MSA MESLEKİ EĞİTİM VE TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

Versiyon:1-2019

1. Kişisel Verileri Saklama ve İmha Politikası'nın Amacı

İşbu Kişisel Verileri Saklama ve İmha Politikası'nın ("**Politika**") amacı, MSA Mesleki Eğitim ve Ticaret A.Ş. ("**Şirket**" veya "**MSA**")'de hukuka uygun olarak Kişisel Verilerin Korunması ve İşlenmesi Politikası uyarınca toplanan, işlenen ve muhafaza edilen kişisel verilerin ne kadar süre ile muhafaza edileceğine ve bu sürenin sonunda imha edilmesine ilişkin düzenlemelerin yapılmasıdır.

2. Kişisel Verileri Saklama ve İmha Politikası'nın Uygulanması ve Değişiklikler

Kişisel Verileri Saklama ve İmha Politikası, MSA Yönetim Kurulu tarafından yürürlüğe koyulacak olup, uygulanması Yönetim Kurulu tarafından görevlendirilen Kişisel Verileri Koruma Komisyonu tarafından takip edilir.

3. Tanımlar

Kişisel Verileri Saklama ve İmha Politikası'nın uygulanmasında:

KISALTMA	TANIM
Kanun:	6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
Kişisel Verileri Koruma Komisyonu:	MSA Yönetim Kurulunun kararı ile oluşturulan ve kişisel verilerin korunması ve işlenmesine ilişkin şirket içi işleyişten sorumlu Kişisel Verileri Koruma Komisyonunu,
Kişisel Verilerin Anonim Hale Getirilmesi:	Kişisel verilerin, başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
Kişisel Verilerin İmha Edilmesi:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kişisel Verilerin Silinmesi:	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kişisel Verilerin Yok Edilmesi:	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Politika:	Kişisel Verileri Saklama ve İmha Politikasını
Şirket/MSA:	MSA Mesleki Eğitim ve Ticaret A.Ş..
Yönetmelik:	28 Ekim 2017 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale getirilmesi Hakkında Yönetmelik'i ifade eder.

4. Kişisel Verilerin Kaydedildiği Ortamlar

Şirket, Kanun'a ve ilgili mevzuata uygun olarak ve Kişisel Verilerin Korunması ve İşlenmesi Politikası uyarınca gerçekleştirmekte olduğu kişisel veri işleme faaliyetleri kapsamında elde ettiği kişisel verileri, işleme amacının gerektirdiği ölçü ile sınırlı olmak kaydıyla muhafaza etmektedir. Bu

kapsamda, elde edilen kişisel veriler Şirket tarafından fiziki ve dijital/elektronik ortamlarda, gerekli tüm teknik ve idari güvenlik tedbirleri alınarak saklanmaktadır.

5. Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Hukuki, Teknik ve Diğer Sebepler

Şirket, kişisel veri içeren bilgi ve belgeleri, 6102 sayılı Türk Ticaret Kanunu, 633 sayılı Vergi Usul Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 4857 sayılı İş Kanunu, T.C. Sağlık Bakanlığı mevzuatı ve ilgili diğer mevzuattan doğan hukuki yükümlülüklerinin yerine getirilmesi ve Kanun 5. ve 6. maddelerinde yer alan ve Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda belirtilen diğer kişisel veri işleme şart ve amaçları kapsamında belirli süreler boyunca saklamakta olup, ilgili saklama süreleri işbu Politika'nın ekinde belirtilmektedir.

Kişisel veriler, Kanun ve Kişisel Verilerin Korunması ve İşlenmesi Politikası'na uygun olarak kişisel verilerin muhafaza edilmesini gerektiren sebeplerin ortadan kalkması halinde imha edilmektedir. Ayrıca, ilgili kişinin açık rızasına dayalı olarak saklanan kişisel veriler, rızanın ilgili kişi tarafından geri alınması halinde de derhal imha edilmektedir. İlgili kişinin Kanun'un 11. maddesinde yer alan hakları kapsamında, kişisel verilerinin silinmesi talebini Şirket'e iletmiş olduğu durumlarda, Kişisel Verileri Koruma Komisyonu tarafından söz konusu talep değerlendirilmekte ve Kanun'da belirtilen kişisel veri işleme şartlarının;

(i) tamamının ortadan kalkmış olduğunun tespit edilmesi halinde kişisel veriler usulüne uygun olarak imha edilmekte ve ilgili kişinin talebi en geç otuz gün içinde sonuçlandırılarak kendisine bilgi vermektedir.

