

**BANDO KAYIŞ SANAYİ VE TİCARET
(TÜRKİYE) ANONİM ŞİRKETİ**

**KİŞİSEL VERİLERİN SAKLAMA VE
İMHA POLİTİKASI**

(13 Kasım 2018, *ver 1*)

İÇİNDEKİLER

1. GİRİŞ VE POLİTİKA’NIN HAZIRLANMA AMACI	3
2. TANIMLAR.....	3
3. İLKELER	4
4. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR.....	5
5. SAKLAMA VE İMHA SÜRELERİ	6
6. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI USULLERİ	7
I. KAYIT ORTAMLARI	7
I. TEKNİK VE İDARİ TEDBİRLER	8
a. İdari Tedbirler:	8
b. Teknik Tedbirler	9
II. PERSONEL	9
III. KİŞİSEL VERİLERİN İMHA USULLERİ	9
7. DİĞER HUSUSLAR.....	14
EK-1	15
PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ	15
EK-2	16
SAKLAMA VE İMHA SÜRELERİ TABLOSU.....	16
EK-3	18
GÜNCELLEME TABLOSU	18

**BANDO KAYIŞ SANAYİ VE TİCARET (TÜRKİYE)
ANONİM ŞİRKETİ.**

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 yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla BANDO KAYIŞ SANAYİ VE TİCARET (TÜRKİYE) ANONİM ŞİRKETİ (“**BANDO**” ya da “**Şirket**”) tarafından hazırlanmıştır.

2. TANIMLAR

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 veya 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,
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	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.

--	--

3. İLKELER

BANDO 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 ilkeler 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 BANDO 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 re'sen 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 işleme şartlarının tamamının ortadan kalkması halinde, kişisel veriler BANDO tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından BANDO'ya 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.

4. SAKLAMA VE İMHAYI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait kişisel veriler, BANDO tarafından özellikle (i) ticari faaliyetlerin sürdürülebilmesi, (ii) hukuki yükümlülüklerin 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 diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

Saklamayı gerektiren sebepler aşağıdaki 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 BANDO'nun meşru menfaatleri için saklanmasının zorunlu olması,
- d. Kişisel verilerin BANDO'nun herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- e. Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

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

- a. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya 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 gerçekleştiği 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 başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- g. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

5. SAKLAMA VE İMHA SÜRELERİ

BANDO tarafından KVKK ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha sürelerinin tespitinde aşağıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır:

1. Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Anılan sürenin sona ermesi akabinde veri hakkında 2. bent kapsamında işlem yapılır.
2. Söz konusu kişisel verinin saklanmasına ilişkin olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;
 - a. Kişisel veriler, KVKK'nın 6. maddesinde yer alan tanımlama baz alınarak, kişisel veriler ve özel nitelikli kişisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının BANDO nezdindeki önem derecesine göre belirlenir.
 - b. Verinin saklanmasının KVKK'nın 4. maddesinde belirtilen ilkelere uygunluğu

örneğin; verinin saklanmasında BANDO’ın meşru bir amacının olup olmadığı sorgulanır. Saklanmasının KVKK’nın 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.

- c. Verinin saklanmasının KVKK’nın 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği 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.

BANDO tarafından tespit edilen saklama, imha ve periyodik imha sürelerine, işbu Politika’nın ekinde (Ek-2) yer alan “Kişisel Veri İşleme Envanteri”nden ulaşabilirsiniz.

Saklama süresi dolan kişisel veriler, işbu Politika’nın ekinde (Ek-2) yer alan imha süreleri çerçevesinde, 6 aylık periyodlarla işbu Politika’da 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, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

6. KİŞİSEL VERİLERİN BANDO TARAFINDAN SAKLANMASI VE İMHASI USULLERİ

I. KAYIT ORTAMLARI

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

Elektronik ortamlar:

- EXCHANGE SERVER
- TIGER LOGO – BORDRO

Fiziksel ortamlar:

- Birim Dolapları
- ARŞİV

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, BANDO tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

a. İdari Tedbirler:

BANDO idari tedbirler kapsamında;

- a. Saklanan kişisel verilere Şirket 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 kişilerle çalışır 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.

b. Teknik Tedbirler:

BANDO 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 olarak sistem zafiyetlerinin kontrolünü sağlar.
- e. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.
- f. Kişisel verilerin yok edilmesi geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlanır.
- g. Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur.

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

BANDO tarafından KVKK ve diğer ilgili mevzuata uygun olarak elde edilen kişisel veriler Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının ortadan kalkması halinde BANDO tarafından re'sen 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:

BANDO 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 kullanılamaz 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 BANDO; 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:

BANDO 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.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademedeki 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.

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

birleřtirilmesiyle anonim hale getirilmektedir.

Genelleřtirme: Veri toplulařtırma yöntemi ile birçok veri toplulařtırılmakta ve kişisel veriler herhangi bir kişiyle iliřkilendirilemeyecek hale getirilmektedir. Örneđin; alıřanların yařlarının tek tek göstermeksizin X yařında Z kadar alıřan bulunduđunun ortaya konulması.

Global Kodlama: Veri tütretme yöntemi ile kişisel verinin içeriđinden daha genel bir içerik oluřturulmakta ve kişisel verinin herhangi bir kişiyle iliřkilendirilemeyecek hale getirilmesi sađlanmaktadır. Örneđin; dođum tarihleri yerine yařların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Deđer Düzensizliđi Sađlayan Anonim Hale Getirme Yöntemleri

Deđer düzensizliđi sađlayan anonim hale getirme yöntemlerinde deđer düzensizliđi sađlamayanların aksine kişisel veri gruplarında bazı verilerin deđiřtirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda dođrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sađlanarak veriden beklenen fayda sađlanmaya devam edilebilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ađırlıklı olduđu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneđin, kilo deđerlerinin olduđu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerek deđerlerin görüntülenmesi engellenmiř ve veriler anonimleřtirilmiř olur.Sapma her deđere eřit ölçüde uygulanır.

Mikro Birleřtirme: Mikro birleřtirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüđe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen deđer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleřtirme sađlanmış olacaktır.

Veri Deđiř Tokuşu: Veri deđiř tokuşu yönteminde saklanan veriler içerisinden seilen iftler arasında bir deđiřkenin deđerleri birbiri ile deđiřtirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile deđiřtirilerek veri tabanının dönüřtürülmesidir.

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

7. DİĐER HUSUSLAR

KVKK ve ilgili diđer mevzuat h k mleri ile iřbu Politika arasında uyumsuzluk olması halinde,  ncelikle KVKK ve ilgili diđer mevzuat h k mleri uygulanacaktır.

BANDO tarafından hazırlanan iřbu Politika ilgili kanunun uygulama tarihinde y r rl ge girmiřtir. Politika'da deęiřiklik olması durumunda, Politika'nın y r rl k tarihi ve ilgili maddeler bu doęrultuda g ncellenecektir. G ncelleme tablosu Ek-3'te yer almaktadır.

BANDO KAYIŐ SANAYİ VE TİCARET (T RKİYE) ANONİM ŐİRKETİ

EK-1

PERSONEL UNVAN, BİRİM VE G REVLİSTESİ

PERSONEL	G�REVLİ	SORUMLULUK
-----------------	----------------	-------------------

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
Mali İşler 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

EK-2

SAKLAMA VE İMHA SÜRELERİ TABLOSU

Şirket tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde süreç bazında tespit edilmiş aşağıda örnekleme yöntemiyle belirlenmiş, gerektiğinde ekleme yapılacaktır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
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
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	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
Ödeme işlemleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel Finansman Süreçleri	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

EK-3

GÜNCELLEME TABLOSU

İşbu Politika'da yapılan değişiklikler aşağıdaki tabloda yer almaktadır.

GÜNCELLEME TARİHİ	DEĞİŞİKLİKLERİN KAPSAMI
13.11.2018	Yayın Taslağı