

**AYZA MIZRAK MAKİNE SANAYİ VE TİCARET LİMİTED ŞİRKETİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

26/07/2022

1. GİRİŞ VE POLİTİKA’NIN HAZIRLANMA AMACI.....	3
2. TANIMLAR	3
3. KAPSAM.....	4
4. TEMEL İLKELER.....	4
a) Kişisel veriler hukuka ve dürüstlük kuralına uygun olarak işlenir.	4
b) Kişisel veriler doğru ve gerektiğinde güncel olarak saklanır.	4
c) Kişisel veriler belirli, açık ve meşru amaçlar için işlenir.	5
d) Kişisel veriler işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenir.	5
e) Kişisel verileri mevzuatta öngörülen veya amaçla bağlantılı süre kadar saklanır.	5
5. KAYIT ORTAMLARI.....	5
6. SAKLAMA SEBEPLERİ.....	5
7. İMHAYI GEREKTİREN DURUMLAR	6
8. SAKLAMA VE İMHA SÜRELERİ	6
9. İMHA İÇİN KULLANILAN TEKNİKLER.....	7
a) Kişisel Verilerin Silinmesi:.....	7
b) Kişisel Verilerin Yok Edilmesi:.....	8
c) Kişisel Verilerin Anonim Hale Getirilmesi:.....	8
i. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	8
ii. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	9
10. TEKNİK VE İDARİ TEDBİRLER.....	9
a) İdari Tedbirler	Hata! Yer işareti tanımlanmamış.
b) Teknik Tedbirler:	Hata! Yer işareti tanımlanmamış.
11. UNVAN, BİRİM VE GÖREVLER	10

1. GİRİŞ VE POLİTİKA’NIN HAZIRLANMA AMACI

AYZA MIZRAK MAKİNE SANAYİ VE TİCARET LİMİTED ŞİRKETİ (“**Şirket**”), olarak kişisel verilerin korunması konusuna azami dikkat ve özen gösteriyor ve tüm faaliyetlerimizde kişisel verilerin hukuka uygun olarak korunmasını gözetiyoruz. Tarafımızca hukuka uygun bir biçimde yürütülen kişisel veri işleme faaliyetlerine ilişkin gerekli tüm idari ve teknik tedbirleri alıyoruz.

İşbu Kişisel Veri Saklama ve İmha Politikası (“**Politika**”), 6698 Sayılı Kişisel Verilerin Korunması Kanunu (“**KVKK**” ya da “**Kanun**”), Kanun’a dayanılarak hazırlanan ve 28 Ekim 2017 tarihli Resmi Gazete’de yayımlanan ve 1 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“**Yönetmelik**”) uyarınca yükümlülüklerimizi yerine getirmek ve yukarıda bahsedilen teknik ve idari tedbirlerin alınması amacıyla veri sorumlusu sıfatıyla ŞİRKET tarafından hazırlanmıştır.

2. TANIMLAR

İşbu Politika’nın uygulanması ve yorumlanmasında aşağıda belirtilen tanımlar kullanılacaktır. Bu Politika’da tanımlanmayan kavramlar için Kanun ve ilgili yönetmeliklerde bulunan tanımlar kullanılabilir.

Kavram	Tanım
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
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 kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
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 kişilere ilişkin her türlü bilgi.
Kişisel Veri İşleme Envanteri	Şirket’in iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel veri işleme faaliyetlerini, kişisel verileri, kişisel veri işleme amaçları, kişisel verilerin aktarıldığı alıcı grubunu, saklama sürelerini, yabancı ülkelere gerçekleştirilen aktarımlar ve kişisel verilerin güvenliğine ilişkin alınan güvenlik önlemlerinin ilgili kişisel veri sahibi grubuyla ilişkilendirerek oluşturduğu ve detaylandığı kişisel veri işleme envanteri
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesi.
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 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.
Politika	Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Sicil (VERBİS)	Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili bilgi sistemi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sahibi	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.

3. KAPSAM

İşbu Politika; Şirket'in veri sorumlusu olarak verileri işlediği veya işlettiği tüm süreçler ve bu süreçler kapsamında işlenen tüm kişisel veriler için geçerli olacaktır. Şirket'in süreçleri kapsamında kişisel veri işleyen tüm çalışanlar ve tüm veri işleyen taraflar İşbu Politika'da belirtilen kurallara riayet edecek ve kişisel verilerin hukuka uygun bir şekilde ve Kanun'da belirtilen ilkeler çerçevesinde ölçülü ve meşru amaçlarla işlenmesinden sorumlu olacaktır.

