

# **TÜRKİYE FOTOĞRAF SANATI FEDERASYONU**

**VERİ SİLME POLİTİKASI VE ARŞİVLEME DÖKÜMANI**

02.06.2025

# DOKÜMAN ONAY SAYFASI

## HAZIRLAYAN

Adı Soyadı	Tarih	İmza
Mehmet Çağdaş SAYGILI	19.02.2022	
Onur DEMİRKAPI	19.02.2022	
Onur DEMİRKAPI Burak ŞENBAK	04.05.2025	

## ONAYLAYAN

Adı Soyadı	Görevi	Tarih	İmza
Mehmet KILIÇOĞLU	Başkan	02.06.2025	
Ela AKTAY	Genel Sekreter	02.06.2025	

# DOKÜMAN DEĞİŞİKLİK SAYFASI

Versiyon No	Sorumlu	Değişiklik Tarihi	Açıklama
V.1.0.0	Mehmet Çağdaş SAYGILI	19.02.2022	İlk yazım.
V.1.1.0	Onur DEMİRKAPI	12.02.2022	Güncellemeler.
V.1.1.1	Mehmet Çağdaş SAYGILI Onur DEMİRKAPI	18.03.2022	Düzeltilmeler ve güncellemeler.
V.1.1.2	Onur DEMİRKAPI Burak ŞENBAK	04.05.2025	Düzeltilmeler ve güncellemeler.

# İÇİNDEKİLER

DOKÜMAN ONAY SAYFASI	2
DOKÜMAN DEĞİŞİKLİK SAYFASI	3
İÇİNDEKİLER	4
GİRİŞ	5
AMAÇ VE KAPSAM	5
KISALTMALAR	5
DAYANAK	5
SORUMLULUK VE GÖREV DAĞILIMLARI	5
KAYIT ORTAMLARI	6
SAKLAMAYA VE İMHAYA İLİŞKİN AÇIKLAMALAR	7
SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER	7
SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI	7
İMHA GEREKTİREN SEBEPLER	7
TEKNİK VE İDARİ TEDBİRLER	8
TEKNİK TEDBİRLER	8
İDARİ TEDBİRLER	10
KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	11
KİŞİSEL VERİLERİN SİLİNMESİ	11
KİŞİSEL VERİLERİN YOK EDİLMESİ	11
KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ	12
SAKLAMA VE İMHA SÜRELERİ	12
PERİYODİK İMHA SÜRESİ	13
POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI	13
POLİTİKA'NIN GÜNCELLENME PERİYODU	14
POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI	14

# GİRİŞ

## AMAÇ VE KAPSAM

Türkiye Fotoğraf Sanatı Federasyonu (TFSF) için geliştirilen yazılımlar ile yönetilen verilere ait yedekleme, silme ve arşivleme politikalarını içermektedir.

## KISALTMALAR

Doküman içerisinde yer alan kısaltmalar bu başlık altında listelenmiştir. Doküman genelinde bu bölümden sonra kısaltmalar kullanılacaktır.

Kısaltma	Açıklama
TFSF	Türkiye Fotoğraf Sanatı Federasyonu
EYS	Elektronik Yönetim Sistemi
Kanun	Kişisel Verileri Koruma Kanunu
Kurul	Kişisel Verileri Koruma Kurulu
KVSİP	Kişisel Verileri Saklama ve İmha Politikası
Başkan	TFSF Yönetim Kurulu Başkanı
Genel Sekreter	TFSF Yönetim Kurulu Genel Sekreteri
Veri Sorumlusu	TFSF Tarafından Atanan Yetkili Yönetim Kurulu Üyesi
Sistem Yöneticisi	TFSF Tarafından Kiralanmış Sunucuları Yönetmekle Yetkili Teknik Personel
Politika	TFSF Veri Silme ve Arşivleme Politikası
Log	İşlem Kayıtları
YK	Yönetim Kurulu
Yarışma Düzenleyici	Yarışma Düzenleyen Kurum veya Kuruluş
Yarışma	TFSF, Kurum veya Kuruluşların Düzenlediği Fotoğraf Yarışmaları
Temsilci	Yarışmalarda TFSF yi Temsilen Bulunan Yetkilendirilmiş Kişi

## DAYANAK

TFSF projelerinde verilerin imhası 6689 sayılı Kanun uyarınca Kurul tarafından hazırlanan "Kişisel Verileri Saklama ve İmha Politikası"na dayanmaktadır.

