KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Kişisel Veri İmha Politikasının (“Politika”) amacı Türkiye Dans Sporları Federasyonu’ nun mevcut ve potansiyel sporcuları, antrenörleri, iş ortakları, ziyaretçileri, yöneticileri, çalışan adayları, işbirliği içinde bulunulan kurum çalışanları ve yetkilileri ile ilgili üçüncü kişilere ait kişisel verilerin imhası hususundaki prensiplerin belirlenmesi, Anayasa’nın 20’nci maddesi, 6698 sayılı Kişisel Verilerin Korunması Kanunu (‘’Kanun’’), 30224 s. Resmi Gazete' de yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") ve ilgili mevzuatlarına uyum sağlanması ve bu doğrultuda gerekli imha usul ve sistemlerinin belirlenmesinden ibarettir.

2. TANIMLAR

Bu politikada ver verilen;

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

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 kişileri,

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

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,

Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

Kurul: Kişisel Verileri Koruma Kurulunu,

Periyodik imha: Kanunda yer alan kişisel verilerin işlenme 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,

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.

3. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN SEBEPLER

Kanun ve diğer ilgili mevzuat çerçevesinde; sporculara, antrenörlere, çalışanlara ve diğer üçüncü kişilere ait kişisel veriler hukuki, teknik ve diğer sebeplerle işlenmekte, saklanmakta ve imha edilmektedir.

İlgili kullanıcılar tarafından veri sahiplerine ait kimlik ve iletişim bilgileri, lokasyon bilgileri, ödemeye ilişkin veriler, sertifika bilileriniz, hukuki işlem bilgileri, imza verileri, görsel verileri, internet sitesini ziyaret veya ortak internet ağına katılma halinde dijital iz verileri gibi genel nitelikli kişisel veriler ile veri sahibinin açık rızasının varlığı halinde sağlık verileri, ırk ve etnik köken, cezai mahkumiyet ve güvenlik tedbirleri gibi özel nitelikli kişisel verileriniz ilgili kişi olan sporcu ve antrenörlerden ve/veya sporcu/antrenör adaylarının lisans kayıtlarının tutulması, lisanslarının oluşturulması, sicillerinin kayıt altında tutulması, müsabakalara katılımının sağlanması ve takibi, ilgilendikleri dans sporu dallarının belirlenmesi, sınav ve seminerlerin düzenlenmesi ve katılımının sağlanması, kulüp bilgilerinin belirlenmesi, talep ve şikâyetlerinizin kayıt altına alınması, çeşitli kanallar üzerinden cevaplanması ve yönetilmesi, sunulan hizmetin özelleştirilmesi ve geliştirilmesi, tanıtım, reklam, kampanya, çekiliş, bilgilendirme, iletişim faaliyetlerinin yürütülmesi, hizmetlerimizin geliştirilebilmesi amacıyla memnuniyet anketi yapılması, organizasyon ve etkinlik yönetimi, bilgi ve veri güvenliğinin temini ve bilgi sistemlerinin sürekliliğinin sağlanması, 5651 sayılı kanun uyarınca elektronik ortamda oluşan log kayıtlarınızın tutulması, resmi kurum ve kuruluşlara gerekli bildirimlerin yapılması, kurumun güvenliğinin sağlanması, inceleme, soruşturma, raporlama, iç kontrol ve denetim faaliyetlerinin gerçekleştirilmesi ve Federasyon kapsamında hizmetlerin yürütülmesi ve geliştirilmesi, Federasyon faaliyetlerinin mevzuata ve politika ve prosedürlerine uyum sağlanması amaç ve sebepleriyle sınırlı olarak işlenmekte saklanmakta ve imha edilmektedir.

