
	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırlandığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

İçindekiler

1. Amaç ve Dayanak	1
2. Kapsam	1
3. Tanımlar	1
4. Sorumluluk Ve Görev Dağılımları	2
5. Kayıt Ortamları	3
6. Saklama Ve İmha İlişkin Açıklamalar	3
6.1. Saklamaya İlişkin Açıklamalar	3
6.1.1. Saklamayı Gerektiren Hukuki Sebepler	3
6.1.2. Saklamayı Gerektiren İşleme Amaçları	3
6.2. İmhayı Gerektiren Sebepler	4
7. Teknik Ve İdari Tedbirler	4
7.1. Teknik Tedbirler	4
7.2. İdari Tedbirler	5
8. Kişisel Verileri İmha Teknikleri	5
8.1. Kişisel Verilerin Silinmesi	5
8.2. Kişisel Verilerin Yok Edilmesi	6
8.3. Kişisel Verilerin Anonim Hale Getirilmesi	6
9. Saklama Ve İmha Süreleri	6
10. Periyodik İmha Süresi	7
11. Politikanın Yayınlanması Ve Saklanması	7
12. Politikanın Güncellenme Periyodu	7
13. Politikanın Yürürlüğü Ve Yürürlükten Kaldırılması	7

Bu Politika metninde yer alan tüm içeriklerin, bireysel kullanım dışında izin alınmadan kısmen ya da tamamen kopyalanması, çoğaltılması, kullanılması, yayımlanması ve dağıtılması yasaktır. Bu yasağa uymayanlar hakkında 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca yasal işlem yapılacaktır. Eserin tüm hakları saklıdır.

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırladığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

1. Amaç ve Dayanak

İş bu Kişisel Verileri Saklama ve İmha Politikası (Politika), Safa Tarım A. Ş. de (Şirket) gerçekleştirilen saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek; çalışanların, çalışan adaylarının, hizmet sağlayıcılarının, tedarikçilerin, müşterilerin, ziyaretçilerin ve diğer üçüncü kişilerin kişisel verilerini; T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ve diğer ilgili mevzuata uygun olarak işlenmesi ve ilgili kişilerin haklarını etkin bir şekilde kullanması amacıyla hazırlanmıştır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, şirketimiz tarafından hazırlanmış olan Politikalara uygun olarak gerçekleştirilir.


İş bu politika Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5/1'inci maddesine dayanılarak hazırlanmıştır.

2. Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcılar, tedarikçiler, müşteriler, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamında olup şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

3. Tanımlar

Alıcı Grubu	Şirketimiz tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişiler
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme	Kişisel verinin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Çalışan	Safa Tarım A. Ş. personeli
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	Şirkete 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	Şirketimizin, iş süreçlerine bağlı olarak gerçekleştirilen kişisel verileri işleme faaliyetleri; kişisel verileri işleme amacı ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirilerek oluşturulan ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami saklama süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırılan 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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırladığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

	getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi
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 resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
Politika	Kişisel Verileri Saklama ve İmha Politikası
Kurul	Kişisel Verileri Koruma Kurulu
Veri İşleyen	Şirketin verdiği yetkiye dayanarak Şirket adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi (Şirket)
Veri Sorumluları Sicil Bilgisi	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


4. Sorumluluk Ve Görev Dağılımları

Şirketin tüm birimleri ve çalışanları, politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanmasında, birim çalışanlarının eğitimi ve farkındalığın artırılmasında, izlenmesi ve denetlenmesinde, kişisel verilerin hukuka aykırı şekilde işlenmesinin önlenmesinde, verilere erişimin önlenmesi ve hukuka uygun saklanmasının sağlanmasında kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik alınan teknik ve idari tedbirlerin uygulanmasında birimlere aktif destek verir.

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

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Genel Müdür	Tüm Müdürlükler	Çalışanların politikaya uygun hareket etmesinden sorumludur.
Bilgi Güvenliği Sistem Yöneticisi	Bilgi Güvenliği Birim Yetkilisi, Bilgi İşlem Elemanı	Politikanın yürütülmesi, ilgili ortamlarda yayınlanması, uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulması ve güncellenmesinden sorumludur.
İnsan Kaynakları Müdürü	İnsan Kaynakları Müdürlüğü	Politikanın hazırlanması, yürütülmesi ve güncellenmesinden sorumludur.
Kalite Güvence Müdürü Dış Ticaret Müdürü Satış Müdürü Mali İşler Müdürü Satınalma Müdürü Ürt. Ve Pln. Müdürü Proje Geliştirme Müdürü Proje Yürütme Müdürü Depo ve Sevk. Müdürü Tohum Müdürü	Kalite Güvence Müdürlüğü Dış Ticaret Müdürlüğü Satış Müdürlüğü Mali İşler Müdürlüğü Satınalma Müdürlüğü Ürt. Ve Pln. Müdürlüğü Ar-Ge Merk. Müdürlüğü Ar-Ge Merk. Müdürlüğü Depo ve Sevk. Müdürlüğü Tohum Müdürlüğü	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırladığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