(<https://www.kvkk.gov.tr/Icerik/5386/KVKK-KISISEL-VERI-SAKLAMA-ve-IMHA-POLITIKASI>)

## SORUMLULUK VE GÖREV DAĞILIMLARI

Kurul'un tüm birimleri ve çalışanları, sorumlu birimce hazırlanan Politika kapsamında alınmakta olan teknik ve idari tedbirleri gereği gibi uygulanması, birim sorumluları ve

alıřanların eđitimi, izlenmesi ve srekli denetimi ile kiřisel verilerin hukuka aykırı olarak iřlenmesinin nlenmesi, kiřisel verilere hukuka aykırı olarak eriřilmesinin nlenmesi ve kiřisel verilerin hukuka uygun olarak saklanması sađlanması amacı ile kiřisel verilerin iřlendiđi tm ortamlarda veri gvenliđini sađlamaya ynelik idari ve teknik tedbirlerin alınması, gerekli durumlarda log tutulmasının sađlanması konularında aktif olarak destek verir.

Kiřisel verileri saklama ve imha srelerinde grevli olanların unvanları ve grev tanımlarına ait dađılım ařađıdaki tabloda belirtilmiřtir.

UNVAN	GREV
Bařkan	Tm birimlerin ve alıřanların "Politika"ya uygun olarak hareket etmesinden sorumludur.
Genel Sekreter	Veri Sorumlusu tarafından bildirilen silinecek verilerin kayıt altına alınması, gerekli grldđ takdirde YK kararı alınmasının sađlanmasından sorumludur.
Veri Sorumlusu	Verilerin gvenliđinin takibi, saklanacak ve periyodik olarak silinecek verilerin tespiti, periyodik olarak kontrol ederek silinmesi gereken verilerin belirlenmesi, korunması gereken bilgilerin yedeklenmesinin takibi iřlemlerinden sorumludur.
Sistem Yneticisi	Verilerin gvenliđinin sađlanması, Veri Sorumlusunca iletilen silinecek verilerin silinmesi, yedeklenmesi nem arz eden bilgilerin periyodik olarak yedeklenmesinin sađlanması, veri yedeklerinin sunucu dıřında bařka bir ortama aktarımı ve veri yedeklerinin korunmasından sorumludur.
Temsilci	Grevlendirildiđi yarıřmaya katılan kiřilerin bilgilerine ve yarıřmaya katıldıkları fotođraflara eriřebilen, yarıřma sresince bu verilerin gvenliđinden sorumlu olan, gerekli durumlarda ilgili bilgileri Yarıřma Dzenleyiciye veya TFSS tarafından yetkili kılınan kiřilere aktarması gereken, yarıřma bařlangıcından sonuların aıklanma tarihinden itibaren 90 gn sonrasına kadar verilerin gvenliđinden sorumludur. Yz yze form ile kayıt alınan yarıřmalarda fiziki evrak gvenliđinin sađlanmasından, gerekli durumlarda bilgi gvenliđine uygun řekilde TFSS genel merkezine iletilmesinin sađlanmasından ve 90 gn sonrasında fiziki evrakların geriye dndrlemez řekilde imha edilmesinden sorumludur.

## KAYIT ORTAMLARI

Kiřisel veriler; sunucular (etki alanı, yedekleme, veritabanı, web, dosyalar, dosya paylařımları vb), elektronik postalar, loglar, kullanıcı bilgileri, ilgili kurumlara aktarılabilecek verilerin aktarılmasına kadar hukuka uygun olarak gvenli bir řekilde saklanır.

## SAKLAMAYA VE İMHAYA İLİŞKİN AÇIKLAMALAR

TFSF tarafından; çalışanlar ve birim sorumluları, web sitesi ziyaretçileri, kurumların veya kuruluşların çalışanlarına ait kişisel veriler kanuna uygun olarak saklanır ve imha edilir.

## SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

TFSF, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 4982 sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürütülmekte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

## SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

TFSF, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar;

- Kurumsal iletişimi sağlamak
- Kurum güvenliğini sağlamak
- İstatistiksel çalışmalar yapabilmek
- Yarışma Düzenleyiciler ile imzalanan protokoller neticesinde Yarışma iş ve işlemlerini yürütmek
- Veriler üzerine doğrudan erişimi olan yetkililerin yaptığı iş ve işlemlerin Log'larını tutmak
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
- Yasal raporlar hazırlamak
- Kullanıcı destek süreçlerini yönetmek
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü

## İMHA GEREKTİREN SEBEPLER

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesi veya saklanması gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun TFSSF tarafından kabul edilmesi,
- TFSSF'nin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevap verilmemesi hallerinde; Kurula şikayette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması gibi durumlarda, TFSSF tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

## TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanununun 12 nci maddesiyle Kanununun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde TFSSF tarafından teknik ve idari tedbirler alınır.