(ii) tamamının ortadan kalkmış ve talebe konu olan kişisel verilerin üçüncü kişilere aktarılmış olduğunun tespit edilmesi halinde, Şirket söz konusu kişisel verileri imha etmekte ve bu durumu üçüncü kişilere bildirerek üçüncü kişiler nezdinde gerekli işlemlerin yapılmasını talep etmektedir.

(iii) tamamının ortadan kalkmamış olduğunun tespit edilmesi halinde, bu talep Şirket tarafından Kanun'un 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanmak kaydıyla en geç otuz gün içinde ilgili kişiye bildirilerek reddedilebilmektedir.

6. Özel Nitelikli Kişisel Veri İşleyen Veri Sorumluları Tarafından Alınması Gereken Yeterli Önlemler

Kişisel Verileri Koruma Kurulu, 31.01.2018 tarihinde verdiği karar doğrultusunda, özel nitelikli kişisel veri sorumluları tarafından alınması gereken yeterli önlemleri aşağıdaki şekilde belirlemiştir.

- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise; bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması, bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

Gerekmektedir.

<u>Özel Nitelikli Kişisel Verilerin İşlenmesi Süreçlerinde Yer Alan Çalışanlara Yönelik,</u>

(i) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi

(ii) Gizlilik sözleşmelerinin yapılması,

(iii) Verilene erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

(iv) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

(v) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterlerin iade alınması

Gerekmektedir.

7. Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesi ve Erişilmesinin Önlenmesi İçin Alınmış Teknik ve İdari Tedbirler

MSA, kişisel verilerin hukuka uygun işlenmesi ve güvenliğinin sağlanması amacıyla her türlü teknik ve idari tedbiri almakta; bu tedbirlere uyulması amacıyla Şirket personeline eğitimler vermekte ve periyodik aralıklarla denetim yapmaktadır.

Şirket, bünyesinde yer alan her bir birimin gerçekleştirdiği kişisel veri işleme süreçlerini ve aşamalarını analiz etmekte, gözden geçirmekte ve ilgili süreçlerde hukuka uygunluğun temini için gerekli aksiyonları almaktadır.

Teknik tedbirler bakımından Şirket'in kendisine ait bir bilgi teknolojileri birimi olmayıp, bu hususta Şirket harici bilgi güvenliği ekiplerinden destek alınmaktadır. Söz konusu bilgi teknolojileri firması Kanun bakımından "veri işleyen" sıfatını haizdir. Kişisel Verileri Koruma Komisyonu, bilgi teknolojileri firmasına Kanun ve ilgili mevzuata uygunluk bakımından alınan hizmet kapsamında ulaşılabilecek kişisel verilerin korunmasına ilişkin protokol akdetmiş olup, gerekli uyarılarda bulunmuştur.

Şirket'in söz konusu analiz ve çalışmalar ışığında almış olduğu idari ve teknik tedbirler, Kişisel Verilerin Korunması ve İşlenmesi Politikası, Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Politikası, Acil Durum Yönergesi, Kişisel Verileri Koruma Komisyonu'nun Görev ve Yetkilerine İlişkin Yönerge, Başvurularda İzlenecek Yöntem Yönergesi ve envanter kapsamında ayrıntılarıyla düzenlenmiştir.

8. Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Teknik ve İdari Tedbirler

MSA, kişisel verilerin hukuka uygun olarak silinmesi, yok edilmesi veya anonim hale getirilmesi için her türlü teknik ve idari tedbiri almakta olup, sahip olduğu teknolojik imkânlar ve bunların uygulama maliyetleri göz önünde bulundurularak, 9. maddede sayılanlar arasından en uygun yöntemleri kullanmaktadır.

