfatıyla Şirketimizle sözleşme imzalayan, imzalayacak olan ve/ya ticari herhangi ilişkisi gerçek kişi müşteriler ile müşteri tüzel kişilerin yetkilisi, ortağı, çalışanı ve temsilcisi konumundaki gerçek kişilere ilişkin olarak işlenen kişisel veriler, belirtilen amaçların gerçekleştirilmesiyle sınırlı olmak üzere ve gerekli güvenlik tedbirleri alınarak; bağımsız denetim kuruluşlarına, mali müşavir ve yeminli mali müşavirlere, bankalara ve diğer finans kuruluşlarına, sigorta şirketlerine, bilgi teknolojileri, saklama, arşivleme, sunucu, bakım ve destek hizmeti aldığımız yurt içindeki ve hizmet altyapısının yurt dışındaki sunucular üzerinden sağlanması halinde yurt dışındaki hizmet sağlayıcılarına, gerektiğinde hukuki danışmanlık ve dava/itiraz süreçleri için çalıştığımız avukatlara ve danışmanlara, aynı ekonomik bütünlük içinde bulunduğumuz grup şirketlerine, sözleşmesel ilişkimiz kapsamında zorunlu olduğu ölçüde hizmet verdiğimiz müşteri grubu şirketlere ve kanunen yetkili kamu kurum ve kuruluşlarına aktarılabilmekte; bu aktarımlar yapılırken 6698 sayılı Kanun'un 8 ve 9. maddelerinde düzenlenen veri aktarım şartlarına ve Kişisel Verileri Koruma Kurulu'nun karar ve rehberlerine uygun hareket edilmektedir.

4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ALINAN ÖNLEMLER

BARİYER GÜVENLİK , Kanunda belirlenen usul ve esaslarla işlemekte olduğu kişisel verilerin korunması için gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmakta, bilinçlendirme ve eğitim faaliyetlerini gerçekleştirmektedir. Personel, sadece kendi görevini ifa etmek için gerekli sistem ve dosyalara erişim yetkisine sahip olmakta; departmanlar arası gereksiz erişimler engellenmektedir. Kullanıcı hesapları kişiye özeldir; kullanıcı adı ve şifreler hiçbir şekilde ortak kullanılmamakta, başkalarıyla paylaşılması disiplin suçu olarak kabul edilmektedir. Erişim yetkileri düzenli aralıklarla gözden geçirilmekte; görev değişikliği, unvan değişikliği veya işten ayrılma gibi hâllerde yetkiler derhal güncellenmektedir. Şirket bilgi sistemlerine erişim, güçlü parola politikaları ile korunmakta; parolaların belirli aralıklarla yenilenmesi zorunlu tutulmaktadır. Kritik sistemlere erişimde çok faktörlü kimlik doğrulama imkânları değerlendirilmekte ve teknik imkânlar ölçüsünde kullanılmaktadır. Taşınabilir cihazlar (dizüstü bilgisayar, harici disk, taşınabilir bellek vb.) üzerinden gerçekleştirilen veri işleme faaliyetlerinde, imkân dahilinde şifreleme ve parola koruması uygulanmakta; bu cihazların kullanımına ilişkin iç prosedürler belirlenmektedir. Sunucu ve istemci sistemlerde güncel antivirüs/antimalware yazılımları kullanılmakta; güvenlik yamaları ve güncellemeler

düzenli şekilde uygulanmaktadır. Uzaktan erişimler, VPN veya benzeri güvenli bağlantı mekanizmaları ile sınırlandırılmakta; yetkisiz erişim ve açıklara karşı gerekli tedbirler alınmaktadır. Kişisel verilerin bulunduğu ofis, arşiv odası, kamera kontrol odası ve benzeri alanlara fiziksel erişim, kimlik kartı, anahtar, güvenlik görevlisi kontrolü gibi yöntemlerle sınırlandırılmakta; yetkisiz kişilerin bu alanlara girişi engellenmektedir.

Sağlık verileri, adli sicil ve güvenlik soruşturması verileri, biyometrik veriler ve diğer özel nitelikli kişisel veriler, Kişisel Verileri Koruma Kurulu'nun özel nitelikli kişisel verilerin işlenmesi ve güvenliğine ilişkin ilke ve rehberlerinde sayılan teknik ve idari tedbirlere uygun şekilde ve diğer verilerden ayrı işlenmekte ve muhafaza edilmektedir.

İşlenen kişisel verilerin teknik ve idari tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi durumunda, BARİYER GÜVENLİK bu durumu mümkün olan en kısa süre içerisinde ilgili kişi ve birimlere haber verir.

6. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

BARİYER GÜVENLİK , kişisel verileri işleme amacı için gerekli olan süre ile ilgili mevzuatta öngörülen en az süre kadar muhafaza eder. BARİYER GÜVENLİK , öncelikle ilgili mevzuatta bir süre belirlenmiş ise bu süreye uygun; yasal bir süre öngörülmemiş ise kişisel verilerin işlenme amacı için gerekli süre kadar kişisel verileri saklar. Kişisel veriler belirlenen saklama sürelerinin sonunda, periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak, belirlenen yöntem (silme, yok etme veya anonimleştirme) ile imha edilir.

Kimlik – İletişim – Özlük – Performans: İş ilişkisinin bitiminden itibaren 10 yıl; Sağlık Verileri: İş sağlığı ve güvenliği mevzuatı gereği 15 yıl; Ceza Mahkûmiyeti – Güvenlik Tedbirleri:İş ilişkisinin bitiminden itibaren 10 yıl; Finans – Ücret – Banka Bilgileri: İşlem tarihinden itibaren 10 yıl; Kamera Kayıtları: 30 gün (özel güvenlik sektörü için uygun süre);Turnike – Giriş Çıkış Logları: 2 yıl; Talep/Şikâyet Kayıtları: 2 yıl; Araç Bilgileri: 10 yıl; İmza – Sözleşme Belgeleri: 10 yıl; Lokasyon / GPS Verileri: 90 gün – 6 ay arası (zorunluluk sona erdiğinde silinir); Denetim & Teftiş Verileri: 10 yıl. Tüm saklama süreleri dolduğunda veriler silinir, yok edilir veya anonim hale getirilir. Tüm kişisel verilerinizi özel nitelikli olan ve olmayan şeklinde ayrı ayrı korumak için gerekli teknik ve idari güvenlik önlemleri almakta ve kontrolleri yapmaktayız.

Müşteri ve/ya iş ilişkisi sıfatıyla Şirketimizle sözleşme imzalayan, imzalayacak olan ve/ya ticari herhangi ilişkisi gerçek kişi müşteriler ile müşteri tüzel kişilerin yetkilisi, ortağı, çalışanı ve temsilcisi konumundaki gerçek kişilerin kişisel verileri akdedilen sözleşme ve/ya ticari ilişki devam ettiği sürece ve sözleşme ilişkisinin sona ermesinden itibaren başta Türk Borçlar Kanunu, Türk Ticaret Kanunu ve vergi mevzuatı olmak üzere ilgili mevzuatta öngörülen zamanaşımı ve zorunlu saklama süreleri boyunca, bu sürelerin sonunda ise doğabilecek uyuşmazlık ve taleplerin ileri sürülebilmesi veya savunmanın tesis edilebilmesi için zorunlu olduğu ölçüde ilave sürelerle sınırlı olarak muhafaza edilmekte; bu sürelerin dolmasını müteakip ise Şirketimizin Kişisel Veri Saklama ve İmha Politikası uyarınca silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Bariyer Güvenlik, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi veya bu durumun tespit edilmesi hâlinde bu durumu en kısa sürede ve en geç 72 saat içinde Kurul'a ve ilgili kişilere bildirmekle yükümlüdür. Bu Veri İhlali Yönetim Politikası, Bariyer Güvenlik'in veri sorumlusu veya veri işleyen sıfatıyla işlediği tüm kişisel veriler bakımından, Bariyer Güvenlik bünyesindeki tüm birim ve çalışanlar ile Bariyer Güvenlik adına kişisel veri işleyen tedarikçi ve alt yüklenicileri kapsar. Kişisel veri ihlali; kişisel verilerin yetkisiz kişiler tarafından elde edilmesi, erişilmesi, ifşa edilmesi, değiştirilmesi, silinmesi, yok edilmesi, kaybolması, hukuka aykırı şekilde paylaşılması veya güvenliğinin başka surette ihlal edilmesi hâllerini ifade eder. Bu Politika kapsamında, hem elektronik ortamda hem de fiziki ortamlarda meydana gelen ihlaller kişisel veri ihlali olarak kabul edilir. Bariyer Güvenlik çalışanları, özel güvenlik görevlileri, yöneticiler ve Bariyer Güvenlik adına veri işleyen tedarikçiler; Kişisel verilerin kaybolduğunu, yetkisiz kişilerce ele geçirildiğini, sosyal medyada paylaşıldığını, yanlış kişiye gönderildiğini,Kamera kayıtları, ziyaretçi kayıt defterleri, turnike logları, vardiya listeleri, özlük dosyaları, elektronik posta sistemleri, bulut sistemleri veya benzeri veri kayıt ortamlarında şüpheli bir erişim, kopyalama veya paylaşım olduğunu,fark eder etmez; bu durumu derhal ve gecikmeksizin yazılı (e-posta, kayıtlı sistem) veya sözlü olarak doğrudan amirine ve KVKK'dan sorumlu birime / KVKK Komitesi'ne bildirmekle yükümlüdür. Bariyer Güvenlik adına veri işleyen konumundaki tedarikçiler, veri işleme sözleşmelerinde öngörülen süreyi beklemeksizin, ihlali tespit ettikleri anda Bariyer Güvenlik'e bildirim yapmakla yükümlüdür. Her bir ihlal veya ihlal şüphesi için ayrı bir "Veri İhlali Olay Dosyası" oluşturulur. Bu dosyada asgari olarak: İhlalin tespit edildiği tarih ve saat, İhlali bildiren kişi ve bildirim kanalı, İhlalin gerçekleştiği düşünülen tarih ve süre, İhlalin türü ve kapsamına ilişkin teknik ve idari bilgiler, Etkilenen veri kategorileri, kişi sayısı ve ilgili kişi grupları,

