FİNSO FİNANSAL TEKNOLOJİ ÇÖZÜMLERİ A.Ş.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

KVK-05-02-02

İÇİNDEKİLER

1 GİRİŞ

1.1 Amaç

Bu politikanın amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri dosyalama sisteminin parçası olmak kaydıyla otomatik olmayan yollarla veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla Kontrolör (Veri Sorumlusu) tarafından işlenen kişisel verilerin saklanması silinmesi, yok edilmesi veya anonim hale getirilme süreçlerine ilişkin usul ve esasları belirlemektir.

1.2 Hukuki Dayanak

Bu politika; 6698 sayılı Kanunun 7. maddesinin üçüncü fıkrası ile 22. maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği"ne uygun olarak hazırlanmıştır.

1.3 Veri Sorumlusu Dayanak

Veri Sorumlusu; Kişisel veri işleme envanterine uygun olarak bu kişisel veri saklama ve imha politikasını hazırlamıştır.

1.4 Politikanın Kapsamı

Bu Politika, Finso Finansal Teknoloji Çözümleri Anonim Şirketi'nin Veri Sorumlusu olarak aşağıdaki hususlara ilişkin bilgilendirmesini kapsamaktadır:

1.4.1 Politikanın hazırlanma amacını ve dayanak mevzuat hükümlerini, Veri Sorumlusu içi uygulama prosedürleri

1.4.2 Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimleri ve tanımlarını

1.4.3 Kişisel verilerin saklanmasına ilişkin amaçları ve hukuki sebeplerini

1.4.4 Kişisel Verilerin kaydedildiği her türlü kayıt ortamlarını

1.4.5 Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaları

1.4.6 Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için Veri Sorumlusu tarafından alınmış teknik ve idari tedbirleri

1.4.7 Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirleri

1.4.8 Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımları

1.4.9 Saklama ve imha sürelerini gösteren tablo

1.4.10 Periyodik imha sürelerine ve imha yöntemleri

1.4.11 Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe İlişkin bilgileri

2 TANIMLAR

2.1 **Alıcı Grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

2.2 **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 kişileridir

2.3 **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

2.4 **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 ifade eder.

2.5 **Elektronik Ortam:** Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.

2.6 **Elektronik Olmayan Ortam:** Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.

2.7 **Hizmet Sağlayıcı:** Veri Sorumlusu ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

2.8 **Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanterdir.

2.9 **Kişisel Veri Saklama ve İmha Politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

2.10 **Periyodik İmha:** 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 ifade eder.

2.11 **Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.

2.12 **Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

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

2.14 **Kişisel Verilerin Silinmesi:** Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

2.15 **Kişisel Verilerin Yok Edilmesi**: Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

2.16 **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, alıcı veya alıcı grupları tarafından geri döndürme ve 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.

2.17 **İlgili Kişi:** Kişisel verisi işlenen gerçek kişiyi ifade eder.

2.18 **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

2.19 **Kişisel Veri Koruma Komisyonu:** Veri Sorumlusu içerisinde kurulmuş ve KVKK süreçlerinde yer alan komisyonu ("KVKK Komisyonu") ifade eder.

3 GÖREV DAĞILIMI

Veri Sorumlusu, tüm birimleri 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 saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama Süreçlerinde Yer alan Birimler ve Görev Dağılımı

Unvan	Birim	Görev
İnsan Kaynakları Müdürü	İnsan Kaynakları	Çalışanlar ve çalışan adayları ile ilgili süreçlerden, bu süreçlerde toplanan verilerin yönetimi ve imha süreçlerinin KVKK'ya ve işbu politikaya uyumundan sorumludur.
Bilgi İşlem Birimi Yöneticisi	Bilgi İşlem Birimi	Şirketin tüm Bilgi İşlem süreçlerinin yönetimi ve imha süreçlerinin KVKK'ya ve işbu politikaya uyumundan sorumludur.
Mali İşler Müdürü	Finans Birimleri, İnsan Kaynakları, Satın alma	Finans ve Muhasebe süreçlerinden, bu süreçlerde toplanan verilerin yönetimi ve imha süreçlerinin KVKK'ya ve işbu politikaya uyumundan sorumludur.
Pazarlama Müdürü	Pazarlama Birimi	Pazarlama süreçlerinden, bu süreçlerde toplanan kişisel verilerin yönetimi ve imha süreçlerinin KVKK'ya ve işbu politikaya uyumundan sorumludur.

