

Kasımpaşa Sportif Faaliyetleri A.Ş.

Kişisel Veri Saklama ve İmha Politikası

Amaç

Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") uyarınca veri sorumlusu **Kasımpaşa Sportif Faaliyetleri A.Ş. ("Şirket")** tarafından, bu Politika'nın dayanağı yasal Mevzuat'a uygun bir biçimde yürütülen kişisel verilerin işlenmesi ve korunması ile işlenen kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Kapsam

Bu Politika, Şirket'in faaliyetleri dahilinde ilişkili olduğu çalışanlarına, çalışan adaylarına, altyapı oyuncularını, aday oyuncularını ve oyuncularına, hissedarlarına, tedarikçi çalışan ve yetkililerine, sürücülerine, vasi/vasi/temsilcilere ve ziyaretçilerine ait kişisel verilerinin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla Şirket tarafından işlenmesi hallerini kapsamaktadır.

Yukarıda belirtilen kişisel veri sahiplerine, bu Politika'nın tamamı uygulanabileceği gibi, sadece birtakım hükümleri de uygulanabilecektir.

Dayanak

Bu Politika 6698 sayılı Kişisel Verilerin Korunması Kanunu, 30286 sayılı Veri Sorumluları Sicili Hakkında Yönetmelik ve 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e dayanılarak hazırlanmıştır.

Kişisel verilerin işlenmesi, korunması ve imhası konusunda bu Politika ile yürürlükte bulunan mevzuat arasında farklılık bulunması halinde Mevzuat hükümleri öncelikle uygulanacaktır.

Tanımlar

Bu Politika'nın uygulanmasında;

- a) **Alıcı grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- b) **Envanter:** Şirket tarafından Mevzuat gereği hazırlanmış olan Kişisel Veri Envanterini,
- c) **İlgili Kullanıcı:** Verilerin teknik olarak depolanması, korunması ve sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,
- ç) **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- d) **Kanun:** 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,
- e) **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 ortamı,
- f) **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- g) **Kişisel veri sahibi/İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,
- ğ) **Kişisel veri envanteri:** Şirket'in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami

süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandığı envanteri,

- h) Kişisel verilerin anonim hale getirilmesi:** Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
- ı) Kişisel verinin 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- i) Kişisel verinin silinmesi:** Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
- j) Kişisel verilerin yok edilmesi:** Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
- k) Kurul:** Kişisel Verileri Koruma Kurulunu,
- l) Kurum:** Kişisel Verileri Koruma Kurumunu,
- m) Özel nitelikli kişisel veri:** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri,
- n) Periyodik imha:** Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,
- o) Politika:** Kanun uyarınca veri sorumlusu olduğu kabul edilen Şirket'in, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptığı bu Kişisel Veri Saklama ve İmha Politikasını,
- ö) Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,
- p) Şirket:** Ticari unvanı Kasımpaşa Sportif Faaliyetleri A.Ş. olan şirketi,
- r) Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişiyi,
- s) Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
- ş) Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

Bu Politika'da yer almayan tanımlar için Kanundaki tanımlar geçerlidir.

Kişisel Veri Kayıt Ortamları

Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda, başta KVKK hükümleri olmak üzere, ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

a) Teknik kayıt ortamları:

- Bilgisayarlar

- Ağ üzerinden veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
- Bulut üzerinden sunulan hizmet platformları (Catapult)

Teknik olmayan veri kayıt ortamları:

- Kâğıtlar,
- Birim Dolapları.

Kişisel Verilerin Saklanması ve İmhasında Genel İlkeler

Şirket, Sicile kayıt yükümlülüğü olan bir Veri Sorumlusudur ve bünyesinde tutmakta olduğu kişisel verileri, Envantere uygun bir şekilde saklamak ve gerektiğinde silmek, yok etmek ya da anonim hale getirmek için bu Politika'ya uygun hareket etmek ile yükümlü olduğunu kabul, beyan ve taahhüt eder.

