

01.01.2020



KVKK

**FİSTAŞ
A.Ş**

**KVKK KİŞİSEL VERİ SAKLAMA VE İMHA
POLİTİKASI**

İçindekiler

1. GİRİŞ.....	3
1.1 Amaç.....	3
1.2 Kapsam	3
2. SORUMLULUK VE GÖREV DAĞILIMLARI.....	3
3. KAYIT ORTAMLARI	4
4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR.....	4
4.1 Saklamaya İlişkin Açıklamalar.....	4
4.1.1 Saklamayı Gerektiren Hukuki Sebepler.....	4
4.1.2 Saklamayı Gerektiren İşleme Amaçları	5
4.2 İmhayı Gerektiren Sebepler.....	5
5. TEKNİK VE İDARİ TEDBİRLER.....	5
5.1 Teknik Tedbirler	5
5.2 İdari Tedbirler	6
6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	6
6.1 Kişisel Verilerin Silinmesi.....	7
6.2 Kişisel Verilerin Yok Edilmesi	7
6.3 Kişisel Verilerin Anonim Hale Getirilmesi	7
7. SAKLAMA VE İMHA SÜRELERİ.....	8
8. PERİYODİK İMHA SÜRESİ	8
9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI	8
10. POLİTİKA'NIN GÜNCELLENME PERİYODU	8
11. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI	8

1. GİRİŞ

1.1 Amaç

FİSTAŞ Fantezi İplik San. Ve Tic A.Ş ("FİSTAŞ" ya da "Şirket"), olarak kişisel verilerin korunması konusuna azami dikkat ve özen gösteriyor ve tüm faaliyetlerimizde kişisel verilerin hukuka uygun olarak korunmasını gözetiyoruz. Tarafımızca hukuka uygun bir biçimde yürütülen kişisel veri işleme faaliyetlerine ilişkin gerekli tüm idari ve teknik tedbirleri alıyoruz.

Bu politika saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

FİSTAŞ; Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Şirketin sahip olduğu ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm bölümleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasıyla sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

FİSTAŞ bünyesinde Kişisel Verilerin Korunması ve İşlenmesi Politikası ve bu Politika 'ya bağlı ve ilişkili diğer politikaları yönetmek üzere Şirket üst yönetiminin kararı gereğince "Kişisel Verileri Koruma Kurulu" oluşturulmuştur.

Kurul aşağıda unvanı, iş birimi ve görev tanımı bulunan birimlerden oluşmakta olup, Kurulun Kişisel verilerin saklama ve imha süreçlerinde görevleri genel olarak Tablo 1'de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

Birim/Ünvan	Görev Tanımı
Kurul Başkanı MALİ İŞLER MÜDÜRÜ	Kurulun toplanması, politikaların uygulanması ve yürütülmesi, sekreteryaya hizmetlerinin gerçekleştirilmesi ve sürece ilişkin Yönetim Kurulunun Bilgilendirilmesi, Kişisel Verilerin Korunması Kurulu ile ilişkilerin takibi, Kurul Kararlarının takibi, uygulanması ve süreçlerin yönetimi. Şirketin Kurul nezdindeki temsili.
BİLGİ İŞLEM SORUMLUSU	Bilgi işlem sistemlerinin oluşturulması, takibi, uygulanması, imha ve anonim hale getirilmesi, yurt içinde ve yurt dışına aktarılması için gerekli mekanizmaları oluşturması, verilerin güvenliğinin sağlanması, veri güvenliği sağlayan sistemler önermesi, uygulaması.
İNSAN KAYNAKLARI SORUMLUSU	İnsan Kaynakları Sorumlusu, FİSTAŞ insan kaynakları işlerinin yürütülmesi, planlanması, görevlerine uygun olarak Politika'ların yürütülmesinden ve kişisel verileri uygun şekilde korunmasından sorumludur.
KALİTE GÜVENCE SORUMLUSU	Politika'ların hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.

3. KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından Tablo 2’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, 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 (Masaüstü, dizüstü) ✓ Mobil cihazlar (telefon, tablet vb.) ✓ Optik diskler (CD, DVD vb.) ✓ Çıkarılabilir bellekler (USB, Hafıza Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi	✓ Kağıt ✓ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ✓ Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunan üçüncü kişilerin, Şirketin veya şirkete bağlı firma çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 Saklamaya İlişkin Açıklamalar

Kanununun 3 üncü maddesinde *kişisel verilerin işlenmesi* kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin *işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi* gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise *kişisel verilerin işleme şartları* sayılmıştır.

Buna göre, Şirketimiz faaliyetleri çerçevesinde kişisel veriler, *ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.*

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Şirket, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir.

Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4857 sayılı İş Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek.
- Şirket iletişimi sağlamak.
- Şirket güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- İletişim Faaliyetlerinin Yürütülmesi (Çağrı merkezi süreçlerini yönetmek)
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.
- Yönetim Faaliyetlerinin Yürütülmesi

4.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette 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,

durumlarında, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

5. 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 Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirket tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Veri kaybı önleme yazılımları kullanılmaktadır.

5.2 İdari Tedbirler

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

- Şirket içerisinde kişisel verilerin korunmasından sorumlu olacak ve ilgili kuralları gözetecek veri sorumlusu temsilcisi ve iribat kişisi seçilmiştir.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği sadece erişmesi gerekli personel ile sınırlandırılmaktadır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a Kurul'un internet sitesinde yer alan formla bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlanmaktadır.
- Çalışanların 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, 4857 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Şirket Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmaktadır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderilir.
- Kişisel verilerin korunmasına yönelik personel ile gizlilik hükümleri içeren taahhütname imzalanmıştır.
- Personele zimmetlenen ve kişisel veri işlenen laptop, masaüstü bilgisayar veya akıllı telefon gibi cihazlar sadece personele ve yetkili birimlere bildirilen şifre ile teslim edilmekte ve şifrenin üçüncü kişilerce bilinmesi halinde değiştirilmesi konusunda gerekli bilgilendirmeler yapılmaktadır.
- Personellerin dosya transferi de dahil olmak üzere üçüncü bulut ve dosya transfer sistemlerine erişimi engellenmiştir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun

olarak aşağıda belirtilen tekniklerle imha edilir.

6.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz 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, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Şirket tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemez şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona 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 üzerindeki veriler okunamaz hale getirilir.

6.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse 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 kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Şirket 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;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Kalite Bölümü tarafından güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi BİLGİ İŞLEM Bölümü tarafından yerine getirilir.

FİSTAŞ tarafından Kanun ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerin saklama ve imha sürelerinin aşağıdaki esaslar çerçevesinde belirlenmektedir;

- a) İlgili mevzuatta veya Kurul kararı ile ilgili kişisel verinin ne kadar süre ile saklanacağı düzenlenmiş ise bu süreye uyulur.
- b) Mevzuatta veya Kurul kararı ile ilgili kişisel verinin ne kadar süre ile saklanacağı düzenlenmemiş ise, yukarıda belirtilen ilkeler dikkate alınarak kişisel verinin saklanma amacı ile uyumlu ve sınırlı bir süre belirlenir. Buna göre, personel özlük dosyanızda veya işveren-işçi ilişkisi nedeniyle işlenen kişisel verileriniz iş sözleşmeniz süresince ve iş sözleşmesinin sona ermesi üzerine sona erme tarihinden itibaren ilgili zamanaşımı uyarınca **5 (beş)** veya **10 (on)** yıl boyunca, sağlık verileri ise mevzuat uyarınca **15 (onbeş)** yıl boyunca saklanacaktır. Mevzuat değişikliği halinde mevzuat değişikliğine uygun olarak bu süre güncellenebilecektir.

Saklama süresi dolan ve imha süresi gelen kişisel veriler, **6 aylık** aralıklarla periyodik olarak gerçekleştirilen imha işlemleri sırasında Politika'da belirtilen usullere göre imha edilir ve tüm işlemler kayıt altına alınarak en az **3 yıl** süreyle saklanır.

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini **6 ay** olarak belirlemiştir. Buna göre, Şirket her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Kalite Bölümü tarafından saklanır.

10. POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

11. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Kalite Bölümü tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az **5 yıl** süre ile Kalite Bölümü tarafından saklanır.

Ek-1 Kısaltmalar ve Tanımlar

Alıcı Grubu	:	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	:	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Çalışan	:	FİSTAŞ personeli.
EBYS	:	Elektronik Belge Yönetim Sistemi
Elektronik Ortam	:	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	:	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Hizmet Sağlayıcı	:	FİSTAŞ ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	:	Kişisel verisi işlenen gerçek kişi.
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 kişiler.
İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	:	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 Veri İşleme Envanteri	:	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri 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 envanter.
Kişisel Verilerin İşlenmesi	:	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul	:	Kişisel Verileri Koruma Kurulu
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.
Periyodik İmha	:	Kanunda yer alan kişisel verilerin işleme 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.
Politika	:	Kişisel Verileri Saklama ve İmha Politikası
Veri İşleyen	:	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Veri Sorumluları Sicil Bilgi Sistemi	:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	:	Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	:	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.