Genel Müdürlük	Genel Müdür, Genel Müdür Yardımcısı,	Bütün birimlerin KVKK'ya uyumlu hareket ettiği ve KVKK kapsamında gerekli imha süreçlerini yerine getirdiğinin takibinden sorumludur.
Teknik Birim Müdürü	Teknik Personel, Bilgi İşlem Birimi	Bilgi Güvenliği süreçlerinin takibi, Kişisel Verilerin Elektronik ortamlarda saklanması, Personelin erişim yetkilerinin kontrolü, prosedürlerin Personele duyurulması, zimmet süreçlerinin takibi
Hukuk Birimi	Hukuk Müşavirliği, Hukuk Departmanı, Avukatlar	Sözleşme süreçlerinde kişisel veri aktarımlarının tespiti, uygun aktarım sözleşmeleri ve protokollerin imzalanmasının sağlanması, personel gizlilik prosedür ve taahhütnamelerinin hazırlanması ve takibi, hukuki süreçlere ilişkin toplanan verilerin KVKK'ya uyumundan ve imhasından sorumludur.
Kişisel Verilerin Korunması Komisyonu		Tüm birimlerin işlediği kişisel veri süreçlerinin yönetimi ve takibi, işbu politikaya uygun hareket edildiğinin takibinden sorumludur.

4 KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI İLE DÜZENLENEN KAYIT ORTAMLARI

4.1 Kâğıt Ortamlar:

- Kâğıt
- Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)
- Yazılı, basılı, görsel ortamlar

4.2 Elektronik Ortamlar:

- Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)
- Yazılımlar
- 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.)
- Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
- Yazıcı, tarayıcı, fotokopi makinesi

5 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

5.1 6698 sayılı Kişisel Verilerin Korunması Kanunu

5.2 6098 sayılı Türk Borçlar Kanunu

5.3 4734 sayılı Kamu İhale Kanunu

5.4 657 sayılı Devlet Memurları Kanunu

5.5 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

5.6 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar

5.7 Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

5.8 5018 sayılı Kamu Mali Yönetimi Kanunu

5.9 6331 sayılı İş Sağlığı ve Güvenliği Kanunu

5.10 4982 Sayılı Bilgi Edinme Kanunu

5.11 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun

5.12 4857 sayılı İş Kanunu

5.13 2547 sayılı Yükseköğretim Kanunu

5.14 5434 sayılı Emekli Sağlığı Kanunu

5.15 2828 sayılı Sosyal Hizmetler Kanunu

5.16 İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik

5.17 Arşiv Hizmetleri Hakkında Yönetmelik

5.18 Kişisel Sağlık Verileri Hakkında Yönetmelik

5.19 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları hakkında Kanun

5.20 Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

6 SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

6.1 Acil Durum Yönetimi Süreçlerinin Yürütülmesi

6.2 Bilgi Güvenliği Süreçlerinin Yürütülmesi

6.3 Çalışan Adayı/Stajyer/Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi

6.4 Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi

6.5 Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi

6.6 Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi

6.7 Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi

6.8 Denetim/Etik Faaliyetlerinin Yürütülmesi

6.9 Eğitim Faaliyetlerinin Yürütülmesi

6.10 Erişim Yetkilerinin Yürütülmesi

6.11 Faaliyetlerin Mevzuata Uygun Yürütülmesi

6.12 Finans ve Muhasebe İşlerinin Yürütülmesi

6.13 Firma/Ürün/Hizmetlere Bağlılık Süreçlerinin Yürütülmesi

6.14 Fiziksel Mekân Güvenliğinin Temini

6.15 Görevlendirme Süreçlerinin Yürütülmesi

6.16 Hukuk İşlerinin Takibi ve Yürütülmesi

6.17 İç Denetim/ Soruşturma/İstihbarat Faaliyetlerinin Yürütülmesi

6.18 İletişim Faaliyetlerinin Yürütülmesi

6.19 İnsan Kaynakları Süreçlerinin Planlanması

6.20 İş Faaliyetlerinin Yürütülmesi/Denetimi

6.21 İş Sağlığı/Güvenliği Faaliyetlerinin Yürütülmesi

6.22 İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması ve Değerlendirilmesi