İhlalin giderilmesi ve etkilerinin azaltılması için alınan tedbirler,Kurul'a ve ilgili kişilere yapılan bildirimler ve tarihleri, İhlal sonrası alınan düzeltici ve önleyici tedbirler, kayda alınır ve en az ilgili mevzuattaki zamanaşımı süreleri boyunca saklanır.

7. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI VE BU HAKLARIN KULLANILMASI

7.1. Kişisel Veri Sahibinin Hakları

Kişisel veri sahipleri Kanundan kaynaklanan aşağıda belirtilen haklara sahiptirler:

- **i.** Kişisel veri işlenip işlenmediğini öğrenme,
- **ii.** Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- **iii.** Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- **iv.** Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- **v.** Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- **vi.** Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- **vii.** İşlenen verilerin münhasıran otomatik sistemler aracılığı ile analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- **viii.** Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Kişisel veri sahipleri, KVKK md. 11 kapsamındaki tüm haklara sahiptir: İşlenip işlenmediğini öğrenme, Düzeltme, Silme/yok etme, Aktarım bilgilerinin verilmesi, Otomatik işleme sonuçlarına itiraz, Zararı halinde tazminat talebi. Başvurular, şirket tarafından hazırlanan "Veri Sahibi Başvuru Formu" ile yapılır. Talepler niteliğine göre, en kısa sürede ve en geç otuz gün içinde ücretsiz sonuçlandırılır; ancak işlemin ayrıca bir maliyet gerektirmesi halinde Kişisel Verileri Koruma Kurulu tarafından belirlenecek tarifeye göre ilgili taraftan ücret talep edilebilir.

BARİYER GÜVENLİK , başvuruda bulunan kişinin isteğini, aşağıda yer alan durumlarda, gerekçesini açıklayarak reddedebilir:

- **i.** Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,
- **ii.** Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,
- **iii.** Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,
- **iv.** Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi,
- **v.** Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- **vi.** Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,
- **vii.** Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
- **viii.** Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması,
- **ix.** Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması,
- **x.** Orantısız çaba gerektiren taleplerde bulunulmuş olması,
- **xi.** Talep edilen bilginin kamuya açık bir bilgi olması.

Kanun'un 14. maddesi gereğince başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; BARİYER GÜVENLİK 'ın cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyette bulunabilir.

BARİYER GÜVENLİK , başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir. BARİYER GÜVENLİK , kişisel veri sahibinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

8. YÜRÜTME

Politika Yönetim Kurulu tarafından onaylanmış ve yürürlülüğe konulmuştur. Politika'nın teknik yürütümü **"Kişisel Veri Saklama ve İmha Politikası"** (Ek) ile sağlanmaktadır.

İş süreçlerinde, taraflar nezdinde Politikanın yürütümü **"Kişisel Verileri İşleme Müşteri Aydınlatma Metni" (Ek), "Çalışan ve Müşteri Kişisel Verileri İşleme Aydınlatma Metinleri" (Ek), "İnternet Sitesi Çerez Aydınlatma Metni" (Ek),** gerçekleştirilmektedir.

Kanun ve Politika'nın yürütülmesinden ve gerektiğinde güncellenmesinden Yönetim Kurulu, bu kapsamdaki tüm iş ve işlemlerin takibinden, koordinasyon ve denetiminden **BARİYER GÜVENLİK** Kişisel Verileri Koruma Komitesi sorumludur.

9. YÜRÜRLÜK ve İLANI

Politika yayımı tarihi itibariyle yürürlüğe girmiştir. Politika'da meydana gelecek değişiklikler BARİYER GÜVENLİK 'ın internet sitesinde (www.bariyerguvenlik.com.tr) yayımlanarak kişisel veri sahiplerinin, ilgili kişilerin erişimine sunulur. Politika değişiklikleri ilan edildiği tarihte uygulamaya girer.

EKLER

1. Veri Sahibi Başvuru Formu
2. Kişisel Veri Saklama ve İmha Politikası
3. Kişisel Verileri İşleme Müşteri Aydınlatma Metni
4. Tedarikçi Gizlilik ve Kişisel Verileri Koruma Sözleşmesi
5. Çalışan Kişisel Verileri İşleme Aydınlatma Metni
6. İnternet Sitesi Çerez Aydınlatma Metni