1e

Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Prosedürü

sürüm 1.0

accert.com.tr
Haziran 2022 Ankara

	DENİZLİ TİCARET ODASI	Doküman No : KVK-1.E
	KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ ve ANONİMLEŞTİRİLMESİ	İlk Yayın Tarihi : 30/06/2022
		Son Güncelleme Tarihi :
		Versiyon : 1.0

Hazırlayan:	Sistem Onayı:	Yürürlük Onayı:
Kişisel Veri Koruma Yöneticisi	Kalite Yöneticisi	Genel Sekreter

REVİZYON TAKİBİ

Revizyon No	: 01	Açıklama:
Tarih	: 30.06.2022	
Dağıtım	: Tüm Bölüm ve Birimler	

POLİTİKA BELGESİNİN İÇERİK VE NİTELİĞİ

Bu Politika Belgesi, Denizli Ticaret Odası için yapılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'na Uyumluluk çalışmaları kapsamındaki bulgu ve değerlendirmeleri içerir.

Bu bulgu ve değerlendirmeler, [ODA] tarafından ACCERT Sertifikasyon Belgelendirme Danışmanlık Eğitim ve Denetim A.Ş (ACCERT A.Ş.) ile paylaşılan bilgi, belge ve beyanlar ölçüsünde, KVKK mevzuatı ile verilerin depolanıp işlendiği ortamlar temel alınarak hazırlanmıştır. ACCERT A.Ş. danışmanlık hizmetini, danışmanlık hizmetinin verildiği tarihteki yasal mevzuat ve mevcut düzenlemeler ile [ODA'nın] kendisi ile paylaştığı bilgi ve veriler kapsamında sağlamış olup [ODA'nın] kendisiyle paylaşmadığı veyahut sonradan mevzuat değişikliği, içtihat değişiklikleri gibi sebeplerle uygulamada ortaya çıkacak farklılıklar nedeniyle ACCERT A.Ş.'nin herhangi bir sorumluluğu bulunmamaktadır.

Ayrıca, bu belgede yer alan değerlendirme ve öneriler tavsiye niteliğinde olup özellikle verilerin toplanması, işlenmesi, aktarılması ve yok edilmesi konusundaki idari ve teknik tedbirlerin KVKK düzenlemelerine uygun biçimde uygulanması konusundaki sorumluluk ve riskler [ODA'nın] uhdesindedir. Kişisel veriler ile ilgili bilgilerin güncel ve doğru olarak işlenmesi için gerekli önlemlerin alınması [ODA'nın] sorumluğundadır.

KVKK düzenlemelerinin öngördüğü bütün tedbirlerin yanı sıra uygulamadan kaynaklanabilecek risklerin yönetimi ve bunların önlenmesine için gerekli denetim sorumluluğu (KVKK Madde 12 (3)) Veri Sorumlusu olarak [ODA'ya] ait olup, ilgili iş birimlerinin beyan etmediği veya eksik beyan ettiği bilgiler nedeniyle ortaya çıkabilecek zararlar başta olmak üzere, [ODA'nın] yükümlülüklerini gereği gibi yerine getirilmesine rağmen diğer nedenlerden oluşabilecek doğrudan veya dolaylı zararlardan ACCERT A.Ş. sorumlu değildir.

İÇİNDEKİLER

1.GİRİŞ

1.1. Amaç ve Dayanak

6698 Satılı Kişisel Verileri Koruma Kanunun 7/3 ve 22/1.e maddelerine istinaden Kişisel Verileri Koruma Kurulu tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hazırlanmış olup 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanmıştır.

Bu Yönetmeliğe dayanarak Kurul tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi hazırlanmış ve kamuoyuna sunulmuştur.

Bu rehbere https://www.kvkk.gov.tr/Icerik/2038/Kisisel-Verilerin-Silinmesi,-Yok-Edilmesi-veya-Anonim-Hale-Getirilmesi adresinden erişilebilir.

Bu dokumanda bu rehber temel alınarak "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi" özetlenmeye çalışılmıştır.