6.23 İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi

6.24 Lojistik Faaliyetlerinin Yürütülmesi

6.25 Mal/Hizmet Satın Alım Süreçlerinin Yürütülmesi

6.26 Mal/Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi

6.27 Mal/Hizmet Satış Süreçlerinin Yürütülmesi

6.28 Mal/Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi

6.29 Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi

6.30 Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi

6.31 Organizasyon ve Etkinlik Yönetimi

6.32 Pazarlama Analiz Çalışmalarının Yürütülmesi

6.33 Performans Değerlendirme Süreçlerinin Yürütülmesi

6.34 Reklam/Kampanya/Promosyon Süreçlerinin Yürütülmesi

6.35 Risk Yönetimi Süreçlerinin Yürütülmesi

6.36 Saklama ve Arşiv Faaliyetlerinin Yürütülmesi

6.37 Sosyal Sorumluluk ve Sivil Toplum Aktivitelerinin Yürütülmesi

6.38 Sözleşme Süreçlerinin Yürütülmesi

6.39 Sponsorluk Faaliyetlerinin Yürütülmesi

6.40 Stratejik Planlama Faaliyetlerinin Yürütülmesi

6.41 Talep/Şikayetlerin Takibi

6.42 Taşınır Mal ve Kaynakların Güvenliğinin Temini

6.43 Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi

6.44 Ücret Politikasının Yürütülmesi

6.45 Ürün/Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi

6.46 Veri Sorumlusu Operasyonlarının Güvenliğinin Temini

6.47 Yabancı Personel Çalışma ve Oturma İzni İşlemleri

6.48 Yatırım Süreçlerinin Yürütülmesi

6.49 Yetenek/Kariyer Gelişimi Faaliyetlerinin Yürütülmesi

6.50 Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi

6.51 Yönetim Faaliyetlerinin Yürütülmesi

6.52 Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

7 İMHAYI GEREKTİREN SEBEPLER

7.1 Kişisel veriler; İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

7.2 İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

7.3 Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,

7.4 Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,

7.5 Kurumun, 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;

7.6 Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,

7.7 Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, durumlarında,

7.8 Veri Sorumlusu tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da resen silinir, yok edilir veya anonim hale getirilir.

8 KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

8.1 Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

8.2 Ağ yoluyla veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

8.3 Anahtar yönetimi uygulanmaktadır.

8.4 Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

8.5 Çalışanlar için yetki matrisi oluşturulmuştur.

8.6 Erişim logları düzenli olarak tutulmaktadır.

8.7 Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

8.8 Gerektiğinde veri maskeleme yöntemi uygulanmaktadır.

8.9 Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

8.10 Kişisel veri güvenliğinin takibi yapılmaktadır.

8.11 Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

8.12 Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.

8.13 Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

8.14 Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

8.15 Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

8.16 Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

8.17 Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.

8.18 Mevcut risk ve tehditler belirlenmiştir.

8.19 Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

8.20 Özel nitelikli kişisel veriler için güvenli şifreleme/kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

8.21 Saldırı tespit ve önleme sistemleri kullanılmaktadır.

8.22 Sızma testi uygulanmaktadır.

8.23 Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

8.24 Şifreleme yapılmaktadır.

8.25 Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklara denetimi sağlanmaktadır.

8.26 Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

8.27 Veri kaybı önleme yazılımları kullanılmaktadır.

8.28 Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

8.29 Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

8.30 Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

8.31 Gizlilik taahhütnameleri yapılmaktadır.

8.32 İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

8.33 Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

8.34 Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

8.35 Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

8.36 Kişisel veriler mümkün olduğunca azaltılmaktadır.

8.37 Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

8.38 Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler mevcuttur.

9 KİŞİSEL VERİLERİN SİLİNMESİ TEKNİKLERİ

9.1 **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.

9.2 **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.

9.3 **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.

9.4 **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.

10 KİŞİSEL VERİLERİN YOK EDİLMESİ TEKNİKLERİ

10.1 **Fiziksel Ortamda Yer Alan Kişisel Veriler:** Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

10.2 **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.

11 KİŞİSEL VERİLERİ ANONİM HALE GETİRME TEKNİKLERİ

11.1 Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Şirket, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

11.2 KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.

11.3 **Maskeleme (Masking):** Veri maskeleme, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, T.C. Kimlik No, ad, soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkânsız hale geldiği bir veri setine dönüştürülmesi.