Kişisel verilerin saklanması ve imhasında aşağıdaki ilkeler geçerli olacaktır:

- I. Şirket, Kanun'un 4'üncü maddesinde yer alan genel ilkelere uyulacağını,
- II. Şirket, bu Politika'yı hazırlamış olmanın tek başına kişisel verilerin mevzuata uygun olarak silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmeyeceğini,
- III. Şirket, kişisel verileri saklarken, silerken, yok ederken veya anonim hale getirirken, Kanun'un 12'inci maddesinde yer alan güvenlik tedbirlerine, ilgili Mevzuat'ta yer alan hükümlere, Kurul kararlarına ve Politika'ya uygun hareket edeceğini,
- IV. Şirket, bünyesinde bulundurduğu kişisel verilerin amacı tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi sırasında bu Politika'ya ve Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını,
- V. Şirket, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alacağını ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklayacağını,

kabul, beyan ve taahhüt eder.

Saklamayı Gerektiren İşleme Amaçları

Kişisel veriler, Anayasa'nın 20. maddesine ve KVKK'nın 4. maddesine uygun olarak, veri sorumlusu Şirket tarafından aşağıdaki amaçlarla işlenmektedir:

- ❖ Altyapı Sporcu Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- ❖ Oyuncu Transfer Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- ❖ Bilgi Güvenliği Süreçlerinin Yürütülmesi
- ❖ Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- ❖ Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- ❖ Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
- ❖ Denetim / Etik Faaliyetlerinin Yürütülmesi
- ❖ Erişim Yetkilerinin Yürütülmesi
- ❖ Finans Ve Muhasebe İşlerinin Yürütülmesi
- ❖ Fiziksel Mekan Güvenliğinin Temini
- ❖ Görevlendirme Süreçlerinin Yürütülmesi
- ❖ Hukuk İşlerinin Takibi Ve Yürütülmesi
- ❖ İş Faaliyetlerinin Yürütülmesi / Denetimi
- ❖ İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- ❖ İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- ❖ Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- ❖ Oyuncu Sakatlık Teşhis Ve Tedavi Süreçlerinin Yürütülmesi
- ❖ Özlük Dosyalarının Oluşturulması

- ◆ Performans Değerlendirme Süreçlerinin Yürütülmesi
- ◆ Sözleşme Süreçlerinin Yürütülmesi
- ◆ Sponsorluk Faaliyetlerinin Yürütülmesi
- ◆ Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
- ◆ Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
- ◆ Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi

Kişisel Verilerin İmhasını Gerektiren Hukuki, Teknik ve Diğer Sebepler

Şirket tarafından ilgili kişilere ait kişisel veriler;

- a) Kanun'un 4'üncü maddesinde yer alan genel ilkeler,
- b) Veri sahibi ilgili kişinin talebi,
- c) Yasal yükümlülüklerin sona ermesi,

Hukuki, teknik ve diğer sebepleri için; ancak bunlarla sınırlı olmamakla birlikte benzer amaç ve sebeplerle imha edilmektedir.

Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesi ve Erişilmesinin Önlenmesi İçin Alınmış Teknik ve İdari Tedbirler

Veri sahibi ilgili kişilere ait kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için Şirket tarafından alınan teknik ve idari tedbirler aşağıda sıralanmıştır:

- I. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- II. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- III. Anahtar yönetimi uygulanmaktadır.
- IV. Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- V. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- VI. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- VII. Çalışanlar için yetki matrisi oluşturulmuştur.
- VIII. Erişim logları düzenli olarak tutulmaktadır.
- IX. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- X. Gerekliğinde veri maskeleyme önlemi uygulanmaktadır.
- XI. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- XII. Güncel anti-virüs sistemleri kullanılmaktadır.
- XIII. Güvenlik duvarları kullanılmaktadır.
- XIV. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- XV. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- XVI. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- XVII. Kişisel veri güvenliğinin takibi yapılmaktadır.
- XVIII. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- XIX. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- XX. Kişisel veriler mümkün olduğunca azaltılmaktadır.
- XXI. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- XXII. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- XXIII. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- XXIV. Mevcut risk ve tehditler belirlenmiştir.
- XXV. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- XXVI. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

- a) Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- b) Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- c) Sızma testi uygulanmaktadır.
- d) Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- e) Şifreleme yapılmaktadır.
- f) Veri kaybı önleme yazılımları kullanılmaktadır.

Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Teknik ve İdari Tedbirler

Veri sahibi ilgili kişilere ait kişisel verilerin hukuka uygun olarak imha edilmesi için Şirket tarafından alınmış teknik tedbirler,

- a) Kişisel verilerin imhasına ilişkin teknolojik açıdan gerekli en güncel sistemlerinin kullanılması, gizlilik ve bilgi güvenliği tedbirlerinin alınması,
- b) İlgili Kullanıcılar'ın kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması, ortadan kaldırılması ve silinmiş verileri geri getirme yetkisinin kaldırılması,
- c) Bulut sistemler ile merkezi sunucuda yer alan kişisel verilerin silme komutu verilerek geri döndürülemeyecek şekilde silinmesi,
- d) Bu sayılanların haricinde teknik olan kayıt ortamlarından uygun olanlar için yok etme (fiziksel demanyetize etme, üzerine yazma) ya da anonimleştirme yöntemlerinden kişisel verinin niteliğine göre uygun olanın tercih edilmesi,
- e) Teknik olmayan kayıt ortamlarında bulunan kişisel verilerin imhası için silme (karartma vs.), yok etme (fiziksel yok etme) yöntemlerinin uygulanması,

olarak belirlenmiştir.

Veri sahibi ilgili kişilere ait kişisel verilerin hukuka uygun olarak imha edilmesi için Şirket tarafından alınmış idari tedbirler,

- a) Kişisel verilerin imhası hakkında gerekli uygulama çalışmasının düzenli olarak yapılması,
- b) Şirket'e ait iş yeri dahilinde özellikle teknik olmayan veri kayıt ortamlarının fiziksel imhasına ilişkin gerekli ekipmanın bulundurulması,

olarak belirlenmiştir.

Kişisel Verilerin Saklanma ve İmha Süreçlerinde Görevli Birimler ve Bilgileri

Şirket'in kişisel verileri saklama ve imha süreçlerinde yer alan görevli birimlerinde çalışan personelin unvanlarını ve görev tanımlarını gösteren liste EK-1'de yer almaktadır.

Saklama ve İmha Süreleri

Veri sahibi ilgili kişilere ait kişisel verilerin kategorilerine göre saklama ve imha sürelerini gösteren tablo EK-2'de yer almaktadır.

Periyodik İmha Süreleri

Şirket tarafından işlenen kişisel verilerin kategorilerine göre bu Politika'nın ekinde bulunan saklama ve imha sürelerini gösteren tabloda belirtilen süreler haricinde periyodik imha süreleri 6 (altı) aydır.

Kişisel Verileri İlgili Kişinin Talep Etmesi Durumunda Silme ve Yok Etme Süreleri

İlgili kişi, Kanun'un 13'üncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

- a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç 30 (otuz) gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.
- b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye en geç 10 (on) gün içinde bildirir; üçüncü kişi nezdinde gerekli işlemlerin yapılmasını temin eder.
- c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanun'un 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Yürütme

Veri Saklama ve İmha Politikası hükümlerinin güncellenmesinden aktif olarak süreçlerin denetlenmesinden, veri güvenliği ilkelerinin Şirketimiz nezdinde farkındalığının artırılmasından ve uygulamasından Şirketimizin KVKK Uyum ve Uygulama Komitesi Üyeleri birlikte sorumludur.