CERTUS ALÇI VE DÖKÜM TEKNOLOJİ SAN.A.Ş.

KVK SİLME, İMHA ETME, ANONİMLEŞTİRME POLİTİKASI

AMAÇ

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a (Kanun) dayalı olarak çıkarılmış olan ve 30224 sayılı Resmi Gazete 'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Yönetmelik) 5. ve 6. maddeleri gereği kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi için şirketimiz genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

KAPSAM

Politika, şirketimiz nezdinde tutulan, Kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri, tüm Şirket çalışanlarını, yöneticilerini, danışmanlarını ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerini, dış hizmeti sağlayıcılarını ve Şirketimizin sair hukuki ilişkiye girdiği gerçek ve tüzel kişileri kapsamaktadır.

Politika Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri kapsamaktadır. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak
adlandırılacaktır.

POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI

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 kayıt ortamı kapsamına girer. Türk Ceza Kanunu'nun 138. Maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Şirketimizin kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir. Bu kapsamda Şirketimiz ilgili yükümlülüğünü bu bölümde açıklanan yöntemlerle yerine getirmektedir.

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ YÖNTEMLERİ

1. Kişisel Verilerin Silinmesi

A. Kişisel Verilerin Silinmesi İşlemi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir. Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

B. Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

C. Kişisel Verilerin Silinmesi Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır: Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365 Salesforce, Dropbox gibi: Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

Kâğıt Ortamında Bulunan Kişisel Veriler: Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

2. Kişisel Verilerin Yok Edilmesi

A. Kişisel Verilerin Yok Edilmesi İşlemi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri yok edebilir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

B. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

a.) **Yerel Sistemler:** Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.

- **De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
- **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
- **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır

b.) **Çevresel Sistemler:** Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

- **Ağ cihazları (switch, router vb.):** Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATAvb.), SCSI (SCSI Express vb.)ara yüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Manyetik bant:** Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
- **Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

- **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.
- **Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- **Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c.) Kâğıt ve Mikro Fiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

d.) Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,
- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

3. Kişisel Verilerin Anonim Hale Getirilmesi

A. Kişisel Verilerin Anonimleştirilmesi İşlemi

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

olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları 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. Şirketimiz, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almaktadır.

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 dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

B. Kişisel Verilerin Anonimleştirilmesi Yöntemleri

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır. Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki tabloda gösterilmektedir:

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	Değişkenleri Çıkartma Kayıtları Çıkartma Alt ve Üst Sınır Kodlama Bölgesel Gizleme Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	Mikro-Birleştirme Veri Değiş-Tokuşu Gürültü Ekleme Tekrar Örnekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler	K-Anonimlik L-Çeşitlilik T-Yakınlık

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri:

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

a-Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

b-Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır. Örneğin anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

c-Bölgesel Gizleme

Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

d-Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir. Örneğin TC Kimlik No 12345678901 olan bir kişi e-ticaret platformundan çocuk bezi aldıktan sonra aynı zamanda ıslak mendil de almış olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan çocuk bezi alan kişilerin %xx'i aynı zamanda ıslak mendil de satın alıyor şeklinde bir sonuca ulaşılabilir.

e-Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

f-Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbekleşerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

g-Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır. Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

a-Mikro Birleştirme

Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

b-Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

c-Gürültü Ekleme

Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin

bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a. K-Anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır

b. L-Çeşitlilik

K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

c. T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

Anonim Hale Getirme Yönteminin Seçilmesi

Şirketimiz, yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak ve sahip olunan veri kümesine dair aşağıdaki özellikler dikkate alınarak karar vermektedir;

- Verinin niteliği,
- Verinin büyüklüğü,
- Verinin fiziki ortamlarda bulunma yapısı,
- Verinin çeşitliliği,
- Veriden sağlanmak istenen fayda / işleme amacı,
- Verinin işleme sıklığı,
- Verinin aktarılacağı tarafın güvenilirliği,
- Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,
- Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,
- Verinin dağıtıklık/merkezilik oranı,
- Kullanıcıların ilgili veriye erişim yetki kontrolü ve
- Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

Bir veri anonim hale getirilirken, Şirketimiz kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmektedir.

Anonimlik Güvencesi

Şirketimiz, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilirken, anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması, bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması, anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi noktalarına dikkate dilemekte olup, Şirketimizce anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapılmakta ve anonimliğin korunduğundan emin olunmaktadır.

Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirmenin Bozulmasına Dair Risklerin Değerlendirilmesi ve Önlenmesi

Anonim hale getirme işlemi, kişisel verilere uygulanan ve veri kümesinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir. Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır. Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere "anonimliğin bozulmasına yönelik saldırılar" denilmektedir. Bu kapsamda, Şirketimizce anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmektedir.