11.4 **Toplulaştırma (Aggregation):** Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.

11.5 **Veri Türetme (Data Derivation):** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehrin belirtilmesi.

11.6 **Veri Karma (Data Shuffling, Permutation):** Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

11.7 **Değişkenleri Çıkarma:** Kişisel verileri gerçek kişi ile ilişkilendirmeye yarayabilecek verilerin bir veya birden çok bölümünün çıkarılması

12 KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

12.1 İmha süreçleri, ilgili kişinin talebi, Kişisel Verileri Koruma Kurulu kararı veya periyodik imha süresinin dolması ile yapılır.

12.1.1 **Periyodik İmha:** Veri Sorumlusu bünyesinde belirlenen periyodik imha süresi her yılın Aralık ve Haziran ayıdır.

12.1.2 **İlgili Kişinin Talebi Üzerine İmha:** İlgili kişinin talebi üzerine imha, talebin uygun görülmesi halinde gecikmeksizin ve her halükârda talebin tebliğinden itibaren 30 gün içinde yerine getirilir ve aynı süre içinde ilgili kişiye cevap verilir. İlgili kişinin başvuru ve talep süreçleri "ilgili Kişi Başvuru Prosedürü"nde belirtilmiştir.

12.1.3 **Kurul Kararı Üzerine İmha:** Kişisel Verileri Koruma Kurulu tarafından kişisel verinin imha edilmesine ilişkin bir karar verilmesi durumunda kararın tebliğinden itibaren gecikmeksizin ve her halükârda 30 gün içinde yerine getirilir ve Kurul'a aynı süre içerisinde cevap verilir.

12.2 Aşağıda yer alan tabloda Veri Sorumlusu içerisinde işlenen veri kategorileri, kanuni ve işleme amacının gerektirdiği işleme ve saklama süreleri ile imha periyodu yer almaktadır.

12.3 Bu tabloda yer almayan ancak Veri Sorumlusu'nun süreçlerinde yer alan kişisel verilerin imhasına veya tablonun güncellenerek eklenmesine; Kurul Kararları ve Kişisel verilerin işleme amacı ile orantılı olmak kaydıyla Kişisel Verilerin Korunması Komisyonu karar vermeye yetkilidir. KVKK Komisyonu vereceği kararda, sürenin KVKK'nın 4. maddesindeki ilkelere uygun olmasını sağlar.

12.4 Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

Tablo 2: Saklama ve İmha Sürelerini Gösteren Tablo

No	Veri Konusu Kişi Grubu	Süreç	Veri Saklama Süresi	İmha Zamanı
1	Çalışan Adayı	Çalışan Adayı Başvuru ve Değerlendirme süreçleri (Özgeçmiş, fotoğraf, iş başvurusu için alınan tüm belgeler)	2 Yıl	İlk Başvurunun yapıldığı tarihten itibaren; işe alınmamış olması şartıyla, saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
2	Çalışan	Özlük Dosyası Süreçleri (iş sözleşmesi, kimlik, iletişim,	15 yıl	İşten Ayrıldığı tarihten itibaren saklama süresinin

		ehliyet, hukuki işlem, disiplin süreçleri, özlük hakları süreçleri, özgeçmiş, adli sicil kaydı ve özlük dosyasındaki diğer belgeler, görsel işitsel kayıtlar, zimmet işlemleri)		geçmesinin ardından ilk periyodik imha süresinde
3	Çalışan	Araç takip sistemi ile edinilen lokasyon bilgisine ilişkin süreçler	2 Yıl	Veri işlemenin yapıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
4	Çalışan	Çalışan ücret ve diğer özlük haklarına ilişkin muhasebe, ödeme ve mali süreçleri	15 yıl	İşten Ayrıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
5	Çalışan	Çalışana tesis edilen e-posta, kurumsal hesap ve cihazlardaki işlem ve içerik kayıtları süreçleri	15 yıl	İşten Ayrıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
6	Çalışan	İşverenin sağlık ve güvenlik kayıtları, kişisel sağlık dosyası ve onaylı deftere ilişkin süreçleri	15 yıl	İşten ayrılma tarihinden itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
7	Çalışan	Kurumsal cihaz, e-posta, telefon kullanım içerikleri ve süreçleri	15 yıl	İşten ayrılma tarihinden itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
8	Çalışan	İşyeri giriş çıkış puantaj kayıtları	15 yıl	İşten ayrılma tarihinden itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
9	Anlaşmalı Mağazaların Satış Görevlileri	Satış görevlilerinin mağazayı temsilen yapmış oldukları satış işlemleri, Satıcı Portalı Uygulaması ve SalesPro Mobil	10 yıl	Satış yetkisinin kaldırılmasının, her halükârda yaptığı son işlemin