4. TEMEL İLKELER

ŞİRKET olarak kişisel verilerin işlenmesi, saklanması ve imhasında aşağıda yer alan ilkelere uyulmaktadır;

a) **Kişisel veriler hukuka ve dürüstlük kuralına uygun olarak işlenir.**

ŞİRKET tüm faaliyetlerinde kişisel verileri hukuka ve dürüstlük kuralına uygun olarak işlemekte, gerekli idari ve teknik tedbirleri almakta ve Mevzuat'ı ve Kurul açıklamalarını yakından takip etmektedir.

b) **Kişisel veriler doğru ve gerektiğinde güncel olarak saklanır.**

ŞİRKET tüm veri işleme faaliyetleri kapsamında toplanan verilerin kaynağını kontrol eder ve işlenen kişisel verilerin doğru olmasına özen gösterir. Söz konusu verilerin sadece gerekmesi halinde güncellenir.

c) Kişisel veriler belirli, açık ve meşru amaçlar için işlenir.

ŞİRKET tarafından işlenen kişisel veriler belirli, açık ve meşru amaçlarla işlenmektedir. Bu kapsamda kişisel veri işleme faaliyetlerinin bu kriterleri sağlayıp sağlamadığı düzenli olarak ŞİRKET tarafından denetlenmektedir.

d) Kişisel veriler işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işlenir.

ŞİRKET tarafından işlenen kişisel veriler, işleme amacı ile bağlantılı, sınırlı ve bu amaç doğrultusunda ölçülü olarak işlenmektedir.

e) Kişisel verileri mevzuatta öngörülen veya amaçla bağlantılı süre kadar saklanır.

ŞİRKET tarafından işlenen kişisel veriler mevzuatta öngörülen süreler veya amacın gerçekleştirilebilmesi için gerekli olan süre kadar saklanır ve hukuka uygunluk sebebinin ortadan kalkması sonrasında, ilgili kişinin hukuka uygun talebi halinde veya ŞİRKET tarafından belirli aralıklarda işbu Politika kapsamında anonim hale getirilir, silinir veya imha edilir. Kurul tarafından aksine bir karar alınmadıkça bu yöntemlerden uygun olanı ŞİRKET tarafından seçilerek uygulanabilir.

5. KAYIT ORTAMLARI

Kişisel veriler, ŞİRKET tarafından aşağıda belirtilen ortamlarda hukuka ve veri güvenliğine ilişkin gerekli standartlara uygun olarak güvenli bir şekilde saklanmaktadır;

- Departman dolapları
- Arşiv
- Şirket içerisinde bulunan Server
- Ağ cihazları
- Laptoplar
- Masaüstü bilgisayarlar
- Mobil telefonlar

6. SAKLAMA SEBEPLERİ

ŞİRKET tarafından toplanan kişisel veriler;

- Yönetim Faaliyetlerinin Yürütülmesi
- Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
- Lojistik Faaliyetlerinin Yürütülmesi
- İş Faaliyetlerinin Yürütülmesi
- İş Sağlığı ve Güvenliği Faaliyetlerinin Yürütülmesi
- Hukuk İşlerinin Takibi Ve Yürütülmesi
- Finans Ve Muhasebe İşlerinin Yürütülmesi
- Fiziksel Mekan Güvenliğinin Temini
- Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar için Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Eğitim Faaliyetlerinin Yürütülmesi
- Görevlendirme Süreçlerinin Yürütülmesi
- Erişim Yetkilerinin Yürütülmesi
- Acil Durum Yönetim Süreçlerinin Yürütülmesi

amaçlarıyla KVKK'nın 5. ve 6. maddelerinde belirtilen kişisel verileri işleme şartları ve amaçları çerçevesinde saklanmaktadır. Yukarıda belirtilen işleme amaçlarının dışında ek işleme amaçlarının ortaya çıkması durumunda bu husus hem bu Politika'da hem de VERBİS'te belirtilecektir.

Bu çerçevede saklama sebepleri ve hukuki dayanakları aşağıda belirtilmiştir;

- a) Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- b) Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması,
- c) Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla ŞİRKET'nun meşru menfaatleri için saklanması zorunlu olması,
- d) Kişisel verilerin ŞİRKET'nun 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.

7. İMHAYI GEREKTİREN DURUMLAR

ŞİRKET kişisel verileri sadece amaçla bağlantılı olduğu sürece veya mevzuatta belirtilen bir süreç içinde saklamaktadır. Bu kapsamda kişisel veriler re'sen veya ilgili kişinin talebi üzerinde silinir, yok edilir veya anonim hale getirilir.

ŞİRKET tarafından yapılacak silme, imha veya anonim hale getirme işlemleri aşağıdaki durumlar gerçekleşmektedir;

- a) Kişisel verilerin işlenmesini veya saklanmasını gerektiren meşru amacın ortadan kalkması,
- b) Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinde kişisel verilerin silinmesini öngören bir değişiklik yapılması,
- 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 söz konusu rızasını geri alması,
- e) İlgili kişinin, kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı hukuka uygun başvurunun veri sorumlusu tarafından kabul edilmesi,
- f) Kurul tarafından belirli bir ilgili kişiye ilişkin kişisel verilerin silinmesi yönünde bir karar alınması,
- g) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen söz konusu veriyi saklamayı haklı kılan herhangi bir koşulun bulunmaması.

8. SAKLAMA VE İMHA SÜRELERİ

ŞİRKET tarafından Kanun ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerin saklama ve imha sürelerinin aşağıdaki esaslar çerçevesinde belirlenmektedir;

- a) İlgili mevzuatta veya Kurul kararı ile ilgili kişisel verinin ne kadar süre ile saklanacağı düzenlenmiş ise bu süreye uyulur.

- b) Mevzuatta veya Kurul kararı ile ilgili kişisel verinin ne kadar süre ile saklanacağı düzenlenmemiş ise, yukarıda belirtilen ilkeler dikkate alınarak kişisel verinin saklanma amacı ile uyumlu ve sınırlı bir süre belirlenir. Buna göre, personel özlük dosyanızda veya işveren-işçi ilişkisi nedeniyle işlenen kişisel verileriniz iş sözleşmeniz süresince ve iş sözleşmesinin sona ermesi üzerine sona erme tarihinden itibaren ilgili zamanaşımı uyarınca 5 (beş) veya 10 (on) yıl boyunca, sağlık verileri ise mevzuat uyarınca 15 (onbeş) yıl boyunca saklanacaktır. Mevzuat değişikliği halinde mevzuat değişikliğine uygun olarak bu süre güncellenebilecektir.

Saklama süresi dolan ve imha süresi gelen kişisel veriler, 6 aylık aralıklarla periyodik olarak gerçekleştirilen imha işlemleri sırasında Politika'da belirtilen usullere göre imha edilir ve tüm işlemler kayıt altına alınarak en az 3 yıl süreyle saklanır.

9. İMHA İÇİN KULLANILAN TEKNİKLER

ŞİRKET tarafından Kanun ve diğer ilgili mevzuata uygun olarak elde edilen ve işlenen kişisel veriler Politika'da belirtilen saklama sürelerinin sona ermesi veya Kanun ve Yönetmelik'te sayılan kişisel veri işleme amaçlarının daha erken ortadan kalkması halinde re'sen bu sürede veya İlgili Kişinin başvurusu üzerine Kanun ve ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen yöntemler kullanılarak silinir, imha edilir veya anonimleştirilir.

Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri:

ŞİRKET tarafından kişisel verilerin silinmesi ve yok edilmesi için uygulanan tekniklere ilişkin usul ve esaslar aşağıda belirtilmiştir. ŞİRKET uygun yöntemi seçerek kişisel verileri silebilir.

ŞİRKET silinen kişisel verilerin İlgili Kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

a) Kişisel Verilerin Silinmesi:

Kişisel verilerin silinmesinde aşağıdaki adımlar uygulanır;

- Silme işlemine konu edilecek kişisel veriler belirlenir,
- Söz konusu kişisel verilere erişim yetkisi bulunan İlgili Kullanıcılar tespit edilir,
- İlgili kullanıcıların erişim yöntemleri tespit edilir,
- Veriler, ilgili kullanıcıların erişim yöntemleri ile tekrar erişemeyeceği bir biçimde silinir.

Yazılımlar içerisinde saklanan verilerin silinmesi: ŞİRKET, dijital ortamlarda saklanan verilerin silinmesi aşamasında, söz konusu kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemleri kullanır.

Bulutta saklanan verilerin silinmesi: Bulutta bulunan kişisel veriler, bulutun barındırdığı sunucuda bulunan dosya ve veri tabanlarının silinmesi ile gerçekleştirilmektedir.

Öte yandan, kişisel verilerin silinmesi işlemi, bu kapsama girmeyen bir takım başka verilerin zarar görmesi veya bunlara erişimin kısıtlanması gibi istenmeyen sonuçlar doğurabilecek ise kişisel veriler anonim hale getirilerek saklanır.