Kişisel verilerin imhası ile ilgili olarak yapılan bütün işlemler kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanmaktadır.

9. Kişisel Verilerin İmhası

Kişisel Verilerin İmhası, verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi şeklinde üç farklı şekilde sağlanabilir. İmha işlemindeki amaç, kalan veriler ile gerçek kişiye ulaşabilmenin mümkün olmamasıdır. MSA, Kişisel Verilerin hukuka uygun olarak Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır.

9.1. Kişisel Verilerin Silinmesi

Tamamen veya kısmen otomatik yollarla işlenen Kişisel Verilerin silinmesi; söz konusu Kişisel Verilerin İlgili Kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

9.2. Kişisel Verilerin Yok Edilmesi

Yok Etme işlemi, MSA'nın verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve MSA bu verileri erişilemeyecek, tekrar kullanılamayacak ve tekrar geri getirilmesi mümkün olmayacak hale getirmekle yükümlüdür.

Yok Etme işlemleri sırasında MSA çalışanları ve ilgili departmanlar Kişisel Verileri Koruma Komisyonu'na yok edilecek ilgili verileri bildirmekle yükümlüdür, sonrasında ise MSA gerekli her türlü teknik ve idari tedbiri alacaktır.

9.3. Kişisel Verilerin Anonim Hale Getirilmesi

Anonim hale getirme işlemi, MSA'nın Kişisel Verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

10. Kişisel Verilerin İmha Edilme Yöntemleri

Şirket, Kurul tarafından aksine bir karar alınmadıkça, Yönetmelik gereği kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçmeye yetkilidir. İlgili kişinin bu yönde belirli bir talebi olması halinde, Şirket uygun yöntemi talep sahibine gerekçesini açıklamak suretiyle seçer.

10.1. Silme

Kişisel Verilerin Silinmesi sırasında MSA çalışanları aşağıdaki yöntemlerden uygun olanı seçerek silme işlemini gerçekleştirir

10.1.1. Bulut Sistemleri

Bulut sisteminde bulunan veriler silme komutu verilerek silinir. MSA, anılan işlemi gerçekleştirilirken İlgili Kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat eder.

a. Kâğıt Ortamında Bulunan Kişisel Veriler

Kâğıt ortamında bulunan Kişisel Veriler karartma yöntemi kullanılarak silinir. 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 İlgili Kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

b. Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosya işletim sistemindeki Silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde İlgili Kullanıcının erişim hakları kaldırılır. Anılan işlem gerçekleştirilirken İlgili Kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilir.

c. Taşınabilir Medyada Bulunan Kişisel Veriler

Flash tabanlı saklama ortamlarındaki Kişisel Veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinir.

d. Veri Tabanları

Kişisel Verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinir. Anılan işlem gerçekleştirilirken İlgili Kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

10.2. Yok Etme

Kişisel Verilerin Yok Edilmesi sırasında MSA çalışanları, aşağıdaki yöntemlerden uygun olanı seçerek Yok Etme işlemini gerçekleştirir.

a. Üzerine Yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine yazılımlarla en az 8 kez 0 ve 1'lerden oluşan rassal veriler yazılarak eski verinin okunamaz hale getirilmesi işlemidir.

b. Manyetize Etme

Manyetik medyanın yüksek değerde manyetik alanda fiziksel değişime sokularak üzerindeki verinin okunamaz hale getirilmesi işlemidir.

c. Fiziksel Yok Etme

Optik medya veya manyetik medyanın eritme, toz haline getirme, öğütme ve benzeri işlemlerle fiziksel olarak yok edilmesi işlemidir. Manyetize etme veya üzerine yazma metotlarının başarısız olduğu durumlarda uygulanabilir.