## TEKNİK TEDBİRLER

TFSSF tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır;

- Sızma (Penetrasyon) testleri ile TFSSF bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmalıdır,
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmelidir,
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır,
- TFSSF bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır,
- Bulut çözümleri sunan hizmet sağlayıcı firmanın güvenlik, fiziksel erişim, yazılımsal güvenlik protokollerinin periyodik olarak incelenmektedir,

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır
- TFSSF içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır
- TFSSF, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için TFSSF tarafından buna uygun bir sistem ve altyapı oluşturulmuştur
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli

güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanmaktadır

- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

## İDARİ TEDBİRLER

TFSF tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların ve birim sorumlularının niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili kanunlar ve mevzuatlar hakkında eğitimler verilmektedir.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce TFSF tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum için periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

## KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, TFSS tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

## KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel veriler aşağıdaki tabloda belirtilen yöntemlerle silinir.

Veri Kayıt Ortamı	Açıklama
Sunucularda yer alan kişisel veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler Veri Yöneticisi tarafından tespit edilerek Sistem Yöneticisi tarafından silme işlemi yapılır
Elektronik ortamda yer alan kişisel veriler	Eposta gibi elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, Veri Yöneticisi ve Sistem Yöneticisi hariç diğer çalışanlar ve birim yetkilileri için erişilmez ve tekrar kullanılmaz hale getirilir
Fiziksel ortamda yer alan kişisel veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca okunmayacak şekilde çizilerek, boyanarak, silinerek erişilmez kılınır.
Taşınabilir medyada bulunan kişisel veriler	USB bellek, usb disk, cd, dvd gibi saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sonra erenler, Sistem Yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece Sistem Yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

## KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel veriler aşağıda belirtilen yöntemlerle yok edilir.

Veri Kayıt Ortamı	Açıklama
Fiziksel ortamlarda yer alan kişisel veriler	Kağıt ortamında yer alan kişisel verilerden saklanması gerektiren süre sona erenler, kağıt kırma makinelerinde geri dönmeyecek şekilde yok edilir
Optik/manyetik medyada yer alan kişisel veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanması gerektiren süre sonra erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca manyetik

	medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerinde veriler okunmaz hale getirilir.
--	--

## KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilirse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler 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 kişi ile ilişkilendirilemez hale getirilmesi gerekir.

## SAKLAMA VE İMHA SÜRELERİ

Saklama süreleri sonra eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Veri Sorumlusu kontrolünde Sistem Yöneticisi tarafından yerine getirilir.

Süreç bazında saklama ve imha süreleri tablosu aşağıda belirtilmiştir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Sunucu Log Kayıt Takip Sistemleri	2 Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Aktivasyonu Tamamlanmamış Üyelikler	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Silinmesi Talep Edilmiş Üyelikler	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarışmaların Fotoğraflarının Orjinal Dosyaları	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarışmaların Fotoğraflarının Büyük Boyuttaki Dosyaları	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarışmaların Ödül Almış Olan Fotoğraflarının Büyük Boyuttaki Dosyaları	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş	90 Gün	Saklama süresinin bitimini takip

Yarıřmaların Ödöl Almış Olan Fotoğraflarının Küçük Boyuttaki Dosyaları		eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarıřmaların Katılımcı Listesi	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Evrak ile Katılım Sağlanmış ve Sonuçları İlan Edilmiş Yarıřmalara Ait Kayıt Formları ve Diğer Yazılı Evraklar	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarıřmalardan Arşive Aktarılmış Fotoğrafların Büyük Boyuttaki Dosyaları	5 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarıřmalardan Arşive Aktarılmış Fotoğraflarının Küçük Boyuttaki Dosyaları	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sonuçları İlan Edilmiş Yarıřmaların Anonimleştirilmiş Katılımcı Listeleri	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Yarıřma Sistemine Üye Olanların Destek Amaçlı Gönderdiği Epostalar	90 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Dava Sonucu Kişisel Verilerinin Silinmesine Karar Verilen Üye Bilgileri	30 Gün	Kararı takiben gerekli prosedürler tamamlandığında
TF SF YK Kararınca Kişisel Verilerinin Silinmesine Karar Verilen Üye Bilgileri	30 Gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

## PERİYODİK İMHA SÜRESİ

TF SF YK kararınca periyodik imha süresi 3 ay olarak belirlenmiştir. Buna göre her yıl Mart, Haziran, Eylül ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

## POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kağıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kağıt nüshası TF SF'de saklanır.

## POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça YK tarafından gözden geçirilir ve Kurul tarafından güncelleme yapıldıysa gerekli olan bölümler tekrar ele alınır ve bir sonraki maddeye göre yürürlüğe girer.

## POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, YK tarafından kabul edildiğinde imzalanarak yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına YK tarafından karar verilmesi halinde, Politika'nın ıslak imzalı nüshaları gerekçeli karar ile birlikte TFSF tarafından iptal edilerek ve en az 5 yıl süre ile saklanır.