Basılı Ortamlarda Bulunan Kişisel Veriler: Basılı evraklarda bulunan kişisel veriler, ilgili evrakın saklanması gerekli değil ise evrak, kâğıt öğütücünden geçirilmek suretiyle, yakılarak imha edilmek suretiyle ya da atık yönetimi / geri dönüşüm alanında faaliyet gösteren firmalardan hizmet alınmak suretiyle imha edilerek silinir. İlgili evrakın saklanması herhangi bir sebep ile gerekli ise, evrak üzerine bulunan kişisel veriler mürekkep ile maskelenir.

b) Kişisel Verilerin Yok Edilmesi:

Üzerine Yazma: Özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerine en az sekiz kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemi kullanılabilir.

Manyetize Etme: Manyetik medyanın yüksek değerde manyetik alanlara maruz bırakılarak üzerindeki verilerin okunamaz bir biçimde bozulması yöntemi kullanılabilir.

Fiziksel Yok Etme: Manyetik medya üzerinden bulunan ve manyetize etme yoluyla yok edilemeyen kişisel veriler, ilgili medyanın tekrar kullanılmayacak hale getirilmesi yoluyla yok edilebilir. Buna ek olarak basılı ortamlarda tutulan veriler sonradan kullanılmayacak bir biçimde (öğütücüden geçirilmesi ve benzeri şekillerde) yok edilebilir.

Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

c) Kişisel Verilerin Anonim Hale Getirilmesi:

ŞİRKET tarafından uygulanan kişisel verilerin anonim hale getirilmesi tekniklerine ilişkin usul ve esaslar aşağıda belirtilmektedir;

i. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Bu çerçevede verinin genelinde değişiklik yapılmak suretiyle anonimleşme sağlanır.

Değişken Çıkartma: Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılması yoludur. Bu yol, değişkenin ilgili kişiyi tanımlamaya yarayacak önemli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması gibi sebeplerle kullanılabilir.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında ilgili veri kümesini bilen bir kişinin tahminini kolaylaştırabilecek derecede tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak veriler anonim hale getirilebilir. Örneğin, bir şirkette avukat olarak görev yapan tek bir kişi var ise, meslek kolonunu tamamen silmek yerine sadece ilgili kişinin verilerinin kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde amaç tahmin edilebilirlik riskini azaltmaktır. Bir veri tabanı içerisinde belirli bir kayda ait değerlerin yarattığı kombinasyon az görülür ve belirlenebilir ise ilgili veri gizlenebilir. Örnek olarak, şirkette çalışan 10 kişinin yaş, cinsiyet meslek ve çocuk sayılarının bulunduğu bir tabloda, 5 çocuğu olan bir kişinin bulunması halinde ilgili kayıt için 5 yerine "bilinmiyor" yazılması ile veriler anonim hale getirilebilir.

Genelleştirme: İlgili kişisel veriyi tanımlayıcı özel bir değerden daha genel bir değere çevirme işlemi olarak tanımlanabilir. Örneğin TC Kimlik No'su 9876543210 olan bir kişi ile yapılan anket çalışmasının 1. ve 3. sorularına "kırmızı" ve "İstanbul" şeklinde cevap vermiş olsun. Genelleştirme işlemi kullanılarak yapılacak çalışma sonucunda anket yapılan kişilerin % xx'unun 1. soruya kırmızı ve 3. soruya İstanbul yanıtını verdiği şeklinde bir sonuca ulaşılarak anonimleştirme yapılabilir.

Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir değişken belirlenerek kategori tanımlanması ile verilerin anonim hale getirilmektedir.

Örnek olarak, bir otoparkın abonelerinden, kalan abonelik süresinin 1 yıldan az, 1 ile 3 yıl arasında veya 3 yıldan çok olmasına göre kategoriler oluşturularak veriler anonim hale getirilebilir:

Örnekleme: Bütün veri kümesi yerine, bir alt küme alınarak açıklanır. Bu sayede bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan örnek alt küme içinde yer alıp almadığı kesin olarak bilinmediği için, kişilere ilişkin tahmin üretme riski düşürülmüş olur.

Global Kodlama: Alt ve Üst Sınır Kodlama uygulanması mümkün olmayan ve sayısal değer içermeyen veri kümelerinde, bir değer için öbeklenmiş bir veri kümesi kullanılmasıdır.

ii. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Bu yöntemlerde, tablolarda belirtilen değerlerin değiştirilmesi yoluyla veri kümesinin değerlerinde bozulma yaratılmaktadır.

Mikro Birleştirme: Tüm veriler ilk olarak anlamlı bir sıraya dizilerek gruplara ayrılır ve grupların ortalaması alınmak suretiyle elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanabilir.

Gürültü Ekleme: Sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda sapmalar eklenerek veriler anonim hale getirilebilir.

Veri Değiş Tokuşu: Saklanan veriler içerisinde seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilerek veriler anonim hale getirilebilir.

Yukarıda belirtilen yöntemlere ek olarak Kurul tarafından yayınlanan veya ileride yayınlanacak rehber (ler)de bulunan yöntemler ŞİRKET tarafından kullanılabilir.

10. TEKNİK VE İDARİ TEDBİRLER

ŞİRKET, kişisel verilerin korunması için gerekli idari ve teknik tedbirleri almaktadır. Aşağıda söz konusu tedbirler belirtilmiştir;

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

11. UNVAN, BİRİM VE GÖREVLER

PERSONEL	BİRİM	GÖREV	SORUMLULUK
[]	[]	Veri İrtibat Kişisi	ŞİRKET'in VERBİS üzerinden gerçekleştirmesi gerektiği bildirimleri gerçekleştirmek ve ŞİRKET ile Kişisel Verileri Koruma Kurulu arasındaki irtibatı sağlamak
[]	[]	Veri Denetçisi	Herhangi bir veri girişi yapma yükümlülüğü olmayıp şirket içerisinde gerçekleştirilecek periyodik ve zamansız denetimleri organize ederek şirket içerisindeki politikalara ve mevzuata uygunluğu denetleyerek ihlalde bulunan kişiler hakkında belirlenecek yaptırımların uygulanmasını sağlamakla görevli olacaktır. Ayrıca, Veri Denetçisi kendisine Raportör tarafından bildirilen olası veri ihlalinin Kişisel Verileri Koruma Kurulu'nun internet sitesinde yayımlanan form çerçevesinde ihlalin tespit edildiği saatten itibaren 72 saat içerisinde Kişisel Verileri Koruma Kurulu'na bildirmekle yükümlüdür.
[]	[]	Veri Kontrolleri	Şirket nezdinde işlenen veri sahiplerine ilişkin SGK Sicil no, T.C. Kimlik no, cinsiyet, işe giriş tarihi, doğum tarihi, öğrenim durumu, bölüm bilgisi, görev girişi, e-mail adresi, telefon numarası, adres bilgisi dahil ancak bunlarla sınırlı olmamak üzere Şirket nezdinde kullanılan her türlü network üzerinde veri girişi gerçekleştirmekle, verileri değiştirmekle, silmekle, kategorize etmekle ve veri üzerinden gerçekleştirilecek her türlü işlemi gerçekleştirmekle görevli olacaktır.
[]	[]	Yazılım ve Donanım Güvenlikçisi	Şirket nezdinde kullanılan yazılımlar için yeterli güvenlik duvarı, koruma önlemleri, antivirüs yazılımları vb. güvencik yazılımlarına sahip olunması, bu yazılımların güncel (up to date) ve yeterli korumaya sahip olması, e-ticaret sitelerindeki güvenli ödeme sistemlerinin oluşturulması, penetrasyon testlerinin yapılması ve bu testlerin yapılma sıklığının belirlenmesi ve network güvenliğini sağlanması görevlerine haiz olacaktır. Şirket nezdinde verilerin işlendiği server, arşiv deposu veya dolapları, santral yönetimi, Wi-Fi yönetimi, işyerinde kullanılan dizüstü ve masaüstü bilgisayarların fiziki güvenliği, veri depolama için kullanılan disket, CD, harici bellekler vb. güvenliği ve switch ve router yönetiminden sorumlu olacaktır.
[]	[]	Raportör	Raportör, aylık olarak şirket nezdinde veri güvenliğine ilişkin alınan idari ve teknik tedbirler ile varsa yapılan denetimlerin sonuçlarını Veri Denetçisine raporlamakla sorumludur. Raportör aynı zamanda olası bir veri güvenliği ihlali halinde durumu derhal Kişisel Veri Açığı Politikası ve Bildirim Prosedürü uyarınca Veri Denetçisine bildirmekle görevlidir.

Veri Kontrolleri, Yazılım Güvenlikçisi, Veri İrtibat Kişisi, Donanım Güvenlikçisi ve Raportör hiyerarşik olarak Veri Denetçisi'ne karşı sorumlu olup Şirket'in Kişisel Verileri Koruma Mevzuatına uyum sağlaması amacıyla aralarında hiyerarşik ilişki olmaksızın işbirliği içerisinde çalışacaktır.