

SIRMAGRUP İÇECEK SAN VE TİCARET A.Ş. KİŞİSEL VERİ KORUMA VE İMHA POLİTİKASI

SIRMAGRUP İÇECEK SAN VE TİC A.Ş.
Küçükbakkalköy mahallesi Vedat Günyol Caddesi Defne sokak
No.3 Büyükhanlı Plaza Kat.11 Ataşehir İstanbul
Tel: 0216 544 27 00
Faks: 0216 340 58 79
E-posta: info@sirmagrup.com

İÇİNDEKİLER

1.GİRİŞ	2
2.AMAÇ VE KAPSAM	2
3.TANIMLAR	2
4.GENEL İLKELER	2
5.KİŞİSEL VERİLERİN İŞLENME ŞARTLARI	3
5.1.Özel Nitelikli Kişisel Verilerin İşlenme Koşulları	3
6.SIRMAGRUP TARAFINDAN İŞLENEN KİŞİSEL VERİLER	3
6.1.Şirket Bünyesinde İşlenen Kişisel Verilerin İşlenme Amaçları	3
6.2.Şirket Bünyesinde İşlenen Genel Nitelikli Kişisel Veriler	4
6.3.Özel Nitelikli Kişisel Veriler	5
7.KİŞİSEL VERİLERİN İŞLENME AMAÇLARI	5
8.KİŞİSEL VERİLERİN GÜVENLİĞİNİ SAĞLAMAK AMACIYLA ALINAN TEKNİK VE İDARİ TEDBİRLER	6
8.1.İdari Tedbirler	6
8.2.Teknik Tedbirler	6
8.3.Özel Nitelikli Kişisel Verilerin Korunması İçin Alınan Tedbirler	7
9.KİŞİSEL VERİLERİN SAKLANMA SÜRELERİ	8
10.KİŞİSEL VERİLERİN AKTARILMASI	8
11.KİŞİSEL VERİLERİN İMHASI VE ANONİMLEŞTİRİLMESİ	8
11.1.İmha Nedenleri	8
11.2.Kişisel Verilerin Silinmesi	8
11.3.Kişisel Verilerin Yok Edilmesi	8
11.4.Kişisel Verilerin Anonim Hale Getirilmesi	9
12.SAKLAMA VE İMHA SÜRELERİ	9
13.SAKLAMA VE İMHA SÜRELERİ	10
14.SORUMLULUK	10
15.İLETİŞİM	10

1.GİRİŞ

Kişilerin, özel hayatının gizliliğini sağlayabilmek için üçüncü kişilerin eline geçmesinde sakınca bulunan verilerinin hukuken korunması için, 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete'de yayınlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) yürürlüğe girmiştir. Şirketimiz de tüm kurumlar gibi bu kanuna tabi olup, yürütülen tüm iş süreçlerinde işlenen tüm veriler bu kapsamda değerlendirilerek kişisel veri olarak kabul edilmekte ve yasa gereği koruma altına alınmaktadır.

SIRMAGRUP, bu anlamda üstlendiği yasal yükümlülüklerin eksiksiz olarak yerine getirilmesi için yürürlüğe koyduğu yazılı politikaların uygulanması için azami özen göstermekte ve gerekli tüm idari ve teknik tedbirleri almaktadır.

2.AMAÇ ve KAPSAM

Bu politika ile hedeflenen amaç, SIRMAGRUP bünyesinde toplanan, işlenen, aktarılan kişisel verilerin korunması konusunda sahip olunan ilkeleri ve yapılan çalışmaları çalışanlarımıza ve kamuoyuna açıklamaktır.

Bu politika, çalışanlarımızın, şirket yöneticilerinin, ziyaretçilerin, çalışan adaylarımızın, ticari birliktelik içinde olduğumuz şirket çalışanlarının, müşterilerin, tüketicilerin, üçüncü kişilerin kanun kapsamında işlenen kişisel verileri için uygulanmaktadır.

3.TANIMLAR

Bu politikanın içeriğinde yer alan ve önem arz eden kavramlar aşağıdaki şekilde tanımlanmıştır.

Kanun; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,

Kişisel Veri; Kişiyi doğrudan veya dolaylı olarak tanımlamaya veya belirlemeye yarayan her türlü bilgiyi,

Veri İşleme; Kişisel veriler üzerinde gerçekleştirilen her türlü işlemi,

Veri Sahibi; Kişisel verinin ait olduğu gerçek kişiyi,

Veri Sorumlusu; Gerçek kişilerin kişisel verilerini toplayan, işleyen ve KVKK'na göre bir takım yükümlülüklerle donatılmış gerçek veya tüzel kişiyi (Sirmagrup),

Anonim Hale Getirme; Kişisel verinin, bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

ifade eder.

4.GENEL İLKELER

SIRMAGRUP nezdinde işlenen kişisel veriler, Kanun'un 4. Maddesi doğrultusunda, aşağıda yazılı ilkelere uygun biçimde işlenebilir:

*Verilerin işlenmesinde hukuka ve dürüstlük kurallarına uyulmalıdır.

*İşlenen veriler doğru ve gerektiğinde güncel olmalıdır.

*Veri işleme işlemleri, ancak belirli, açık ve meşru amaçlar için yapılmalıdır.

*Veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü biçimde işlenmelidir.

* Kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

5.KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

“Kişisel verinin işlenmesi kavramı”, Kanun’un 3.maddesinde tarif edilmiştir. Buan göre; “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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”, veri işleme olarak tarif edilmektedir.

Kişisel verilerin işlenmesinde, Kanun’un 5 ve 6. Maddelerinde sayılan koşullara uyulması gerekmektedir. Kural olarak kişisel verinin, ilgili kişinin açık rızası olmaksızın işlenmemesi esastır. Ancak Kanun’un 5.maddesi, bazı durumlarda veri sahibinin açık rızasına gerek duyulmaksızın kişisel verilerin işlenmesine izin vermektedir. Kişilerin açık rızasının alınmasına gerek duyulmaksızın verilerin işlenebileceği durumlar aşağıdaki gibidir:

- a) Kanunlarda açıkça öngörülmesi.
- b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- e) Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması.
- f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Şirketimiz bünyesinde toplanan kişisel veriler genellikle yasal ve sözleşmesel yükümlülüklerin yerine getirilmesi amacıyla işlenmektedir. Aşağıda, SIRMAGRUP bünyesinde genel olarak hangi tür kişisel verilerin işlendiğine ilişkin bilgiler ayrıntılarıyla yer almaktadır.

5.1.Özel Nitelikli Kişisel Verilerin İşlenme Koşulları

Özel nitelikli kişisel veriler, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle Kanun, diğer kişisel verilere göre farklı bir koruma sistemi benimsemiştir. Özel nitelikli kişisel veri, işlenme amacı ne olursa olsun, şirketimiz açısından her şekilde veri sahibinin açık rızasının alınmasını zorunlu kılmaktadır. Kanunda sınırlı sayma yolu ile belirlenen bu veriler; “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”nden ibarettir.

6.SIRMAGRUP TARAFINDAN İŞLENEN KİŞİSEL VERİLER

6.1.Şirket Bünyesinde İşlenen Kişisel Verilerin İşlenme Amaçları

SIRMAGRUP bünyesinde işlenen kişisel veriler, ilgili veri sahibi kategorisine göre aşağıdaki şekilde farklılık göstermektedir.

Çalışan Adayı Verileri: SIRMAGRUP, yürüttüğü insan kaynakları prosedürlerine uygun olarak, iş başvurusunda bulunan adayların kişisel verilerini, mülakat ve işe alım süreçlerinin tamamlanması, ileride doğabilecek yeniden değerlendirme olasılıkları sebebiyle işler. Çalışan adayı kişisel verileri bu kapsamda ileride değerlendirilebilir ise saklanır aksi halde imha edilir.

Çalışan Verileri: İş kanunu'nun 75.maddesi kapsamında, SIRMAGRUP çalışanlarının kişisel verileri, işverenin özlük dosyası hazırlama ve saklama yükümlülüğünün bir gereği olarak, iş sözleşmesinden ve iş mevzuatından kaynaklanan yükümlülüklerin yerine getirilmesi, şirket içi prosedürlerin uygulanması, iş sağlığı ve güvenliğinin sağlanması, şirket faaliyet alanına giren ticari faaliyetlerin yürütülmesi ve uygulanması amacıyla işlenmektedir.

Müşteri/Bayi/İş Ortağı Verileri: SIRMAGRUP'un ana faaliyet alanı, ambalajlı su ve maden suyu üretimi ve satışlarıdır. Faaliyet alanına giren konuların gereği gibi yapılması ve finansal yükümlülüklerin yerine getirilmesi amacıyla tedarikçilerimizin, bayilerimizin, müşterilerimizin ve iş ortaklarımızın kişisel verileri işlenmektedir.

Tüketici Verileri: Tüketicilere daha kaliteli hizmet sunulması, talep ve şikayet yönetimi, muhtemel ve/veya mevcut uyuşmazlıkların çözümü için tüketicilerimizin kişisel verileri işlenebilmektedir.

Ziyaretçi Verileri: SIRMAGRUP merkez ofis, fabrikalar ve depoları ziyaret eden kişilerin kişisel verileri, fiziki güvenlik protokollerinin bir gereği olarak işlenebilmektedir. Kimlik bilgilerinin yanısıra ziyaretçilerin görüntüleri kameralar aracılığı ile kaydedilmekte, kaydedilen görüntüler şifreli olarak güvenli ortamlarda saklanmakta ve maximum 40 gün sonunda imha edilmektedir. Kamera görüntüleri özel nitelikli kişisel veri kapsamına girdiğinden, ziyaretlerimiz bu konuda özel olarak aydınlatılmakta ve yalnızca bu konuya özel olarak açık rızaları alınmaktadır.

6.2.Şirket Bünyesinde İşlenen Genel Nitelikli Kişisel Veriler

Şirketimiz nezdinde işlenen kişisel veriler, ilgili kişilerden alınan açık rıza aracılığı ile veya Kanun'un 5.maddesi kapsamında açık rıza gerektirmeyen haller münasebeti ile işlenebilmektedir.

Şirket bünyesinde işlenen kişisel veriler kategorilerine göre şu şekilde listenebilir:

VERİ KATEGORİLERİ	AÇIKLAMA
Kimlik Bilgileri	ad-soyad, tc kimlik numarası, ses kayıtları, cinsiyet ve yaş.
İletişim Bilgileri	Telefon numarası, adres.
Özlük Bilgileri	giriş çıkış kayıtları, bakmakla yükümlü olunan kişilerin kimlik bilgileri, yıllık izin bilgileri, bordro.
Aile Bireyleri ve Yakınlık Bilgileri	Bakmakla yükümlü olunan kimselerin kimlik bilgileri.

Güvenlik Bilgileri	Şirket ofisi, deposu gibi fiziksel mekana girişte veya fiziksel mekanın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler.
Finansal Bilgiler	Banka hesap numarası, maaş bilgileri, bordrolar, vergi levhası.

6.3.Özel Nitelikli Kişisel Veriler

Şirketimiz nezdinde işlenen özel nitelikli kişisel veriler için mutlak surette Kanun'un 6.maddesinin emredici hükmü doğrultusunda ilgililerin açık rızası alınmaktadır. İşlenen özel nitelikli kişisel veriler;

- *Akciğer grafisi, odyometre, hemogram, kan grubu analizi, solunum fonksiyonu testi, göz muayenesi gibi sağlık raporları ve sağlık verileri,
- *Sabıka kaydı,
- *Mesai saatlerinin belirlenmesinde kullanılan pdks sistemi, parmak izi, retina taraması, avuç içi taraması,
- *Kamera görüntüleri ve kayıtları,
- *Fotoğraf,
- *İmza,
- *Ses kaydı,
- *Uyruk,
- *Dini inanç'tan ibarettir.

Fotoğraf, uyruk, dinin inanç, imza, ve ses kaydı; yasal zorunluluklar, açık rıza gibi hukuksal nedenlerle işlendiğinden bu özel nitelikli kişisel veriler onay prosedürüne dahil edilmemektedir.

7.KİŞİSEL VERİLERİN İŞLENME AMAÇLARI

SIRMAGRUP bu kişisel verileri;

- *Ürün ve hizmetlerin yasal çerçevede sunulabilmesi,
- *Çalışanlarla ilgili yasal yükümlülüklerin yerine getirilmesi,
- *Ticari ilişkilerin yürütülmesi,
- *Sözleşmelerden kaynaklanan yükümlülüklerin ifası,
- *Müşteri memnuniyeti ve tüketici şikayetlerinin giderilmesi,
- *Vergisel yükümlülüklerin yerine getirilmesi, muhasebe kayıtlarının tutulması,
- *Hizmet kalitesinin artırılması, veri sahipleri ile iletişime geçilmesi, ürün satışı, pazarlama ve bilgilendirme faaliyetlerinde bulunulması,
- *Müşteri edinimi, risk analizi, müşteri ve tüketici ihtiyaçlarına yönelik geliştirmeler yapılabilmesi, bülten ve davetiye gönderimi, risk analizi,
- *İç denetim, raporlama, pazar araştırması ve modelleme çalışmalarının yürütülmesi amaçları kapsamında işlemekte veya aktarabilmektedir.

8.SAKLAMA ORTAMLARI

Kişisel veriler, şirketimiz tarafından aşağıdaki tabloda gösterilen ortamlarda saklanır ve koruma altına alınır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)	Kağıt ve dosyalar
Yazılımlar (ofis yazılımları, portal,)	Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)
Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)	Birim dolapları,
Kişisel bilgisayarlar (Masaüstü, dizüstü)	Arşiv şirketi,
Mobil cihazlar (telefon, tablet vb.)	
Optik diskler (CD, DVD vb.)	
Çıkarılabilir bellekler (USB, Hafıza Kart vb.)	
Yazıcı, tarayıcı, fotokopi makinesi	

9.KİŞİSEL VERİLERİN GÜVENLİĞİNİ SAĞLAMAK AMACIYLA ALINAN TEKNİK VE İDARİ TEDBİRLER

SIRMAGRUP için kişisel verilerin güvenliğinin sağlanması konusundaki en önemli öncelik farkındalık eğitimleridir. Çalışanlarımızın bu konuda bilinçlendirilmeleri adına, tüm teknik ve idari tedbirlerin yanısıra ve hepsinden önce sürekli biçimde tekrarlanan eğitimler ve iç denetimlerle çalışanlarımızın konuya olan hassasiyetlerinin artırılması büyük önem taşımaktadır.

SIRMAGRUP, kişisel verilerin, iş bu güvenlik politikasında belirtilen amaçlar doğrultusunda işlenmesi, kötüniyetli kullanımların önüne geçilmesi ve hukuka aykırı erişimlerin önlenmesi adına teknik ve idari tüm tedbirleri almakta, alınan tedbirler zaman içinde gözden geçirilmekte ve güncellenmektedir.

9.1.İdari Tedbirler

Kişisel verilerin korunması kapsamında şirketimizde;

*Veri koruma programlarına tam olarak uyum sağlamak için tekrarlanan eğitimler ve farkındalık çalışmaları düzenlenmektedir.

*Ayrıntılı kişisel veri envanteri hazırlanarak her bir kişisel veri kategorisi için gerekli olan koruma yöntemi ayrı ayrı belirlenmektedir.

* Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.

*Gizlilik, Veri Koruma ve İmha Prosedürleri, kanunun yürürlüğe girmesinden sonra kanuna uygun hale getirilen şirket sözleşmeleri, yılda iki kez güncellenmektedir.

*Şirket bünyesinde bir veri koruma ekibi kurularak düzenli olarak prosedürlere uyum konusunda çalışmalar ve şirket içi denetimler yapılmaktadır. Veri koruma ekibi, 1 bilgi işlem, 1 hukuk müşavirliği, 1 iç denetim çalışanından oluşur.

*Veri koruma ekibinin toplantıları ve denetimleri bir tutanağa bağlanarak saklanır.

*Özel nitelikli kişisel veriler için, ilgili çalışanın yazılı açık rızası alınarak İnsan Kaynakları tarafından saklanır.

*Kişisel veri içeren dosyalar, özellikle çalışan özlük dosyaları, sözleşmeler, noter evrakları, şirket yazışmaları kilitli dolaplarda saklanır.

9.2.Teknik Tedbirler

Sırmagrup tarafından işlenen kişisel verilere ilişkin olarak alınan teknik tedbirler, aşağıda sıralanmıştır:

*Tüm personel bilgisayarları 90 saniye kullanılmama durumunda otomatik olarak kilitli ekrana geçmektedir.

*Tüm personel bilgisayarlarının kullanıcı parolası, 90 günde bir yenilenir.

*Personel, kendi bilgisayarından server bulunan verileri veya herhangi bir yazılımı kullandığında yalnızca yetkilendirildiği klasörlere ve yazılımın izin verilen bölümlerine erişebilmektedir.

*Kullanılacak parolaların güçlü parola olma özelliğine sahip olması zorunludur. (Büyük-küçük harf, rakam, minimum 8 karakter)

*WAN Networkünün sunucu erişimi sadece VPN üzerinde yapılmaktadır.

*VPN kullanıcı verilen outsource firmalar ile imzalanan sözleşmeler, gizlilik hükümleri içermektedir.

*B2B , ERP vb. uygulamalarda yetkilendirme ile veri erişimi kısıtlanmalı olarak yapılmaktadır. (örneğin fatura kesme personeli, cari hesap bilgilerini görebilirken, müşteriye tanımlı fiyat bilgilerini görememektedir).

*Sızma testleri yapılarak bilişim sistemlerine yönelik muhtemel tehditler önceden tespit ve bertaraf edilmektedir.

*Bilişim sistemlerine zarar verebilecek tehditler sürekli olarak izlenmektedir.

*Şirketin bilişim sistemleri donanımı, yazılım ve verilerin fiziksel güvenliği için gerekli tedbirler alınmakta, bu anlamda çevresel tehditlere karşı bilişim güvenliğinin sağlanması için, donanımsal tedbirler (sistem odasına yalnızca yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal tedbirler (firewall, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) 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 fiziksel ortamlara erişimler kayıt altına alınmaktadır (loglama).

*Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve koruma yazılımları güncel halde tutulmaktadır.

*Her türlü elektronik ortam, güçlü parolalarla korunmaktadır.

*Kötü senaryolar gözetilerek veri yedekleme programları kullanılmaktadır.

9.3.Özel Nitelikli Kişisel Verilerin Korunması İçin Alınan Tedbirler

Özel nitelikli kişisel veriler, her durumda ilgili kişinin rızasını zorunlu kılmaktadır. Bu nedenle ayrı bir aydınlatma ve onay metni ile işlenmeleri gerekir. Özel nitelikli kişisel veri sahibi, ayrıca ve özel olarak bilgilendirilir. Sirmagrup bünyesinde, üstte açıklanan teknik ve idari tedbirlere ilave olarak;

*Özel nitelikli kişisel veri işleme alanında çalışanlara yönelik özel nitelikli kişisel veri güvenliği eğitimi verilmekte ve bu konuda özel olarak farkındalık oluşturulmaktadır.

*Özel nitelikli kişisel verilerin gerek e-posta gibi dijital ortamlar veya taşınabilir bellek, CD, DVD gibi fiziki araçlar yolu ile taşınması durumunda, verilerin saklandığı dosya şifrelenmektedir. Kağıt yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı maximum hassasiyet gösterilmekte ve verilerin saklandığı fiziksel ortamlar ancak yetkili kişilerin erişimine açılmaktadır.

10.KİŞİSEL VERİLERİN SAKLANMA SÜRELERİ

Şirketimiz nezdinde işlenen kişisel veriler ilgili kanun ve yönetmeliklerde öngörülen süreler boyunca saklanmaktadır. Bu kapsamda iş sözleşmesinin uygulanmasından kaynaklanan ve Sosyal Sigortalar mevzuatı kapsamında yürütülen işlere ilişkin kişisel veriler 10 yıl, sağlık verileri ise İş Sağlığı Ve Güvenliği Hizmetleri Yönetmeliği kapsamında, işten ayrılma tarihinden itibaren en az 15 (onbeş) yıl süreyle saklanmaktadır. Farklı bir hukuki gerekçe ile işlenen kişisel veriler ise, iş mevzuatında yer alan en uzun dava zamanaşımı süresi olan 10 yıl boyunca saklanmaktadır.

11.KİŞİSEL VERİLERİN AKTARILMASI

Şirketimiz elde ettiği ve işlediği kişisel verileri, KVKK'nun 8. maddesine uygun olarak yurtiçinde veya yurtdışında üçüncü kişilere (iş ortakları, müşteriler, tedarikçiler, grup şirketleri) aktarabilmektedir. Bu kapsamda Şirketimiz nezdinde bulunan kişisel verilerin bir kısmı şirket içi iletişim, denetim, iş geliştirme veya yürütülen ticari faaliyetler kapsamında paylaşılmaktadır.

Bunun yanı sıra hukuka uygun kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemleri alarak bazı kişisel verileri, grup şirketleri bünyesinde yürütülen bazı projeler kapsamında yurtdışındaki grup şirketlerine aktarabilmektedir.

12.KİŞİSEL VERİLERİN İMHASI VE ANONİMLEŞTİRİLMESİ

12.1.İmha Nedenleri

Kişisel veriler, Kurum tarafından re'sen veya veri sahibinin/ilgili kişinin başvurusu üzerine bu başvurunun kabul edilmesi ile veya Kanun'un 5 ve 6. Maddesinde sayılan sebeplerin veya iş bu politikada sayılan amaçların ortadan kalkması veya saklama süresinin dolması halinde resen silinir, yok edilir veya anonimleştirilir.

Kişisel verinin aktarılmış olması durumunda, mutlaka aktarıldığı yerde takibi yapılarak imha edilmesi veya anonimleştirilmesi sağlanır.

12.2.Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda belirtilen yöntemlerle silinir:

12.2.1.Serverlar'da Yer Alan Kişisel Veriler: Sunucularda yer alan kişisel veriler, saklama süresinin tamamlanmasını takiben, sistem yöneticisi tarafından silinir.

12.2.2.Elektronik Ortamda Yer Alan Kişisel Veriler: Elektronik ortamda bulunan kişisel veriler, saklama süresinin dolmasını müteakiben veri tabanı yöneticisi tarafından silinir.

12.2.3.Fiziksel Ortamda Bulunan Kişisel Veriler: Fiziksel ortamda tutulan kişisel veriler, saklama süresinin tamamlanmasını müteakiben evrak arşivinden sorumlu birim yöneticisi tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

12.3.Kişisel Verilerin Yok Edilmesi

12.3.1. Fiziksel Ortamda Bulunan Kişisel Veriler: Saklama süresi dolan fiziksel ortamdaki kişisel veriler, kağıt öğütücü kullanmak suretiyle yok edilir.

12.3.1. Manyetik Ortamda Bulunan Kişisel Veriler: CD gibi manyetik ortamlarda bulunan kişisel veriler Saklama süresinin dolması üzerine, kırma, yakma, toz haline getirme gibi yollarla kullanılamaz hale getirilir.

12.4.Kişisel Verilerin Anonim Hale Getirilmesi:

Kişisel verilerin anonim hale getirilmesi, verinin hiçbir biçimde kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

13.SAKLAMA VE İMHA SÜRELERİ

Saklama süresine ilişkin olarak, Mevzuatta bir süre öngörülmüş ise her durumda bu süreye riayet edilir. Anılan sürenin sona ermesi ile veriler silinir, yok edilir ya da anonim hale getirilir. Mevzuatta saklama süresi öngörülmemesi durumunda, işleme amaçları ve hukuki sebep değerlendirilerek, şirketin menfaatleri doğrultusunda uygun saklama süresi tespit edilir. Tespit edilen sürelerin, zaman içinde revizyona ihtiyaç duyması durumunda koruma ve imha politikası güncellenir.

Saklama süresi dolan kişisel veriler, işbu Politikada belirtilen imha süreleri çerçevesinde, 6 (altı) aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak anonim hale getirilir veya imha edilir. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanır.

14.SORUMLULUK

Bu politikanın uygulanmasında Ek-1'de yer alan listede yazılı olan şirket çalışanları, kişisel verilerin korunmasına yönelik şirketçe alınan teknik ve idari tedbirler bir yana, kendi bölümlerinde işlenen kişisel verilerin korunması, saklama sürelerinin takibi ve imhası açısından birinci derecede sorumludurlar.

15.İLETİŞİM

Sirmagrup İçecek San ve Tic A.Ş. (Veri Sorumlusu)

Küçükbakkalköy mah. Vedat Günyol Cad. Defne sokak Büyükhanlı Plaza No.3 Kat.11 Ataşehir / İstanbul

İrtibat Kişisi:

Sedat Yıldız

Sedat.yildiz@sirmagrup.com

EKLER:

- 1.Sorumluluk çizelgesi .
- 2.Saklama ve imha süreleri tablosu .

EK-2 SAKLAMA VE İMHA SÜRELERİ TABLOSU		
KİŞİSEL VERİ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Hukuk		
Sözleşmeler	Sözleşme süresinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Dava dosyaları ve icra takipleri	Davanın veya icra takibinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Çalışanlarla ilgili resmi yazışmalar	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
İnsan Kaynakları		
Personel özlük dosyası	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Değerlendirme dışı bırakılan iş başvuruları	Başvurunun olumsuz sonuçlanmasından itibaren 2 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Ücret ve maaşlara ilişkin tüm belgeler	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Sabıka kayıtları	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Çalışanlarla ilgili sağlık kayıtları, özel sağlık ve ferdi kaza poliçeleri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Eğitim kayıtları	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Parmak izi kayıtları	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Güvenlik kamera görüntüleri	(ziyaretlerde 1 yıl, çalışan kayıtlarında iş ilişkisinin sona ermesinden 10 yıl)	Saklama süresinin bitimini takip eden 180 gün içinde.
Bilişim Sistemleri (IT)		
Loglar	1 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
İnternet ve wifi aracılığı ile ediletilen bilgiler	1 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
İdari İşler		
Taahhüt plaka bilgileri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Araç takip sistemi raporları	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Ziyaretçi kayıtları	1 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Tüketici şikayeti ses kayıtları	2 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.

Finans		
Ödeme işlemleri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Banka hesap bilgileri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Cari kart verileri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Kambiyo senetleri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Kalite		
Tüketici şikayetleri	5 yıl	Saklama süresinin bitimini takip eden 180 gün içinde.
Kişisel verinin Türk Ceza Kanunu anlamında bir suçta konu olması durumunda, saklama süresi hüküm kesinleşinceye kadar uzatılır.		