5. Kayıt Ortamları

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
<ul style="list-style-type: none"> Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) 	<ul style="list-style-type: none"> Kağıt
<ul style="list-style-type: none"> Yazılımlar (ofis yazılımları, portal, 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.) Çıkartılabilir bellekler (USB, Hafıza Kart vb.) Yazıcı, tarayıcı, fotokopi makinesi 	<ul style="list-style-type: none"> Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) Yazılı, basılı, görsel ortamlar

6. Saklama Ve İmhaya İlişkin Açıklamalar

Şirket tarafından; çalışanlar, çalışan adayları, tedarikçiler, müşteriler, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

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

6.1. Saklamaya İlişkin Açıklamalar

Kanunun 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.*

6.1.1. Saklamayı Gerektiren Hukuki Sebepler

Şirketimizde, 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,
- 4734 sayılı Kamu İhale Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2547 sayılı Yükseköğretim Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

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

6.1.2 Saklamayı Gerektiren İşleme Amaçları

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

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırladığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

- Şirket güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

6.2 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,
- Kanununun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirketimiz tarafından kabul edilmesi,
- Şirketimizin, 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 şikâyetinde 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 resen silinir, yok edilir veya anonim hale getirilir.


7. Teknik Ve İdari Tedbirler

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 şirket tarafından teknik ve idari tedbirler alınır.

7.1. Teknik Tedbirler

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

- Sızma (Penetrasyon) testleri ile Şirketimiz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile şirketin aktif director üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirketimiz bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket 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.
- Şirketimiz, 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 Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırlanma Tarihi	01.07.2020
		Revizyon Tarihi/No	
		Geçerlilik Tarihi	Süresiz

- 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.
- 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 testleri düzenli olarak yapılmakta veya yaptırılmakta, test sonuçları kayıt altına alınmaktadır.
- 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. 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.

7.2. İdari Tedbirler

Kişisel verilerin işlenmesiyle ilgili Şirketimiz tarafından alınan idari tedbirler:

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

8. Kişisel Verileri İmha Teknikleri


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

8.1. 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 veriler, saklanmasını gerektiren sürenin sonunda sistem yöneticisi tarafından ilgili kullanıcıların erişime kapatılarak silinir.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel veriler, saklanmasını gerektiren sürenin sonunda, veritabanı yöneticisi hariç çalışanların (ilgili kullanıcıların) hiçbir şekilde erişemeyeceği ve tekrar kullanamayacağı hale getirilerek silinir.

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırlanma Tarihi	01.07.2020
		Revizyon Tarihi/No	
		Geçerlilik Tarihi	Süresiz

Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel veriler, saklanmasını gerektiren süre sonunda 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 uygulanabilir.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel veriler, saklanmasını gerektiren süre sonunda, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

8.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Şirketimiz tarafından Tablo-4'te belirtilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel veriler, saklanmasını gerektiren süre sonunda kâğıt kırma makinelerinde geri döndürülemez şekilde yok edilir.
Optik / Manyetik Ortamda Yer Alan Kişisel Veriler	Optik ve manyetik ortamda yer alan kişisel veriler, saklanmasını gerektiren süre sonunda eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel yollarla yok edilir.

8.3 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.

9. Saklama Ve İmha Süreleri

Şirketimiz 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.

Saklama süreleri sona eren kişisel veriler için resen silme, yok etme veya anonim hale getirme işlemi Bilgi Güvenliği Sistem Sorumlusu tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Yönetim Kurulu Kararları	30 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

	KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI	Doküman No	GP 28
		Hazırlandığı Tarih	01.07.2020
		Revizyon Tarih/No	
		Geçerlilik Tarihi	Süresiz

Ziyaretçi ve Toplantı	Etkinliğin sona ermesini takiben 2yıl	Saklama süresinin bitimini takip eden
Katılımcılarının Kaydı	Etkinliğin sona ermesini takiben 2 Yıl	ilk periyodik imha süresinde
Kamera Kayıtları	45 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

10. Periyodik İmha Süresi

Yönetmeliğin 11/2'inci maddesi gereğince Şirketimiz, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirketimizde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

11. Politikanın Yayınlanması Ve Saklanması

Politika, fiziksel ve elektronik olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Fiziksel ortamdaki nüshası da Bilgi Güvenliği Sistem Sorumlusu dosyasında saklanır.

12. Politikanın Güncellenme Periyodu

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

13. Politikanın Yürürlüğü Ve Yürürlükten Kaldırılması

Politika, Şirketin Genel Müdürün onayı ile yürürlüğe girmiş olur. Yürürlükten kaldırılmasına karar verilmesi halinde, Politikanın ıslak imzalı eski nüshaları Genel Müdür onayı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Bilgi Güvenliği Sistem Sorumlusu tarafından saklanır.