d. Bulut Sistemleri

Bulut sistemleri üzerinde tutulan Kişisel Verilerin yok etme bildiriminin anlaşmalı servis sağlayıcıya yapılmasının ardından Kişisel Verilerin şifreleme anahtarlarının tüm kopyalarının İmha edilmesi işlemidir.

e. Çevresel Sistemlerde Yer Alan Kişisel Verilerin Yok Edilmesi

Yazıcı, parmak izi ünitesi, kapı giriş turnikesi gibi sistemler içerisinde yer alan ve Kişisel Verileri barındıran, mevcut ise iç ünite, mevcut değil ise tüm cihaz üzerinde üzerine yazma, manyetize etme veya fiziksel yok etme uygulanarak yapılması gereken yok etme işlemidir. Bu tip yok etme işlemlerinin, cihazların yedekleme, bakım ve benzeri işlemlere tabi olmasından önce uygulanması zorunludur.

f. Kâğıt ve Mikrofiş Ortamlarında Yer Alan Kişisel Verilerin Yok Edilmesi

Söz konusu ortamlardaki Kişisel Veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür.

Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan Kişisel Verilerin ise bulundukları elektronik ortama göre yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

10.3. Anonim Hale Getirme

Anonim Hale Getirme işleminin uygulanması sonucunda elde edilen veriler Veri Öznesinin kimliğinin saptanabilmesinin engeller veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybeder.

MSA, bir Kişisel Verinin Silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar vermesi durumunda için aşağıdaki şartları yerine getirir:

a. Anonim Hale Getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması,

b. Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması,

c. Anonim Hale Getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Yukarıda sayılan riskler sebebiyle MSA, Anonim Hale Getirdiği veri kümeleri üzerinde düzenli kontroller yapar ve anonimliğin korunduğundan emin olur.

Aşağıda belirtilen Anonim Hale Getirme yöntemleri uygulanırken MSA tarafından verinin niteliği, büyüklüğü, fiziki ortamlarda bulunma yapısı, çeşitliliği, sağlanmak istenen fayda / işleme amacı, işleme sıklığı, aktarılacağı tarafın güvenilirliği, Anonim Hale Getirilmesi için harcanacak çabanın anlamlı olması, anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı, dağıtıklık/merkezilik oranı, kullanıcıların ilgili veriye erişim yetki kontrolü, anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcanacak çabanın anlamlı olması ihtimalini dikkate alınır.

Bir veriyi Anonim Hale Getiren MSA, 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 eder.

Kişisel Verilerin Anonim Hale Getirilmesi sırasında MSA, çalışanları aşağıdaki yöntemlerden uygun olanı seçerek Anonim Hale Getirme işlemini gerçekleştirir:

10.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan yöntemlerde veri kümesinin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır.

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.

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.

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. Genelleştirme işlemi sonucunda elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

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.

10.3.2. 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 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.

10.3.3. 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 indirerek veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a. K-Anonimlik

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

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.

11. Kişisel Verileri İmha Süreçlerinde Yer Alanların Unvanları, Birimleri ve Görev Tanımları

Kişisel verilerin imhası, Şirket bünyesinde kurulan ve kişisel verilerin hukuka uygun olarak işlenmesini temin etmekle görevli olan Kişisel Verileri Koruma Komisyonu tarafından gerçekleştirilir.

Kişisel Verileri Koruma Komisyonu, işbu Politika'da belirtilen belgelerin belirlenen sürelerde imha edilmesi işini, Şirket içinden üçüncü kişilere devredebilmekle birlikte böyle bir devir halinde Kişisel Verileri Koruma Komisyonu'nun imha sürecini denetim yükümlülüğü devam edecektir. Böyle bir durumda, imha etme görev ve yetkisinin devredildiği kişi/kişilerin adı soyadı, unvan, birim ve görev tanımları gibi bilgileri her bir imha sürecinde yazılı olarak tutulacak olup, söz konusu kayıtlar Genel Müdür'e bildirilecektir. Kişisel Verileri Koruma Komisyonu, imha edilecek belgelerin "özel nitelikli kişisel veri" ihtiva etmesi halinde, bu durumu da imha etme işini devrettiği üçüncü kişi/kişilere bildirir. Periyodik imha süreçleri, Kişisel Verilerin Korunması Komisyonu tarafından belirlenen görevlilerden en az iki kişi tarafından müştereken gerçekleştirilmekte ve imha edilen kişisel verilerin herhangi bir kopyasının alınmadığı hususunda bu kişilerden yazılı taahhüt alınmaktadır.

12. Periyodik İmha Süreleri

Şirket, işlemiş olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

Periyodik imhanın gerçekleştirileceği zaman aralığı 6 ay olup, Şirket'in işlemekte olduğu kişisel veriler bakımından, verilerin saklanma ve imha süreleri ile saklama sürelerinin hukuki dayanaklarına ilişkin mevzuat hükümleri aşağıdaki tabloda gösterilmiştir.

13. Güncelleme

İşbu Politika gerektiğinde Kanun ve ilgili mevzuattaki değişikliklere ve Kurul kararlarına istinaden revize edilecektir.

VERİ KATEGORİSİ	SAKLAMA VE İMHA SÜRESİ	HUKUKİ DAYANAK
Şirket çalışanlarına ilişkin kişisel veriler	İş ilişkisi devam ettiği süre boyunca ve işten çıkış tarihini takiben 10 yıl (çalışanların kişisel sağlık dosyaları işten çıkış tarihini takiben 15 yıl) boyunca saklanır ve bu süre sonunda imha edilir.	6098 sayılı Türk Borçlar Kanunu, 4857 sayılı İş Kanunu, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Hizmetleri Yönetmeliği ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat.
Şirketin mal ve/veya hizmet almakta olduğu tedarikçilere ve tedarikçi temsilcilerine ilişkin kişisel veriler	Ticari ilişki devam ettiği sürece ve ticari ilişkinin bitişini takiben 10 yıl boyunca saklanır ve bu süre sonunda imha edilir.	6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat.
Öğrenci adaylarına ilişkin kişisel veriler	Periyodik imha süresine uygun olarak 6 ay boyunca saklanır ve bu süre sonunda imha edilir.	6102 sayılı Türk Ticaret Kanunu, 5237 sayılı Türk Ceza Kanunu, 6098 sayılı Türk Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat
Öğrencilere ilişkin kişisel veriler	Taraflar arasındaki ilişki devam ettiği sürece ve işbu ilişkinin bitişini takiben 10 yıl boyunca saklanır ve bu süre sonunda imha edilir.	6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat
Kapalı Devre Görüntüleme Sistemleri vasıtasıyla elde edilen kamera kayıtları	Adli vakıa veya resmi kurum talebi bulunmuyor ise 6 ay süreyle saklanır ve bu süre sonunda imha edilir.	6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak veri sorumlusu Şirket'in meşru menfaatleri kapsamında makul süre ile saklanmaktadır.
Şirket içinde unutulan ve kişisel veri içeren eşyalar	Eşya sahibine ulaşılamamış ise, [*en çok 6*] ay süre ile muhafaza edilir. Süre bitiminde bir tutanak ile yok edilir.	6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak veri sorumlusu Şirket'in meşru menfaatleri kapsamında 6 aylık makul süre ile saklanmaktadır.

İş ve Staj Başvuruları-Özgeçmişler	Başvurular, ilgili kişinin açık rızası ile sisteme işlenir ve 2 (iki) ay süreyle saklanır.	Başvuru sahibinin açık rızası doğrultusunda saklanmaktadır.
E-posta verileri	Hizmet ilişkisi süresince ve hizmet ilişkisinin bitimini takiben 10 yıl boyunca saklanır ve bu süre sonunda imha edilir.	
Muhasebe, finans, vergi departmanındaki kişisel veriler	213 sayılı Vergi Usul Kanunu uyarınca 5, 6102 sayılı Türk Ticaret Kanunu uyarınca 10 yıl boyunca saklanır ve bu süre sonunda imha edilir.	6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat.