

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ VE POLİTİKA'NIN HAZIRLANMA AMACI

İşbu Kişisel Veri Saklama ve İmha Politikası ("**Politika**"), 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**" ya da "**Kanun**") ve Kanun'un ikincil düzenlemesini teşkil eden 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") uyarınca yükümlülüklerimizin yerine getirilmesi ve kişisel verilerin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi işlemi ile silme, yok etme ve anonim hale getirme işlemleri için dayanak olarak kullanılması ve bu işlemler hakkında ilgili kişilerin bilgilendirilmesi amacıyla, veri sıfatıyla **İSTANBUL GALATA ÜNİVERSİTESİ AĞIZ VE DİŞ MERKEZİ** (Bundan sonra **İGAU ADSM** olarak yazılacaktır.) tarafından hazırlanmıştır.

2. KAPSAM

Bu politika, kurum nezdinde tutulan, kurumun tüm çalışanlarını, danışmanlarını ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerini, tedarikçilerini ve kurumun diğer hukuki ilişkiye girdiği gerçek ve tüzel kişileri, bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri kapsamaktadır. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.

3. TANIMLAR

Kısaltma	Tanım
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
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 kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi 2veya anonim hale getirilmesi.

Kanun/KVKK	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 Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
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.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.

Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	28 Ekim 2017 tarihinde Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

4. KURALLAR

İGAU ADSM tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilmektedir:

1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'un 4. maddesinde sayılan ilkeler¹ ile 12. maddesi kapsamında alınması gereken ve işbu Politikanın 6.2. maddesinde belirtilen teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.
2. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler **İGAU ADSM** tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.
3. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilmektedir. Ancak, İlgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.
4. Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler **İGAU ADSM** tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından İGAU ADSM başvurulması halinde;
 - a. İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir,
 - b. Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.

a)Hukuk ve dürüstlük kurallarına uygun olma, b)Doğru ve gerektiğinde güncel olma, c)Belirli, açık ve meşru amaçlar için işlenme, d)İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, e)İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

5. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŐKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, İGAU ADSM tarafından özellikle (i) hizmet faaliyetlerin sürdürülebilmesi, (ii) hukuki yükümlölüklerin yerine getirilebilmesi, (iii) çalışan haklarının ve yan haklarının planlanması ve ifası ile (iv) müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diđer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aŐağıdaki gibidir:

- a. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- b. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla İGAU ADSM meŐru menfaatleri için saklanmasının zorunlu olması,
- d. Kişisel verilerin İGAU ADSM 'nin herhangi bir hukuki yükümlölüğünü yerine getirmesi amacıyla saklanması,
- e. Mevzuatta kişisel verilerin saklanmasının açıkça öngörölmesi,
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması. Yönetmelik uyarınca, aŐağıda sayılan hallerde veri sahiplerine ait kişisel veriler, İGAU ADSM tarafından resen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

Yönetmelik uyarınca, aŐağıda sayılan hallerde veri sahiplerine ait kişisel veriler, İGAU ADSM 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 deđiştirilmesi veya ilgası,
- 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 gerçekleştiđi hallerde, ilgili kişinin 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 baŐvuruyu reddetmesi, verdiĐi cevabın yetersiz bulunması veya Kanun'da öngörölen süre içinde cevap vermemesi hallerinde; Kurul'a Őikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,

- g. KiŐisel verilerin saklanması gerektiren azami sürenin geçmiŐ olmasına raĐmen, kiŐisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir Őartın mevcut olmaması.