KİŞİSEL VERİLERİ KORUMA KOMİTESİ'NİN GÖREV VE YETKİLERİ

Kişisel Verileri Koruma Komitesi Politikanın ilgili iş birimlerine duyurulmasından ve gereklerinin şirketimiz birimlerince yerine getirilmesinin takibinden sorumludur. Kişisel Verileri Koruma Komitesi kişisel verilerin korunmasına ilişkin mevzuat değişiklikleri, Kurulun düzenleyici işlemleri ile kararları, mahkeme kararları veya süreç, uygulama ve sistemlerdeki değişiklikler gibi durumları ilgili iş birimlerinin takip etmesi ve gerekiyorsa iş süreçlerini güncellemeleri için gerekli duyuruları ve bildirimleri yapar, Kişisel Verileri Koruma Komitesi; Kanun ve ikincil düzenlemeleri ile Kurulun kararları ve düzenlemeleri, mahkeme kararları ve sair yetkili makamların kararlarının ve/veya taleplerinin incelenmesi, değerlendirilmesi, takibi ve sonuçlandırılmasına yönelik süreçleri belirler ve ilgili birimlere duyurur.

KİŞİSEL VERİLERİN İŞLENME ŞARTLARININ ORTADAN KALKMASI DURUMUNDA YAPILACAKLAR

Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının

tamamının oradan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok edilir veya anonim hale getirilir. Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi şirket birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç altı aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildirimi üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır.

Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır. Merkezi Bilgi Sistemlerinde yer alan çok paydaşlı veri sahipliği bulunan kişisel verilerin imhasına yönelik karar alınması gerektiğinde ise Kişisel Verileri Koruma Komitesi'nin görüşü alınacak ve söz konusu kişisel veri hakkında işbu politikaya göre verinin saklanmasına veya silinmesine, yok edilmesine veya anonim hale getirilmesine ilgili veri sahibi iş birimi tarafından karar verilecektir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere **en az üç yıl** süreyle saklanır.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4.maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden şirketimize başvurarak kendisine ait kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini talep ettiğinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Bu durumda detayları Veri İmha Prosedüründe belirleneceği şekilde; talep, başvuru tarihinden itibaren en geç otuz gün içinde sonuçlandırılır ve ilgili kişiye bilgi verilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, ilgili veri sahibi iş birimi bu durumu derhal aktarım yapılan üçüncü kişiye bildirir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, kişisel veri sahiplerinin verilerinin silinmesi veya yok edilmesine yönelik talepleri Şirket tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir.

Ret cevabı ilgili kişiye **en geç 30 gün** içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara

yönlendirilecektir.

POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR

İşbu Politika tüm çalışanlara duyurularak yürürlüğe girecek ve yürürlüğü itibariyle tüm iş birimleri, danışmanlar, dış hizmet sağlayıcıları ve sair şirket nezdinde kişisel veri işleyen herkes için bağlayıcı olacaktır.

Şirketimiz çalışanlarının Politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın amiri tarafından bağlı bulunan bir üst amire bildirilecektir. Aykırılığın önemli boyutta olması halinde ise üst amir tarafından vakit kaybetmeksizin Kişisel Verileri Koruma Komitesi'ne bilgi verilecektir.

Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır. Politika gereklerinin yerine getirilmesi için şirketimiz tarafından; gerekli tüm güvenlik önlemleri alınmaktadır.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI

Şirket içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette şirketimiz nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerinde bulunması durumunda, söz konusu veri bilgi sistemlerinden sorumlu birimler tarafından saklanacaktır.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak ilgili bilgi sistemleri bölümlerince yapılacaktır.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

1. Kişisel Verileri Saklama ve İmha Süreleri

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo'da yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Şirket kişisel veri envanterinde yer alacak süreçlerin sahibi iş birimlerince, tereddüt halinde Kişisel Verileri Koruma Komitesi değerlendirmeleri de alınarak güncellenecektir.

2. Periyodik İmha Süreleri

Kişisel Verileri Periyodik İmha Süresi veri sahibi ilgili iş birimleri tarafından tespit ve tayin edilir; ancak her halde bu süre **6 (altı) ayı** geçemez.

YÜRÜRLÜK VE GÜNCELLEME

Politika yayınlanma tarihi itibari ile yürürlüğe girecektir. Politikanın şirketimiz genelinde duyurulması ve gerekli güncellemelerin yapılması Kişisel Verileri Koruma Komitesi'nin sorumluluğundadır.

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo

Kişisel veriler aksine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça Politikanın 6. maddesinde belirtilen hususlar dikkate alınarak aşağıdaki tabloda belirtilen süreler boyunca saklanacak, süre sonunda ise imha edilecektir:

Genel dava zaman aşımı süresini düzenleyen Borçlar Kanunu'nun 146. Maddesi gereği	10 yıl
Sair ilgili mevzuat gereği	İlgili mevzuatta öngörülen süre kadar
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması veya bir suç ile ilişkili olması durumunda Türk Ceza Kanunu'nun 66. ve 68. maddeleri gereği	Dava zaman aşımı ve Ceza Zaman aşımı müddetince