		Uygulaması'ndaki kişisel verileri		ardından ilk periyodik imha süresinde
10	Çalışan Ziyaretçi Web Sitesi Ziyaretçisi	İşlem Güvenliği Süreçleri (İnternet kullanımı IP log kayıtları, kullanıcı log kayıtları, IP adresi)	2 yıl	Kayıt tarihinden itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
11	Çalışan Ziyaretçi Veri Sorumlusu Lokasyonlarında Bulunan Herkes	Fiziksel mekân güvenliği kamera kayıt süreçleri	45 gün	Kaydın yapılmasının ardından saklama süresinin geçmesi ile
12	Ziyaretçi Veri Sorumlusu Lokasyonlarında Bulunan Herkes	Fiziksel mekân güvenliği giriş çıkış ziyaretçi kayıt süreçleri	5 yıl	Kayıt tarihinden itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
13	Tüm İlgili Kişi Grupları (Çalışanlar Ayrı Bir Kategoride Belirtilmiştir)	Hukuki işlem süreçleri	10 yıl	Hukuki işlemin yapıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
14	Tedarikçi, İş Ortakları ve Müşteriler	Müşteri işlem bilgileri (çek, senet, fatura, talep, şikâyet)	10 yıl	İşlemin yapıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
15	Tedarikçi, İş Ortakları ve Müşteriler	Çağrı Merkezi kayıt süreçleri	10 yıl	İşlemin yapıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
16	Tedarikçi, İş Ortakları ve Müşteriler ve Sözleşme Yapılan Kişiler (Çalışanlar Ayrı	Sözleşme ve Ticari işlem süreçleri (Yazılı veya yazılı olmayan sözleşme ve ekleri, imza sirküleri, tarafların iletişim bilgileri,	10 yıl	Sözleşmenin ve aynı zamanda hukuki ve fiili ticari ilişkinin sona ermesinin ardından saklama süresinin sona ermesini izleyen ilk periyodik imha süresinde

	Bir Kategoride Belirtilmiştir)	sözleşmeye ilişkin teslimat ve sevkiyat belgeleri)		
17	Tüm İlgili Kişi Grupları (Çalışanlar Ayrı Bir Kategoride Belirtilmiştir)	Muhasebe ve finans süreçleri (yapılan ve alınan ödemeler, faturalar, mali belgeler, slipler, ekstreler)	10 yıl	İlişki sözleşmeye dayalı ise, sözleşmenin ve aynı zamanda hukuki ve fiili ticari ilişkinin sona ermesinden itibaren, ilişki sözleşmeye dayalı değil ise işlem tarihinden itibaren saklama süresinin sona ermesini izleyen ilk periyodik imha süresinde
18	Ziyaretçiler	İnternet sitesi çerez bilgileri	İnternet sitemizde belirtilen sürelerde saklanmaktadır.	İnternet sitemizde belirtilen süreler sonunda imha edilmektedir.
19	Bankalar ve Finans Kuruluşları	Müşterilere sunulan kredi türü ve miktarına ilişkin tekliflerin ve işlemlerin kayıtları	10 yıl	Teklifin yapıldığı ve/veya işlemin tamamlandığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde
20	Müşteriler	Müşterilere ilişkin kişisel veri ve işlem kayıtları, Müşterilerin yüklediği dosyalar, Müşterilerin elektronik ticaret siteleri ve fiziksel mağazalar aracılığı ile oluşturduğu alışveriş paketleri, ödemeleri ve durumlarına ilişkin kayıtlar, Müşterilerin kredi başvurusu yaptığı bankalar, başvurduğu kredi türleri, vadeleri, miktarları ve başvuru durumlarına ilişkin kayıtlar	10 yıl	İşlemin yapıldığı tarihten itibaren saklama süresinin geçmesinin ardından ilk periyodik imha süresinde