Çalışan ve çalışan adaylarına ait kişisel verileri (kimlik verileri, iletişim verileri, lokasyon verileri, görsel verileri, özlük verileri, eğitim verileri, adli sicil kaydı, imza verisi, dijital iz veriler, vb. veriler) ve özel nitelikli kişisel veriler (sağlık verileri) paylaşılan diğer veriler, (*ayrıca özel nitelikli kişisel verilerden olup da kimlik belgelerinde yer alan din bilgisi ve kan grubu gibi bilgileri de dolaylı olarak kimlik ve/veya ehliyet suretinden gelebilmektedir.*) iş akdinin ifası, performans değerlendirmesi ile yan hak ve menfaatlerin temini, eğitim, oryantasyon ve acil durum tatbikat süreçlerinin yürütülmesi, özlük dosyasının oluşturulması dâhil mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi, işyeri hekimi tarafından işe giriş muayene ve periyodik muayene ile sağlık hizmetlerinin sunulması, iş sağlığı ve güvenliği ile ilgili yükümlülüklerin yerine getirilmesi, etkinlik, seyahat, vize ve organizasyon süreçlerinin yürütülmesi, işyeri güvenliğinin sağlanması amacıyla kamera kayıtlarının alınması, giriş çıkışların takibi, 5651 sayılı Kanun uyarınca elektronik ortamda oluşan log kayıtlarının tutulması, Federasyonumuzun tanıtım görsellerinin oluşturulabilmesi için işyerinde video ya da fotoğraf çekimi yapılması durumunda görsel verilerin işlenmesi ve yayınlanması, inceleme, soruşturma, raporlama, iç kontrol ve denetim faaliyetlerinin gerçekleştirilmesi, işten çıkıldığı takdirde iş sürekliliğinin sağlanabilmesi için mail arşivleri ile masaüstü dosyalarının saklanması ve kullanılması, kamu kurum ve kuruluşlarının taleplerinin yerine getirilmesi ve bildirimlerin yapılması, veri ve bilgi güvenliğinin sağlanması, erişim yetkilerinin yönetimi, hizmetlerin sunulması, yürütülmesi, geliştirilmesi, taleplerin ve cevapların karşılanması, ilgili

mevzuata, politika ve prosedürlere uyum sağlanması amaç ve sebepleriyle sınırlı olarak işlenmekte saklanmakta ve imha edilmektedir.

4. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi işleminde izlenen süreç; silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi, erişim yetki ve kontrol matrisi kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi, ilgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi, ilgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması şeklinde gerçekleştirilir.

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

Merkezi sunucuda yer alan dosyaların işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılır.

Kullanılan veri tabanlarında kişisel verilerin bulunduğu ilgili satırlar, veri tabanı komutları ile silinir.

5. KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel veriler kanunen veya veri sorumlusu tarafından belirlenen saklama süreleri sona erdiğinde ilgili kullanıcı tarafından, demanyetize etme, fiziksel imha ve üzerine yazma yöntemleri kullanılarak yok edilir.

6. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Anonimleştirme ile; kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilir.

7. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ YÖNTEMLERİ

Anonim hale getirme, bir veri kümesindeki tüm doğrudan veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır.

Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir.

Anonim hale getirmede aşağıdaki tabloda yer verilen yöntemler kullanılmaktadır:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt Ve Üst Sınır Kodlama • Global Kodlama • Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro Birleştirme • Veri Değiş Tokuşu

Kişisel verilerin; niteliği, büyüklüğü, fiziki ortamlarda bulunma yapısı, çeşitliliği, sağlanmak istenen fayda ve işleme amacı, işlenme sıklığı, aktarılacağı tarafın güvenilirliği, anonim hale getirilmesi için harcanacak çabanın anlamlı olması, anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı, dağıtıklık/merkezilik oranı, kullanıcıların ilgili veriye erişim yetki kontrolü kıstasları ve anonimliği bozacak bir saldırı kurgulanması, hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali gözetilerek her bir kişisel veri grubu için yukarıda belirtilen yöntemlerden uygun olanları kullanılarak anonimleştirme sağlanır.

8. KİŞİSEL VERİLERİN KAYIT ORTAMLARI

Federasyon tarafından toplanan kişisel veriler, aşağıda yer alan tabloda belirtilen kayıt ortamlarında hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Kayıt Ortamları	**Elektronik Olmayan Kayıt Ortamları**
• Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS.) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Yazıcı, tarayıcı, fotokopi makinesi.	• Kağıt • Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) • Yazılı, basılı, görsel ortamlar

9. SORUMLULUK VE GÖREV DAĞILIMLARI

Türkiye Dans Sporları Federasyonu'nun tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya

yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

10. KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜRELERİ

Türkiye Dans Sporları Federasyonu tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak; Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde, süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Çalışan adaylarına ait kişisel veriler	İşe başvurudan itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş Kanunu kapsamında saklanılan veriler	İş ilişkisinin sona ermesinden itibaren 10 yıl	
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler	İş ilişkisinin sona ermesinden itibaren 15 yıl	
SGK mevzuatı kapsamında tutulan veriler	İş ilişkisinin sona ermesinden itibaren 10 yıl	
Sair ilgili mevzuat gereği toplanan veriler	İlgili mevzuatta öngörülen süre kadar	
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması halinde	Dava zaman aşımı müddetince	
Müşterilere ait kişisel veriler	TTK m. 82'e göre ticari defterlere dayanak teşkil eden faturaların düzenlenmesine esas bilgiler anılan kanun maddesi gereği 10 yıl, bunun dışındaki Müşteri Bilgileri ise azami 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log kayıtları	10 yıl	
Kamera kayıtları	6 ay	
Firmalar Tarafından Federasyon ile Paylaşılan Bilgiler	Federasyon ile olan ilişkisi süresince ve sona ermesinden itibaren TBK m. 146 uyarınca 10 yıl	
Potansiyel müşterilerle ilgili telefon kayıtları	Görüşmeden itibaren 2 yıl	

11. PERİYODİK İMHA SÜRESİ VE İMHA TUTANAKLARI

Yönetmelik uyarınca periyodik imha 6 ayda bir yapılır. Buna göre, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir. Öngörülen saklama süresi geçtiği tespit edilen kişisel veriler; veri sorumlusu tarafından silme, yok etme veya anonim hale

getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde silinir, yok edilir veya anonim hale getirilir.

Kişisel verilerin çeşitli yöntemler kullanılarak imha edilmesi halinde, hangi kişisel verilerin imhasının kim tarafından, ne zaman ve ne şekilde yapıldığı tutanak altına alınarak imha işlemini gerçekleştiren kişi tarafından imzalanır. İmha tutanakları 3 yıl süre ile saklanır.

12. ALINAN TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması ve imha edilmesi ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için teknik ve idari tedbirler alınmıştır.

13.1. İdari Tedbirler

- "Kişisel Veri İşleme Envanteri" hazırlanmıştır.
- "Kişisel Verilerin Korunması Politikası", "Çalışan Bilgilendirme, Taahhütname ve Elektronik Posta Kullanım Politikası" ve "Kişisel Veri Saklama ve İmha Politikası" başta olmak üzere kurumsal politikalar hazırlanmıştır.
- Veri sorumlusu ve veri işleyen 3. Kişilerle yapılmış sözleşmelere KVKK uyumluluğuna ilişkin ek protokoller imzalanmıştır.
- Özel nitelikli veri işleyen çalışanlar ve genel nitelikli veri işleyen çalışanlar ile ayrı ayrı gizlilik sözleşmeleri akdedilmiştir.
- Kurum içi periyodik/ rastgele denetimler ve risk analizleri yapılmaktadır.
- Mevcut iş sözleşmelerine KVKK uyumluluğuna ilişkin ek hükümler ilave edilmiştir.
- KVKK ve bilgi güvenliğine ilişkin eğitimler ve farkındalık toplantıları gerçekleştirilmiştir.

13.2.Teknik Tedbirler

Yetki Matrisi hazırlanarak Yetki Kontrolü sağlanmaktadır. Erişim Logları ve Log Kayıtları tutulmaktadır. Şifreleme kullanılmaktadır. Kullanıcı Hesap Yönetimi ile her ilgili kullanıcının işlemleri tespit edilebilmektedir. Periyodik olarak yapılan Sızma Testleri, Veri Kaybı Önleme Yazılımları, Güvenlik Duvarları ve Güncel Anti-Virüs Sistemleri ile Uygulama ve Ağ Güvenliği sağlanmaktadır. Saldırı Tespit ve Önleme Sistemleri, veri maskeleme ve yedekleme yapma suretiyle kişisel verilerin güvenliği sağlanmaktadır.

14. İLGİLİ KİŞİNİN HAKLARI

Kişisel verilerin korunması mevzuatı çerçevesinde, ilgili kişisel verilerinin silinmesini veya yok edilmesini isteme, kişisel verilerinizin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesine veya kişisel verilerin silinmesine veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme haklarına sahiptir.

Kanun kapsamında, ilgili kişiler kişisel verilerine ilgili başvurularınızı bilgi@tdsf.gov.tr adresinden form ile aşağıda belirtilen kanallardan birini kullanarak;

- bilgi@tdsf.gov.tr adresine kimlik teyidinizin yapılması sağlanarak bizzat; veya
- Güvenli elektronik veya mobil imzanız ile bilgi@tdsf.gov.tr adresine veya
- Kimlik teyidinizin yapılması sağlanarak, Kanun ve ilgili mevzuatta belirtilen diğer usuller ile veri sorumlusuna iletebilecektir.

Veri sorumlusu, Kanunu’nun 13. maddesine uygun olarak, başvuru taleplerini, talebin niteliğine göre ve en geç 30 (otuz) gün içinde sonuçlandıracaktır. İşlemin maliyet gerektirmesi halinde, Kişisel Verilerin Korunması Kurulu tarafından belirlenen tarife uygulanacaktır.