1.2. Tanımlar

Alıcı grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini
Doğrudan tanımlayıcılar	Tek başlarına ilişki içinde oldukları kişiyi doğrudan açığa çıkaran ifşa eden ve ayırt edilebilir kılan tanımlayıcıları
Dolaylı tanımlayıcılar	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran ifşa eden ve ayırt edilebilir kılan tanımlayıcıları
İlgili kişi	Kişisel verisi işlenen gerçek kişiyi
İlgili kullanıcı	Verilerin teknik olarak depolanması korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariçolmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişileri
İmha	Kişisel verilerin silinmesi yok edilmesi veya anonim hale getirilmesini
Karartma	Kişisel verilerin bütününün kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi
Kayıt ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı
Kişisel Veri Saklama ve İmha Politikası	Veri sorumlularının kişisel verilerin işlendikleri amaçiçin gerekli olan azami süreyi belirleme işlemi ile silme
Maskeleme	Kişisel verilerin belli alanlarının kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi

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

2. Kişisel Verilerin Silinmesi ve Yok Edilmesi

Kişisel verilerin silinmesi ve yok edilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıda açıklanacak yöntemlerle gerçekleştirilebilir.

2.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

2.1.1. 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.

2.1.2. Kişisel Verilerin Silinmesi Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

a) 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.

b) Kağıt Ortamında Bulunan Kişisel Veriler

Kağıt 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.

c) 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.

ç) Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

d) 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.

2.2. Kişisel Verilerin Yok Edilmesi

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.

2.2.1. 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, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> 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, parmakizli 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) Kağıt ve Mikrofiş Ortamları

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kağıt 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.

ç) 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

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 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.

Veri sorumlusu, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir.

3.1. Kişisel Verilerin Anonim Hale Getirilmesi

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/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 Çıkarma ✓ Kayıtları Çıkarma ✓ Bölgesel Çıkarma ✓ Genelleştirme ✓ Alt ve Üst Sınır Kodlama ✓ Global Kodlama ✓ Örnekleme Değer

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	✔ Mikro Birleştirme ✔ Veri Değiş Tokuşu ✔ Gürültü Ekleme
Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler	✔ K- Anonimlik ✔ L-Çeşitlilik ✔ T- Yakınlık

3.1.1 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. Değer düzensizliği sağlamayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır:

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 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 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.

ç) 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 imkansız 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.

d) 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.

e) 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 öbeklenerek 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.

Bu veri kümesinde tek bir ilçedeki kadınların nüfusuna ait verinin meslek değişkeninde iki kategoride yığılma görüldüğünden söz konusu iki kategorinin birleşiminden tek bir kategori elde edilebilir ve bu durumda veri daha güvenli hale getirilmiş olur.

f) 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.

3.1.2. 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

c) Gürültü Ekleme

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

3.1.3. Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel 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 getirilmesiyle oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.

b) L-Çeşitlilik

K=4 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 denilmektedir.

3.2. Anonim Hale Getirme Yönteminin Seçilmesi

Veri sorumluları yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak karar verirler. Anonim hale getirme yöntemleri uygulanırken sahip olunan veri kümesine dair aşağıdaki özelliklerin de veri sorumluları tarafından dikkate alınması tavsiye edilir:

- Verinin niteliği,
- Verinin büyüklüğü,
- Verinin fiziki ortamlarda bulunma yapısı,
- Verinin çeşitliliği,
- Veriden sağlanmak istenen fayda / işleme amacı,
- Verinin işlenme 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,
- Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

Bir veriyi anonim hale getirdiğini düşünen veri sorumlusu, 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 etmek sorumluluğundadır.

3.3. Anonimlik Güvencesi

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir. Bu şartların yerine getirilmiş olmasını veri sorumluları sağlamalıdır:

- 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 oluşturamaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Bu riskler sebebiyle veri sorumlularının, anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapmaları ve anonimliğin korunduğundan emin olmaları gerekmektedir.

3.4. Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirmenin Bozulmasına Dair Riskler

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 açıklandıktan 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 saldırılar farklı profildeki kullanıcılar tarafından farklı motivasyonlarla gerçekleşebilmektedir.

Saldırıların motivasyonlarını aşağıdaki başlıklarda toplayabiliriz:

- Anonimliğin derecesini ve güvenilirliğini test etmek amacıyla yapılan saldırılar,
- Kurumları, şirketleri, organizasyonları, belirli bir kişiyi veya topluluğu zor durumda bırakmaya ve itibar riski yaratmaya yönelik saldırılar,
- Anonimliğin bozulması sonucu ortaya çıkacak kişisel verilerden ve elde edilebilecek değerlerden maddi veya manevi fayda sağlama amacıyla yapılan saldırılar.

Yukarıda sıralanan senaryoların farklılığına bağlı olarak saldırıları yürüten kullanıcıların profilleri ve erişim yetkileri de değişkenlik göstermektedir. Bu kişiler aşağıda listelenen örneklerdeki profillere sahip olabilirler:

- Kamuya açılmış veriye erişimi olan genel bir kullanıcı,
- Yazılım, istatistik, veri madenciliği konularında uzmanlaşmış bir profesyonel, akademisyen veya araştırmacı,
- Kuruluş, şirket, organizasyon içinde çalışan veya sistemlere erişim hakkı olan bir kullanıcı,
- Anonim hale getirilmiş veriyi kullanarak çalışan ancak diğer bazı verilere veya sistemlere erişimi olan kullanıcı,
- Açıklanmış /paylaşılmış veri kümesinde yer aldığını bildiği bir kişinin yakını, aile üyesi veya arkadaşı.
- Saldırıların sonucunda başarılı olunmuş ve anonimlik bozulmuşsa ortaya çıkan kişisel veriye dair üç farklı senaryo oluşmaktadır. Bu senaryolar;
- Gerçek kişinin kimliğinin tamamen ortaya çıkmış olması,
- Gerçek kişiye ait belli bir bilginin ortaya çıkmış olması,
- Bir kişiye dair varsayımsal bir bilginin ortaya çıkmış olması, olarak sayılabilir.

Kişinin kimliğinin tamamen ortaya çıkmış olması durumu, çoğunlukla saldırganın elindeki anonim hale getirilmiş veriyi elde ettiği veya erişiminin olduğu bir başka veri kümesiyle birleştirmesinden veya doğrudan tanımlayıcılar yerine kullanılan kod veya takma isimlerin kodlamalarının bozulmasından kaynaklanabilir. Böyle bir durumda gerçek kişinin doğrudan tanımlayıcılarına ulaşılır ve kimlik tamamen saptanabilir hale gelir.

Bazı hallerde kimlik tamamen tespit edilebilir hale gelmese de bir kişinin ilgili anonim hale getirilmiş veri kümesi içinde yer aldığını bilen bir kullanıcı anonim hale getirilmiş veri kümesinin dar bir tanımlama yapıyor olmasından ötürü o kişiye ait bir özelliğini ortaya çıkartabilir. Örneğin, bir hastanenin 20 yaşındaki tüm kadın hastalarına dair tek bir teşhis ve tedavi bilgisi paylaşıyor olması halinde, tanıdığı 20 yaşındaki kadının o hastanede tedavi edildiğini bilen bir kişi, tanıdığı kişinin hastalığını öğrenmiş olmaktadır. Bu halleri engelleyebilmek için hastanenin sadece 20 yaşındaki kadın hastalar yerine yaş aralığını ve cinsiyeti genişleterek ve teşhis ve tedavi bilgilerinin çeşitlenmesini sağlayacak önlemler alması ve tekil olarak belli bir kişinin ayırt edilebilme ihtimalini düşürmesi gerekmektedir.

Buna benzer şekilde, özellikle belli bir sınıf, grup veya topluluğa dair çok kesin ve çeşitliliği az olan tekil bilgilerin açıklanıyor veya paylaşılıyor olması halinde o gruba, sınıfa veya topluluğa mensup olduğu bilinen kişilerle ilgili varsayımsal sonuçlar çıkartılmasına mahal verilecektir. Örneğin; belli bir coğrafi bölgede yaşayan bireyler için bir kamu organının tek bir hastalığa dair yüksek oranlar paylaşmış olması o coğrafyada seyahat etmiş tüm insanlara dair varsayımlar yürütülmesini sağlayacaktır.

Bu kapsamda, 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 edilmelidir.