13 POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır.

14 POLİTİKANIN GÜNCELLEME PERİYODU

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

15 YÜRÜRLÜK

Politika, çalışanlara duyurulması ve Veri Sorumlusu'nun internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

16 VERİ SORUMLUSU BİLGİLERİ

Veri Sorumlusu Unvanı	:	Finso Finansal Teknoloji Çözümleri Anonim Şirketi
Mersis Numarası	:	0388143442200001
E-Posta Adresi	:	info@finso.com.tr
Kayıtlı Elektronik Posta Adresi	:	finsoteknoloji@fhs05.kep.tr
Fiziki Posta Adresi	:	Küçükbakkalköy Mahallesi Kayışdağı Caddesi Allianz Plaza Sitesi No: 1 İç Kapı No: 108 Kat:29 Ataşehir-İstanbul

EKLER

EK-1: İLGİLİ KİŞİNİN TALEBİ ÜZERİNE İMHA TUTANAĞI

İLGİLİ KİŞİ TALEBİ ÜZERİNE DOKÜMAN İMHA TUTANAĞI

Aşağıda listelenmiş olan kişisel ve özel nitelikli kişisel veriler içeren dokümanlar, **Veri Sorumlusu sıfatıyla** Finso Finansal Teknoloji Çözümleri Anonim Şirketi tarafından; 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat uyarınca, ilgili kişinin talebi doğrultusunda kişisel verilerin imha edilmesi gerçekleştirilmiştir. İlgili kişinin talebi doğrultusunda imha edilen dokümanlarla ilgili kullanılan imha tekniği ve tarihi, imha edilen dokümanların ve dosyaların içeriği aşağıdaki tablolarda detaylı olarak belirtilmiştir.

İlgili Kişi	
İlgili Kişi İmha Talep Tarihi	
İmha Tekniği	
İlgili Kişiye İmha Evrakı Tebliğ Tarihi	
Dokümanlarda Bulunan Veri Kategorileri	(Kimlik, iletişim, finans, mesleki deneyim, görsel işitsel kayıtlar vb.)
Dokümanların Bulunduğu Ortam	(Fiziki ise özlük dosyası, sanal ise Google Drive/Cloud vb.)

İmha Edilen Doküman Listesi	
1.	**2.**
3.	**4.**
5.	**6.**
7.	**8.**
9.	**10.**
11.	**12.**
13.	**14.**
İMHA EDEN **Adı Soyadı / Pozisyon / İmza**	**İMHAYA TANIK OLAN** **Adı Soyadı / Pozisyon / İmza**

EK-2: PERİYODİK İMHA TUTANAĞI

PERİYODİK İMHA TUTANAĞI

Aşağıda listelenmiş olan kişisel ve özel nitelikli kişisel veriler içeren dokümanlar, **Veri Sorumlusu sıfatıyla** Finso Finansal Teknoloji Çözümleri Anonim Şirketi tarafından; 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat uyarınca, kişisel ve özel nitelikli kişisel veriler içeren dokümanların **Kişisel Veri Saklama ve İmha Politikası uyarınca saklama sürelerinin bitmesi nedeniyle** imha edilmesi gerçekleştirilmiştir. Yasal saklama sürelerinin bitmesi doğrultusunda imha edilen dokümanlarla ilgili kullanılan imha tekniği ve tarihi, imha edilen dokümanların ve dosyaların içeriği aşağıdaki tablolarda detaylı olarak belirtilmiştir.

Verileri imhaya Konu İlgili Kişi	
İmha Tarihi	
Kullanılan İmha Tekniği	
Dokümanlarda Bulunan Veri Kategorileri	(Kimlik, iletişim, finans, mesleki deneyim, görsel işitsel kayıtlar vb.)
Dokümanların Bulunduğu Ortam	(Fiziki ise özlük dosyası, sanal ise Google Drive/Cloud vb.)

İmha Edilen Doküman Listesi	
1.	**2.**
3.	**4.**
5.	**6.**
7.	**8.**
9.	**10.**
11.	**12.**
13.	**14.**
İMHA EDEN **Adı Soyadı / Pozisyon / İmza**	**İMHAYA TANIK OLAN** **Adı Soyadı / Pozisyon / İmza**