

ANKARA TREN GARI İŐLETMECİLİĐİ A.Ő
KİŐİSEL VERİ SAKLAMA Ve
İMHA POLİTİKASI

İçindekiler

| | |
|--|----|
| 1.GİRİŞ | 2 |
| 1.1 Amaç..... | 2 |
| 1.2 Kapsam..... | 2 |
| 1.3 Kısaltmalar ve Tanımlar | 2 |
| 2.İLKELER | 4 |
| 3.KAYIT ORTAMLARI..... | 5 |
| 4.SAKLAMA VE İMHA YA İLİŞKİN AÇIKLAMALAR | 5 |
| 4.1 Saklamayı Gerektiren İşleme Amaçları | 5 |
| 4.2 Saklamayı ve İmhayı Gerektiren Sebepler..... | 6 |
| 5. TEKNİK VE İDARİ TEDBİRLER..... | 7 |
| 5.1 Teknik Tedbirler..... | 7 |
| 5.2 İdari Tedbirler | 8 |
| 6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ..... | 8 |
| 6.1 Kişisel Verilerin Silinmesi | 9 |
| 6.2 Kişisel Verilerin Yok Edilmesi | 9 |
| 6.3 Kişisel Verilerin Anonim Hale Getirilmesi..... | 10 |
| 7. SAKLAMA VE İMHA SÜRELERİ | 10 |
| 8. PERİYODİK İMHA SÜRESİ | 11 |
| 9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI | 11 |
| 10. POLİTİKA'NIN GÜNCELLENME PERİYODU | 11 |
| 11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI..... | 11 |

1.GİRİŞ

1.1 Amaç

İşbu Kişisel Verileri Saklama ve İmha Politikası (“Politika”), şirketimizin sorumlu olduğu kişisel verileri 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“Yönetmelik”) uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerini kişisel verileri işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme veya anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla veri sorumlusu sıfatıyla Ankara Tren Garı İşletmeciliği A.Ş (“Şirket”) tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

1.2 Kapsam

Çalışan, çalışan adayı, misafir, müşteri, ziyaretçiler ve diğer üçüncü kişilerin kişisel verileri Kanun ve Yönetmeliğe uygun olarak işlenmesi ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanması öncelik olarak belirlenmiştir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.3 Kısaltmalar ve Tanımlar

| Kısaltma | 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 |
| Elektronik Ortam | Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar |
| Elektronik Olmayan Ortam | Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar |
| İlgili Kullanıcı/Veri İşleyen | 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 gerçek ya da tüzel kişilerdir |
| İlgili Kişi/Veri Sahibi | Kişisel verisi işlenen gerçek kişilerdir |
| İmha | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi |
| Hizmet Sağlayıcı | Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi |
| Kanun | 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 Veri İşleme Envanteri | Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme |

| | |
|--|---|
| | faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter |
| 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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale 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 hale 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 |
| Politika | Kişisel Verileri Saklama ve İmha Politikası |
| Veri Sorumlusu | Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi |
| Yönetmelik | 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik |

2. İLKELER

Ankara Tren Garı İşletmeciliği A.Ş tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket edilmektedir;

i. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'a ve ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.

ii. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirket tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanmaktadır.

iii. 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.

iv. Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Okul tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu hususta İlgili Kişi tarafından şirkete başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.

3. KAYIT ORTAMLARI

Veri sahiplerine ait kişisel veriler, Ankara Tren Garı İşletmeciliği A.Ş tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır.

| | |
|-----------------------------|---|
| Elektronik Ortamlar | Sunucular (Etki Alanı, Yedekleme, e-posta, Veritabanı, web, vb.) Yazılımlar (Ofis yazılımları) Bilgi güvenliği cihazları (Güvenlik Duvarı, Saldırı Tespit ve Engelleme, Günlük Kayıt Dosyası, Antivirüs vb.) Kişisel Bilgisayarlar (Masaüstü, Dizüstü) Mobil Cihazlar (Telefon, Tablet vb.) Optik Diskler (CD, DVD, vb.) Çıkarılabilir Bellekler (USB, Hafıza Kartı, Depolama Cihazı, vb.) |
| Elektronik Olmayan Ortamlar | Verilerin kâğıt üzerine basılarak tutulduğu ortamlardır. |

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Veri sahiplerine ait veriler, Ankara Tren Garı İşletmeciliği A.Ş tarafından faaliyetlerinin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının planlanması, müşteri/misafirlere sunulan hizmetlerin yerine getirilebilmesi, hizmet sağlayıcıları ile süreçlerin işletilebilmesi amacıyla elektronik ve/veya fiziki ortamlarda güvenli bir biçimde Kanun ve diğer ilgili yönetmelikte belirtilen sınırlar çerçevesinde saklanmakta ve imha edilmektedir.

4.1 Saklamayı Gerektiren İşleme Amaçları

Ankara Tren Garı İşletmeciliği A.Ş, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- Sözleşmenin kurulabilmesi ve değerlendirme yapılması
- İletişim kurulması, tedarikçi kartının açılması ve finansal işlemlerin yerine getirilmesi
- Eğitim kaydı yapılması, eğitim katılım durumunun tespiti
- Herhangi bir uyuşmazlıkta delil olarak kullanılabilmesi
- Şirketimizin faaliyet ve organizasyonlarının tanıtımının yapılabilmesi
- Otele giriş ve çıkış işlemlerinin tamamlanması
- Emniyet ve kolluk birimlerine bilgi verilmesi
- Ödeme işlemlerinin alınması ve fatura düzenlenmesi
- Hizmetimizi ve yükümlülüklerimizi yerine getirebilmek
- Misafir taleplerini yerine getirebilmek
- Kayıp eşya durumunda gereğinin yapılması
- Rezervasyon işlemlerinin tamamlanması
- İnternet kullanımının sağlanması
- İnternet erişim ve kullanım kaydının tutulmasına ilişkin yükümlülüklerin yerine getirilmesi
- Veri güvenliği faaliyetlerinin planlanması ve icrası
- Hukuken gerekli işlemlerin/kayıtların/bildirimlerin gerçekleştirilmesi
- Bilgi güvenliği süreçlerinin yürütülmesi
- Kullanıcı kaydı oluşturulması
- Soru ve mesajların değerlendirilmesi, yanıtlanması,
- Fiziksel mekân güvenliğinin sağlanması ve izinsiz giriş çıkışın engellenmesi
- Konaklama ücretinin tahsil edilmesi
- Konaklama ile konaklama ücretinin eşleştirilmesi
- İşveren tarafından mesai takibinin yapılması
- Çalışanların iş faaliyetlerinin takibi ve/veya denetimi
- Herhangi bir uyuşmazlık durumunda delil olarak kullanma
- Otopark üyelik işlemlerinin tamamlanması
- İletişim faaliyetlerinin yürütülmesi
- Hukuk işlerinin yürütülmesi
- Acil durum yönetimi süreçlerinin yürütülmesi
- İzin süreçlerinin yürütülebilmesi

- Çalışanın ilgili imkan, hak ve menfaatlerden faydalanabilmesi ve ilgili resmi mercilere bildirimlerin yapılabilmesi, iş sağlığı ve güvenliğine ilişkin önlemlerin alınması/aldırılabilmesi amacıyla işlenmesi,
- Bilgi güvenliği süreçlerinin planlanması, şirketin kullandığı bilişim sistemlerinin güvenliğinin sağlanması, bilgi teknolojileri alt yapısının oluşturulması ve yönetilmesi,
- Taşınır mal ve kaynakların güvenliğinin temini
- Veri sorumlusu operasyonlarının güvenliğinin temini
- Erişim yetkilerinin yürütülmesi
- Faaliyetlerin mevzuata uygun yürütülmesi
- Çalışanlar için yan haklar ve menfaatlerin belirlenmesi süreçlerinin yürütülmesi,
- Çalışanların iş faaliyetlerinin takibi ve/veya denetimi
- Risk yönetimi süreçlerinin yürütülmesi,
- Finans ve muhasebe işlemlerinin yürütülmesi,
- İç denetim / soruşturma / istihbarat faaliyetlerinin yürütülmesi
- İş sağlığı ve iş güvenliği faaliyetlerinin yürütülmesi,
- Saklama ve arşiv faaliyetlerinin yürütülmesi,
- Yetenek / kariyer gelişimi faaliyetlerini yürütülmesi
- Denetim / etik faaliyetlerin yürütülmesi,
- Görevlendirme süreçlerinin yürütülmesi,
- Çalışanlara iş kıyafeti ve kişisel koruyucu ekipman verilebilmesi,
- Ücret politikalarının yürütülmesi,
- Performans değerlendirme süreçlerinin yürütülmesi,
- Organizasyon ve etkinlik yönetimi,
- Çalışanları için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi,
- Çalışanlar için meslek içi eğitim planlamasının yapılması, eğitimlerin raporlaması, eğitim sertifikalarının hazırlanması, gerçekleşen eğitimlere katılan çalışanların takip edilebilmesi, çalışanların aldıkları eğitimler sonucu gelişim süreçlerinin takip edilebilmesi,
- İnsan kaynakları süreçlerinin planlanması,
- Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi,
- Bina ve tesis yerleşkeleri ve/veya tesisleri ile demirbaşlarının ve/veya taşınır ve kaynaklar ile bireylerin güvenliğinin temini,
- Üçüncü kişilerle yürütülen tedarik, satın alma gibi teklif alma-verme ile ilgili sözleşme süreçlerinin yönetilmesi
- Şirket içi politika ve prosedürlere uyum sağlanması, iç ve dış denetimlerin yapılması
- İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi
- İşten ayrılmalarla ilgili süreçlerin yürütülmesi
- İş sağlığı ve iş güvenliği faaliyetlerinin yürütülmesi
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde hukuki yükümlülüklerin yerine getirilmesinin sağlanması
- Şirket çalışanlarının ve şirketin iş ilişkisi içerisinde bulunduğu üçüncü tarafların hukuki, ticari ve iş güvenliğinin temin edilmesi

- Kurulacak çalışan adayı işveren hukuki ilişkisi çerçevesinde iş sözleşmesinin kurulması için gerekli olması nedeniyle iş başvurunuzu değerlendirme
- Uygun faaliyet ve etkinlikler, kampanyalar hakkında bilgi verilmesi ve şirketimi faaliyet ve etkinlikleri, kampanyalar hakkında bilgilendirme yapılması

4.2 Saklamayı ve İmhayı Gerektiren Sebepler

- Kanun ve kanuna bağlı ikincil mevzuatta kişisel verilerin saklanması ya da imhasının açıkça öngörülmesi,
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için saklanması zorunlu olması,
- Kişisel verilerin veri sorumlusunun herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri kapsamında veri sahiplerinin açık rızasının bulunması,

Yönetmelik uyarınca, aşağıda sayılan hallerde kişisel ya da özel nitelikli kişisel veriler, veri sorumlusu tarafından re'sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir;

- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- 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,
- Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyetle bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesi çerçevesinde Ankara Tren Garı İşletmeciliği A.Ş tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

- Bilgi İşlem sistemlerinin kötü niyetli yazılımlara karşı uygulamalar aracılığı ile korunması,
- Zafiyet ve Sızma (Penetrasyon) testleri ile bilişim sistemlerine yönelik risk, tehdit ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınması,
- Ağ ve uygulama hizmetleri kimlik doğrulama ile erişim gerçekleştirilmesi,
- Ağ ve uygulama hizmetlerine erişimde şifreleme kullanılması,
- Erişim kontrolü ve bilgiye erişim kısıtlamalarının uygulanması,
- Erişim kayıtlarının toplanması ve değerlendirilmesi,
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır,
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için sistem odasına sadece yetkili personelin girişini sağlayan erişimin sağlanması,
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik risklere uygun teknik tedbirlerin alınması ve alınan tedbirlere yönelik teknik kontrollerin yapılması,
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimlerin önlenmesi,
- Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz hale getirilmesinin sağlanması,
- Kişisel verilerin yok edilmesi geri dönüştürülemez ve denetim izi bırakmayacak şekilde sağlanır
- Güvenlik açıklarının takibi ve uygun güvenlik yamalarının yüklenerek bilgi sistemlerinin güncel tutulması,
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemlerinin kullanılması,
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programlarının kullanılması,
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim sınırlandırılması,
- Kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte,

kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2 İdari Tedbirler

- Kişisel verilerin hukuka aykırı olarak erişilmesinin, işlenmenin önlenmesi, muhafazasının sağlanması ile ilgili Kanun ve bağlantılı mevzuat hakkında bilgilendirmeler yapılmaktadır.
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgili Kurul’a bildirilir.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.
- Şirket tarafından yürütülen faaliyetlerde kişisel verilere ulaşımı olan personele gizlilik sözleşmeleri imzalatılmaktadır.
- Kişisel veri işlemeye başlamadan önce ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Periyodik ve rastgele denetimler yapılmaktadır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
- Fiziksel mekanların güvenliği sağlanmaktadır
- Veri paylaşımı yapılan ve veri işleyen konumunda olan 3. Gerçek / tüzel kişilerle yapılan sözleşmelere ek olarak veri güvenliği taahhütnamesi alınmaktadır
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- 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.
- Mevcut risk ve tehditler belirlenmiştir

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Ankara Tren Garı İşletmeciliği A.Ş tarafından kişisel verilerin silinmesi ve/veya imha edilmesine ilişkin usul ve esaslar aşağıda belirtilmiştir.

6.1 Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

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. 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.

Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için ilgili birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

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.

Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

De-manyetize Etme: Manyetik medya özel bir cihazdan geçirilerek yüksek deęerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir. 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: Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemeyecek şekilde yok edilir. Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin geri döndürülmeyecek şekilde eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi, okunamaz hale getirilmesi işlemi uygulanır.

6.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Ankara Tren Garı İşletmecilięi A.Ş tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde, Kişisel Veri Saklama ve İmha Politikasında ve VERBİS kayıtlarında yer almaktadır.

Söz konusu saklama sürelerinde gerekmesi halinde şirket tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi de yerine getirilir.

8. PERİYODİK İMHA SÜRESİ

Ankara Tren Garı İşletmecilięi A.Ş periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. KVKK KOMİSYONU

Şirketimiz tarafından, kişisel verilerin korunması mevzuatına uygunluęun sağlanması, muhafazası ve sürdürülmesi kapsamında Şirket bünyesinde gerekli koordinasyonu sağlayacak olan “Kişisel Verileri Koruma Komisyonu” (“KVK Komisyonu”) kurulmuştur. Aşağıda ünvanları belirtilen kişiler komisyonun üyesidir.

İnsan Kaynakları

Bilgi İşlem

Ön Büro

Satış

Muhasebe

10. KİŞİSEL VERİLERİ SAKLAMA SÜRELERİ

| SUREÇ | SAKLAMA SURESI | IMHA SURESI |
|---|--|--|
| İSG dosyaları | 15 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sözleşmeler | Sözleşmenin sona ermesini takiben 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İnsan Kaynakları Süreçlerinin Yürütülmesi | Faaliyetin sona ermesini takiben 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi | 2 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Ziyaretçi ve Toplantı Katılımcılarının Kaydı | Etkinliğin sona ermesini takiben 2 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Kamera Kayıtları | 2 Ay | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Müşteri Rezervasyon ve Girişi Süreçleri Kayıtları | 5 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

11. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuoyuna açıklanır. Basılı kâğıt nüshası da Kişisel Verileri Koruma Komisyonu tarafından dosyasında saklanır.

12. POLİTİKANIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir