

PENELOPE ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKA

İşbu Politikanın hazırlanma amacı 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin işlenmesi, saklanması ve imhasını belirleyen ilkelerin tespiti, saklama ve imhaya ilişkin usul ve esaslar ile sürelerin belirlenmesi kayıt ortamları ile teknik imkanların ve ilgili personelin unvan, birim ve görevlerinin açıklanmasını sağlamaktan ibarettir.

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 Gazetede 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 veri sorumlusu sıfatıyla Penelope A.Ş. (“Penelope” ya da “Şirket”) tarafından hazırlanmıştır.

2. TANIMLAR:

Kısaltmalar ve Tanımlar:

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	Kişisel Veri Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Verilerin İşlenmesi	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.

3. İLKELER:

Penelope A.Ş. 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 (1.Hukuk ve dürüstlük kurallarına uygun olma, 2.Doğru ve gerektiğinde güncel olma, 3.Belirli, açık ve meşru amaçlar için işleme, 4.İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, 5.İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.) 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 Penelope 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 Penelope tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından Penelope'ye 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:

- 4.1. Veri sahiplerine ait kişisel veriler, Penelope A.Ş. tarafından özellikle; ticari faaliyetlerin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması ve ifası ile 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 Penelope'nin meşru menfaatleri için saklanması zorunlu olması,*
- d. *Kişisel verilerin Penelope'nin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,*
- e. *Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,*
- f. *Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.*

4.2.Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, Penelope 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. maddesinin2 (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 şikâyette 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 kılabilecek herhangi bir şartın mevcut olmaması,*

5. SAKLAMA VE İMHA SÜRELERİ:

Penelope A.Ş. 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 saklanması ile ilgili olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanması ile ilgili 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 saklanması Penelope A.Ş. nezdindeki önem derecesine göre belirlenir.*
- b. *Verinin saklanmasının KVKK. 4. maddesinde belirtilen ilkelere uygunluğu örneğin; verinin saklanmasında Penelope'nin meşru bir amacının olup olmadığı sorgulanır. Saklanmasının KVKK. 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.*
- c. *Verinin saklanmasının KVKK. 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.*

Penelope A.Ş. tarafından tespit edilen saklama, imha ve periyodik imha sürelerine, işbu Politikanın ekinde (Ek-2) yer alan "Kişisel Veri İşleme Envanteri" nden ulaşabilirsiniz.

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

6. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI USULLERİ:

6.1.KAYIT ORTAMLARI:

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

1. Elektronik ortamlar:

- MICROSOFT EXCHANGE SERVER (MAILLER)
- TIGER LOGO – BORDRO
- SQL TABANLI FİRMAMIZ TARAFINDAN GELİŞTİRİLEN PROGRAMLAR
- FİRMAMIZ BÜNYESİNDE BULUNA SERVERLAR
- QNAP YEDEKLEME ÜNİTESİ
- USB HARİCİ DİSK

2. Fiziksel ortamlar: • Birim Dolapları • ARŞİV

6.2.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. 12. maddesindeki ilkeler çerçevesinde, Penelope tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır.

1. İdari Tedbirler:

Penelope 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 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:

Penelope 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.

6.3.PERSONEL:

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

6.4.KİŞİSEL VERİLERİN İMHA USULLERİ:

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

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

1. Kişisel Verilerin Silinmesi:

1.1.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.

1.2.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.

1.3.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.

2. Kişisel Verilerin Yok Edilmesi:

2.1. 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.

2.2. 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.

2.3. 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 Penelope; KVKK, Yönetmelik ve ilgili diğer mevzuat hükümlerine veri güvenliğinin sağlanması amacıyla tam uyum sağlamak ve gerekli tüm idari ve teknik tedbirleri almaktadır.

b. Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

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

1. 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. Bu yöntem ile yüksek derecede çalışan kişinin isim ve adres kaydı belirtilmeksizin betimleme yapılmaktadır.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarımlar saklanan veriler anonim hale getirilmektedir.

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 birleştirilmesiyle anonim hale getirilmektedir.

Deneyimli Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.

Global Kodlama: Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır.

2. 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.

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.

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.

KVKK. 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

7. DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır.

Penelope A.Ş. tarafından hazırlanan işbu Politika 01.07.2019 tarihinde yürürlüğe girmiştir. Politikada değişiklik olması durumunda, Politikanın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

EK-1

PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ PERSONEL GÖREV SORUMLULUK

PERSONEL	GÖREV	SORUMLULUK
Mesul Müdür	Üretim 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 Teknolojileri 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
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
Üretim Müdürü	Üretim 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

SAKLAMA VE İMHA SÜRELERİ TABLOSU

Şirket tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde süreç bazında tespit edilmiştir

Süreç	Saklama Süresi	İmha Süresi
Kurumsal İletişim Faaliyetlerinin Planlanması ve İcrası	İş ilişkisinin sona ermesine müteakip 10 yıl	Veri sahibinin imha başvurusunu takiben 30 gün içerisinde
Genel Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme/icra bilgi talepleri	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
İş Sağlığı ve Güvenliği Uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özel salık ve ferdi kaza sigorta poliçelerinin hazırlanması	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara araç tahsisi	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Log/Kayıt/Takip Sistemleri	1 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
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirkete ait kart/kredi kartı tahsisi	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ödeme İşlemleri	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
Sözleşme sürecinin bir bölümü ve sözleşmenin muhafazası	İş ilişkisinin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kaza Raporlama	Ceza Zamaşımı süresi dikkate alınarak en az 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Toplantı Notlarının Katılımcılar ile Paylaşılması	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Eğitim Kayıtlarının Dosyalanması	İş ilişkisinin sona ermesini müteakip 10 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
İş Başvurusu	6 ay	Saklama süresinin bitimini takiben 180 gün içerisinde