

GAZEBO ÇİÇEKÇİLİK ORGANİZASYON SANAYİ VE TİCARET LİMİTED ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

MADDE 1 – VERİ SORUMLUSU TANIMI

Levent Mah., Ebulula Mardin Cad., 4. Gazeteciler Sitesi, A 1/2 Blk., No:67 Beşiktaş/İstanbul adresinde bulunan ve İstanbul Ticaret Sicili Müdürlüğü nezdinde 26824-5 sicil numarası ile kayıtlı olan Gazebo Çiçekçilik Organizasyon Sanayi ve Ticaret Limited Şirketi (“Şirket”)’dir.

MADDE 2- AMAÇ

Gazebo Çiçekçilik Organizasyon Sanayi ve Ticaret Limited Şirketi olarak, 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nun (“KVKK” veya “Kanun”) yürürlüğe girdiği tarihten itibaren, ticari faaliyetlerimizi yerine getirirken herhangi bir şekilde temas ettiğimiz tüm gerçek kişilere ait kişisel verilerin korunmasına ve bu çerçevede KVKK’ da yer alan gerekliliklerin eksiksiz olarak yerine getirilmesine büyük önem vermekteyiz. Kanun’una uyum projesi kapsamında Şirket tarafından; T.C. Anayasası, Kanun ve ilgili mevzuata uygun olarak Şirket çalışanlarına, aday çalışanlara, müşterilere, aday müşterilere ve tedarikçilere yönelik kişisel verilerin işlenmesi ve ilgili kişilerin talep ettikleri haklarını kullanması birincil nitelikte önem arz etmektedir.

Bu sebeple; iş bu **Kişisel Verileri Saklama ve İmha Politikası** (“Politika”), kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silinmesi, yok edilmesi ve anonim hale getirilmesi hakkında veri sorumlusu sıfatıyla Şirket tarafından sizleri bilgilendirmek amacıyla hazırlanmıştır.

MADDE 3- KAPSAM

Kanun ile tanımlanan Şirket nezdinde tutulan kişisel veriler ve özel nitelikli kişisel veriler, tüm Şirket çalışanları, çalışan adayları, müşteriler, aday müşteriler ve tedarikçilere ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamındadır.

Şirketin sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

MADDE 4- TANIMLAR

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
Çalışan	: Şirket 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	: Şirket 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
Periyodik imha	: 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
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 işleme 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 işlenmesi	: 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
Politika	: Kişisel Verileri Saklama ve İmha Politikası
Şirket	: Gazebo Çiçekçilik Organizasyon Sanayi ve Ticaret Limited Şirketi
Veri işleyen	: 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 kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Yönetmelik	: 28 Ekim 2017 tarihli Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

MADDE 5- SORUMLULUK VE GÖREVLER

Şirketin tüm çalışanları ve yöneticileri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması konusunda sorumlu kişilere tam ve aktif destek verir. Politika kapsamında alınan idari ve teknik tedbirlerin uygulanmasında, çalışanlarının eğitilmesinde, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesinde ve kişisel verilerin hukuka uygun olarak muhafazasında tüm çalışanlar ve yöneticiler, sorumlu kişilere destek olur.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları ve görev tanımlarına ait dağılım aşağıdaki tabloda gösterilmiştir.

UNVANI	GÖREVİ
Şirket Müdürü	Çalışanların politikaya uygun davranmasından sorumludur.
Şirket Müdürü	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Şirket Müdürü	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
Şirket Müdürü	Veri saklama ve imha süreçlerinin ilgili kanunlara ve politikaya uygun şekilde yerine getirilmesinden sorumludur.
Diğer Tüm Şirket Çalışanları	Şirket Müdürü'nün talimat ve yetkilendirmesi dahilinde, görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

MADDE 6- KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel bilgisayarlar Mobil Cihazlar Optik diskler Yazıcılar, tarayıcılar, fotokopi makineleri Çıkarılabilir ve taşınabilir bellekler Sunucular Yazılımlar Bilgi güvenliği cihazları Sunucular (Database, yedekleme, e-posta vb.) Bilgisayar formatları (PDF vb.) Kamera DVR depolama cihazı Kariyer.net	Basılı- Kağıtlar Dosyalanmış ve dolaplarda kilitlenmiş Basılı – ilgili defterler Basılı – dosya ve klasörler Görsel kayıtlar Manuel veri kayıt sistemleri

MADDE 7- SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Veri sahiplerine ait kişisel veriler, ŞİRKET tarafından özellikle ticari faaliyetlerin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması ve ifası ile müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan fiziki veya elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır. Şöyle ki;

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,

- c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketim meşru menfaatleri için saklanması zorunlu olması,
- d. Kişisel verilerin Şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- e. Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

MADDE 8- SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Kanun'un 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. 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. maddelerde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır. Şirket'de, 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,
- İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6502 Sayılı Tüketici Kanunu ve ilgili yönetmelikler
- 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

Şirket aşağıdakiler dahil olmakla birlikte ancak bunlarla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir veya saklayabilir:

- a- İnsan kaynakları süreçlerini yürütülmesi ve planlanması
- b- Kurumsal iletişimi sağlamak
- c- Şirket güvenliğini sağlamak
- d- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
- e- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
- f- Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
- g- Yasal raporlamalar düzenlemek
- h- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek
- i- Şirket hukuk işlerinin icrası/takibini yapmak

- j- İş faaliyetlerinin yürütülmesi / denetimi
- k- Erişim yetkilerinin yürütülmesi
- l- Organizasyon ve etkinlik yönetimi
- m- Denetim / etik faaliyetlerinin yürütülmesi
- n- Fiziksel mekân güvenliği
- o- Acil durum yönetimi süreçlerinin yürütülmesi
- p- Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi
- q- Bilgi güvenliği süreçlerinin yürütülmesi
- r- Mal / hizmet satın alım süreçlerinin yürütülmesi
- s- Finans ve muhasebe işlerinin yürütülmesi

MADDE 9- İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Çalışanlar, aday çalışanlar, müşteriler, aday müşteriler ve tedarikçiler olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanun'a uygun olarak saklama ortamlarında muhafaza edilir ve imhayı gerektiren sebeplerden birinin gerçekleşmesi halinde silinerek, yok edilerek veya anonim hale getirilerek Şirket tarafından imha edilir.

Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Şirket tarafından re'sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

- a. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması,
- b. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- c. Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması.
- d. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması
- e. İlgili kişinin, Kanun'un 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- f. Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması.

MADDE 10- KİŞİSEL VERİLERİN SAKLANMASINA İLİŞKİ USULLERİ

10.1 KAYIT ORTAMLARINDAKİ TEDBİRLER

Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:

- EXCHANGE SERVER
- FILE SERVER

Fiziksel ortamlar:

- Kilitli Dolapları
- ARŞİV

10.2 TEKNİK TEDBİRLER

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

- a- Kurulan sistemler kapsamında gerekli iç kontrolleri yapar
- b- Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür
- c- Verilerin şirket dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar
- d- Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti olarak sistem zafiyetlerinin kontrolünü sağlar
- e- Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar
- f- Kişisel verilerin yok edilmesi geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlanır
- g- Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur
- h- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerini sürekli takip ederek gerekli güvenlik testlerinin düzenli olarak yaptırılmasını sağlar.
- i- Özel nitelikli kişisel verilere bir yazılım aracılığı ile erişilen durumlarda bu yazılıma ait kullanıcı yetkilendirmelerini yaparak bu yazılımların güvenlik testlerinin düzenli olarak yaptırılmasını sağlar.
- j- Özel nitelikli kişisel verilere uzaktan erişim gereken hallerde en az iki kademeli kimlik doğrulama sistemi sağlar.
- k- Özel nitelikli kişisel verilerin aktarıldığı durumlarda;

Verilerin e-posta ile aktarılması gerekiyor ise bunların şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmasını,

Verilerin kâğıt ortamında aktarımı gerekiyorsa evrakın “gizlilik dereceli belgeler” formatında gönderilmesini sağlar.

10.3 İDARİ TEDBİRLER

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

- a- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli çalışan ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- b- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul’a bildirir.
- c- 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 sağlar.
- d- Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli çalışan istihdam eder ve çalışanlarına kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- e- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

MADDE 11- KİŞİSEL VERİLERİN İMHA YÖNTEMLERİ VE USULLERİ

Şirket tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel verileriniz; 6698 Sayılı Kanun madde 7/1’e göre işlenmesi gerektiren amaçların ortadan kalkması veya kullanım amacına yönelik saklama süresinin dolması halinde Şirket tarafından re’sen yahut İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak tarafımızca silinecek, yok edilecek ve anonimleştirilecektir.

Kişisel verilerin, Şirket tarafından re’sen ya da ilgili kişinin başvurusu üzerine imha edilmesinde Kanunun 4. maddesindeki genel ilkelere, 12. madde uyarınca alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun olarak hareket edilmesi zorunludur.

11.1 Kişisel Verilerin Silinmesi

Tamamen veya kısmen otomatik yollarla işlenen kişisel verilerin silinmesi; söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Şirket, kişisel verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirecektir. Şirket bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti etmektedir. Bu garanti, veri sorumlusunun sorumluluğu altındadır.

Silme sırasında, silinmemesi gereken kişisel veriler de yapılan silmeden etkileniyorsa ve erişilemeyecek ve/veya kullanılamayacak hale geliyorsa Şirket, Kişisel verileri aşağıda belirtilen yöntemlerle siler.

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortam	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 ortam	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 medya	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.

11.2 Kişisel Verilerin Yok Edilmesi

Yok etme işlemi, Şirketin verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve Şirket bu verileri tekrar geri getirilmesi mümkün olmayacak hale getirmekle yükümlüdür. Bu işlemler sırasında Şirket çalışanları ve ilgili departmanlar KVKK Çalışma Grubu'na yok edilecek ilgili verileri bildirmekle yükümlüdür, sonrasında ise Şirket gerekli her türlü teknik ve idari tedbiri alacaktır.

Kişisel veriler aşağıda yer alan tabloda belirtilen yöntemlerle yok edilir.

Veri Kayıt Ortamı	Yok Edilme Yöntemi
-------------------	--------------------

Fiziksel ortam	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medya	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

11.3- Kişisel Verilerin Anonimleştirilmesi

Anonim hale getirme işlemi, Şirket'in kişisel verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonimleştirilmesi Şirket'in içerisinde veri sahibi iş biriminin görevidir. Veri sahibi iş birimi, verilerin yok edilmesi için denetimi kendisi tarafından yapılmak kaydıyla Şirket'in farklı departmanlarından destek alabilir.

Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirmeye yöntemleridir.

Değişken Çıkartma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden "yüksek dereceli betimleyici" olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır. Örneğin, şirketin futbol takımının yedek listesinde olan ilgili veri sorumluları arasında yalnızca bir kişi 65 yaşında ise yaş, cinsiyet ve sağlık

durumu yönünden futbol oynayabilecek olup olmadığı bilgisinin birlikte saklandığı bir veri kümesinde 'Yaş:65' yerine 'Bilinmiyor' yazılması veya bu kısmın boş bırakılması anonimleştirmeyi sağlayacaktır.

Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin; çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

Global Kodlama: Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır.

Örneğin, maaş bilgisi için; 10.000 TL altı ve üstü iki grup yapılırsa, 10.000 ve daha az maaş alan kişilerin maaşlarının toplamı kişi sayısına bölünür ve 10.000TL altında maaş alan herkesin maaş kümesine elde edilen bu değer yazılır.

Veri Değiş Tokuşu: Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.

KVKK'nın 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

MADDE 12- SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasıyla ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bunun haricinde; aşağıdaki tabloda yer alan saklama ve imha süresi tablosu esas alınır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş Sağlığı ve Güvenliği İle İlgili Veriler	İş ilişkisinin bitimini takiben 15 yıl	Saklama süresinin bitimini takiben 180 gün
İş Kanunu Kapsamında Saklanan Veriler	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Personel Mahkeme/ Adliye Taleplerinin Cevaplandırılması	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Eğitim Kayıtlarının Dosyalanması	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Acil Durum Hazırlıkları	İş ilişkisinin bitimini takiben 15 yıl	Saklama süresinin bitimini takiben 180 gün
Log Kayıt Takibi	Kayıt altına alınmasına müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün
Kamera Kayıtları	Kaydedilmesinden itibaren 1 ay	Saklama süresinin bitimini takiben 180 gün
Şirket Ortakları ve Yönetim Kurulu Üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün
Çalışan Adaylara İlişkin Veriler	Başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün
Stajyerlere İlişkin Veriler	Stajın sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Müşterilere İlişkin Veriler	Kayıt altına alınmasından itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Aday Müşterilere İlişkin Veriler	Kayıt altına alınmasından itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün
Organizasyona Ait Veriler	Etkinliğin sona ermesinden sonra 10 yıl	Saklama süresinin bitimini takiben 180 gün
Etkinlik ve Organizasyonlarda Elde Edilen Görsel ve İşitsel kayıtlar	Etkinliğin sona ermesinden sonra 10 yıl	Saklama süresinin bitimini takiben 180 gün
Tedarikçiler Ait Veriler	Kayıt altına alınmasından itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün

Muhasebe Kayıtları	Kayıt altına alınmasından itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Sair İlgili Mevzuat Gereği Toplanan Veriler	İlgili mevzuatta öngörülen süre kadar	Saklama süresinin bitimini takiben 180 gün

MADDE 13- PERİYODİK İMHA SÜRESİ

Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; ŞİRKET işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re 'sen gerçekleştirilecek bir işleme siler, yok eder veya anonim hale getirir.

Ayrıca kişisel veri sahipleri Şirket'e yazılı talep ile bildirim yaptığında, ilgili kişiye ait tüm veriler imha yöntemi prosedürüne göre silinir, yok edilir veya anonim haline getirilir.

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 (altı) ay olarak belirlemiştir.

MADDE 14- POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuoyuna ilan edilir. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

MADDE 15- YÜRÜRLÜK

Politika, şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 3 yıl süre ile şirket tarafından saklanır.