6. SAKLAMA VE İMHA SÜRELERİ

İGAU ADSM tarafından KVKK ve diĐer ilgili mevzuat hükümlerine uygun olarak elde edilen kiŐisel verilerinizin saklama ve imha sürelerinin tespitinde aŐaĐıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır:

1. Mevzuatta söz konusu kiŐisel verinin saklanmasına iliŐkin olarak bir süre öngörölmüŐ ise bu süreye riayet edilir. Anılan sürenin sona ermesi akabinde veri hakkında 2. bent kapsamında iŐlem yapılır.
2. Söz konusu kiŐisel verinin saklanmasına iliŐkin olarak mevzuatta öngörölen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanmasına iliŐkin olarak herhangi bir süre öngörölmemiŐ olması durumunda sırasıyla;
 - a. KiŐisel veriler, KVKK'nın 6. maddesinde yer alan tanımlama baz alınarak, kiŐisel veriler ve özel nitelikli kiŐisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduĐu tespit edilen tüm kiŐisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliĐi ve saklanmasının İGAU ADSM nezdindeki önem derecesine göre belirlenir.
 - b. Verinin saklanmasının KVKK'nın 4. maddesinde belirtilen ilkelere uygunluĐu örneĐin; verinin saklanmasında İGAU ADSM' nin meŐru bir amacının olup olmadıĐı sorgulanır. Saklanmasının KVKK'nın 4. maddesinde yer alan ilkelere aykırılık teŐkil edebileceĐi tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
 - c. Verinin saklanmasının KVKK'nın 5. ve 6. maddelerinde öngörölmüŐ olan istisnalardan hangisi/hangileri kapsamında deĐerlendirilebileceĐi tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.

İGAU ADSM tarafından tespit edilen saklama, imha ve periyodik imha sürelerine, politikanın ekinde (Ek-2) yer alan "KiŐisel Veri İŐleme Envanteri"nden ulaŐabilirsiniz.

Saklama süresi dolan kiŐisel veriler, Politikanın ekinde (Ek-2) yer alan imha süreleri

çerçevesinde, 6 aylık periyodlarla politikada yer verilen usullere uygun olarak imha edilir.

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

7. KİŐİSEL VERİLERİN İGAU ADSM TARAFINDAN SAKLANMASI VE İMHASI USULLER

I. KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, İGAU ADSM tarafından aŐağıdaki tabloda listelenen ortamlarda baŐta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliđi prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:

- Sunucular
- Çıkarılabilir bellekler (USB, Hafıza Kart vb.)
- Bilgi güvenliđi cihazları (güvenlik duvarı, günlük kayıt dosyası, antivirüs vb.)
- Kişisel bilgisayarlar,
- Optik diskler (CD, DVD vb.)
- Yazıcı, tarayıcı, fotokopi makinesi,
- Yazılımlar (ofis yazılımları, devlet kurumlarına ait yazılımlar)
- Mobil cihazlar (telefon, tablet vb.),
- TrTek (Hastane İşletim Sistemi)

Fiziksel ortamlar:

- Kâğıt
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)
- Yazılı, basılı, görsel ortamlar
- Kilitli Dolaplar

II. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nın 12. Maddesindeki ilkeler çerçevesinde, İGAU ADSM tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

1. İdari Tedbirler:

İGAU ADSM idari tedbirler kapsamında;

- a. Saklanan kişisel verilere Kurum içi erişimi iş tanımı gereği erişmesi gerekli personel 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 personel istihdam eder ve personeline 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.

2. Teknik Tedbirler:

İGAU ADSM teknik tedbirler kapsamında;

- 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 kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar.
- d. Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak 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. Kişisel verilerin güvenli olarak saklanmasını sağlayan yedekleme programları kullanılmaktadır.

III. PERSONEL

Kişisel veri saklama ve imha sürecinde yer alan personelin unvanlarına, birimlerine ve görev tanımlarına işbu Politika'nın EK-1'nde yer alan listeden ulaşabilirsiniz.

IV. KİŞİSEL VERİLERİN İMHA USULLERİ

İGAU ADSM tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde İGAU ADSM tarafından resen yahut İlgili Kişinin başvurusu üzerine yine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen teknikler ile imha edilecektir.

a. Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri:

İGAU ADSM tarafından kişisel verilerin silinmesi ve yok edilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır:

Kişisel Verilerin Silinmesi:

Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

- Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılmaz hale getirilecek biçimde güvenli olarak silinir.

Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması: Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

Kişisel Verilerin Yok Edilmesi:

De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.

Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Kağıt ve mikrofiş ortamındaki verilerin yok edilmesi de, başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.

Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve

yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

Yukarıda sayılan durumlar gerçekleşmesi sırasında İGAU ADSM; KVKK, Yönetmelik ve ilgili diğer mevzuat hükümlerine veri güvenliğinin sağlanması amacıyla tam uyum sağlamakta ve gerekli tüm idari ve teknik tedbirleri almaktadır.

b. Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

İGAU ADSM tarafından kişisel verilerin anonim hale getirilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır:

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.

Örneğin, aşağıdaki tabloda veri setindeki değişkenlerden yüksek derecede betimleyici olan veri gruplarının çıkartılması ile anonimleştirme sağlanmıştır.

Çalışanın Adı	Yaşadığı İl	Yaşadığı İlçe	Yaşadığı Mahalle	Pozisyonu	Aylık Geliri	Kıdemi (Yıl)
Merve	İstanbul	Sarıyer	Alibey	Doktor	9750 TL	12
Özge	Ankara	Şişli	Söğütözü	İşçi	1800TL	5
Ali	İzmir	Alsancak	Kordon	Mimar	6500TL	6
Kerem	İstanbul	Beyoğlu	Gültürk	Mühendis	5650 TL	3
Eda	İstanbul	Bakırköy	Abbasağa	İşçi	6550TL	4

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir. Örneğin, bir Kurumte 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, Kurumin 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.

Örneğin, bir işyerinde çalışan personelin işyerindeki çalışma yılının 5 yıldan az, 5 ile 10 yıl arasında veya 10 yıldan çok olmasına göre (çok deneyimli), (deneyimli) ya da (deneyimsiz) olarak birleştirilerek anonim hale getirilebilir:

Çalışanın Pozisyonu	Yaşı	Cinsiyeti	Aylık Geliri	Kıdemi (Yıl)
Bilgi İşlem Uzmanı	31	E	5600 TL	9
Sekreter	26	K	1800 TL	4
Müdür Yardımcısı	28	E	3800 TL	8
Şef	39	K	5500 TL	13
Memur	43	K	1900 TL	8
Avukat	32	E	8500 TL	7

İkinci örnekte ise kıdem değişkenine belirlenen yıl ölçütüne göre alt ve üst sınır kodlaması uygulanarak üç kategoriye halinde anonimleştirilmiş şeklini göstermektedir.

Çalışanın Pozisyonu	Yaşı	Cinsiyeti	Aylık Geliri	Kıdemi
Bilgi İşlem Uzmanı	43	E	5600 TL	Çok Deneyimli
Sekreter	23	K	1800 TL	Deneyimsiz
Müdür Yardımcısı	31	E	2800 TL	Deneyimli

12/18

Şef	39	K	5500 TL	Çok Deneyimli
Memur	43	K	1900 TL	Deneyimsiz
Avukat	29	E	8500 TL	Deneyimli

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.

Çalışanın Pozisyonu	İkamet Adresi	Çocuğu	Aylık Geliri	Kıdem i(Yıl)
Hizmetli	Atakent Mah. Papatya Sok. 25/3 Şirinevler, İstanbul	Var	1750 TL	12
İşçi	Söğütözü Mah. Güneş Sok. 32/3 Hadımköy, Ankara	Yok	1800TL	8
Doktor	Kozyatağı Mah. Kaya Sok. 32/6 Beylikdüzü, İstanbul	Yok	8500TL	7
Memur	Türkali Mah. Konak Sok. 14/7 Kadıköy, İstanbul	Var	1550 TL	5

Aşağıdaki tabloda veri türetme yoluyla anonimleştirme yöntemi uygulanmıştır:

Çalışanın Pozisyonu	İkamet Edilen Bölge	Çocuğu	Aylık Geliri	Kıdem i(Yıl)
Hizmetli	İstanbul Avrupa Yakası	Var	1750 TL	12
İşçi	İstanbul Avrupa Yakası	Yok	1800TL	8
Doktor	İstanbul Avrupa Yakası	Yok	8500TL	7
Memur	İstanbul Anadolu Yakası	Var	1550 TL	5

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 yapılır ise, 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.

Örneğin, aşağıdaki tabloda 'Yaş: 45', 'Cinsiyet: Kadın', 'İl: Ankara' verileri bulunan kişilere ait gelir bilgisi 'Yaş: 30', 'Cinsiyet: Kadın', 'İl: İzmir' olanlar ve 'Yaş: 25', 'Cinsiyet: Erkek' 'İl: İzmir' olanların gelir bilgileri ile 'Yaş:35', 'Cinsiyet: Erkek' 'İl: İstanbul' olanların gelir bilgileri birbirleri içerisinde değiştirilerek veri tabanı dönüştürülmüştür.

Yaş	Cinsiyet	İl	Gelir
45	Kadın	Ankara	70.000
30	Kadın	İzmir	55.000
25	Erkek	İzmir	37.000
35	Erkek	İstanbul	22.000
55	Erkek	İzmir	15.000

Aşağıdaki tabloda veri değiş tokuş yöntemi uygulanmıştır:

14/18

YaŐ	Cinsiyet	İl	Gelir
45	Kadın	Ankara	23.000
30	Kadın	İzmir	17.000
25	Erkek	İzmir	58.000
35	Erkek	İstanbul	42.000
55	Erkek	İzmir	31.000

KVKK'nın 28. maddesi uyarınca, kiŐisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araŐtırma, planlama ve istatistik gibi amaçlarla iŐlenmesi durumunda bu durum Kanun kapsamı dıŐında kalacak ve açık rıza temini gerekmeyecektir.

DİŐER HUSUSLAR

KVKK ve ilgili diŐer mevzuat hükümleri ile iŐbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diŐer mevzuat hükümleri uygulanacaktır.

İGAU ADSM tarafından hazırlanan iŐbu Politika 30.07.2021 tarihinde yürürlüŐe girmiŐtir. Politika'da deŐiŐiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doŐrultuda güncellenecektir. Güncelleme tablosu Ek-3'te yer almaktadır.

İGAU ADSM

EK-1

PERSONEL UNVAN, BİRİM VE GÖREV LİŐTESİ

PERSONEL	GÖREV	SORUMLULUK
----------	-------	------------

Avukat	Veri İşleyen Sıfatıyla İş Ortağı HukukBürosu- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kurumsal Direktörü	Kurumsal İletişim Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İnsan Kaynakları Müdürü	İnsan Kaynakları Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	Bilgi İşlem Müdürlüğü - Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe Müdürü	Mali İşler Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İdari İşler Müdürü		Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

EK-2

SAKLAMA VE İMHA SÜRELERİ TABLOSU

Kurum tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde süreç bazında tespit edilmiş olup, anılan envantere ilişkin bilgiler aşağıdaki tabloda sunulmuştur.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kurumsal İletişim Faaliyetlerinin Planlanması ve İcrası	İş ilişkisinin sona ermesine müteakip 10 yıl	Veri sahibinin imha başvurusunu takiben 30 gün içerisinde
Genel Kurul İşlemleri	Burs ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İhale/işyeri açma/bakanlıklar-müşteşarlıklar evrak hazırlama süreçleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşmelerin hazırlanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İşe alım	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Bordrolama	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özel sağlık ve ferdi kaza sigorta poliçelerinin hazırlanması	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara araç tahsis edilmesi	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Log/Kayıt/Takip Sistemleri	3 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ana veri oluşturma süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

Kurum ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kurum kredi kartı tahsisi	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Odeme işlemleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel Mali Süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşme sürecinin bir bölümü ve sözleşmenin muhafazası	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kaza Raporlama	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Toplantı notlarının, katılımcılar ile paylaşılması	5 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Doküman hazırlanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Acil Durum Hazırlıkları	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Eğitim kayıtlarının dosyalanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde