**REFERANS GRUP İLETİŞİM SİSTEMLERİ LOJİSTİK İNŞAAT TURİZM OTOMOTİV SANAYİ VE TİCARET LİMİTED ŞİRKETİ**

**Referans Grup İletişim Sistemleri Lojistik İnşaat Turizm Otomotiv Sanayi ve Ticaret Limited Şirketi** (“**Referans Grup”**); gerçek kişilere ait kişisel verileri, 6698 sayılı Kişisel Verilerin Korunması Kanun’u ile 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik başta olmak üzere ilgili mevzuata uygun olarak saklamakta, gerektiği şekilde ve sürede imha etmektedir.

 Yürütülmekte olan iş faaliyetleri sırasında elde edilen tüm kişisel verilerin imhası ve saklanması işbu Kişisel Verileri Saklama Ve İmha Politikası’na **(“Politika”)** göre belirlenmekte ve gerçekleştirilmektedir.

 Kişisel verilerin saklanması ve imhası sürecinde, bu verilerin hukuka aykırı olarak saklanmasını ve imhasını önlemek amacıyla her türlü teknik ve idari tedbir alınmaktadır. Kişisel verilerin saklanması ve imhası süreçlerinde veri güvenliği sağlanmaktadır.

 Referans Grup kişisel verileri mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar saklamaktadır. Mevzuatta belirtilen sürenin bitmesi ya da amacın gerçekleşmesi halinde kişisel veriler re’sen ya da ilgilinin talebi üzerine silinmekte, yok edilmekte ya da anonim hale getirilmektedir.

 **KAPSAM**

 İşbu Politika, gerçek kişilerin Referans Grup tarafından işlenmekte olan bütün kişisel verilerini kapsamaktadır.

**SORUMLULUK VE GÖREV DAĞILIMLARI**

 Kişisel verilerin saklama ve imha süreçlerinde görev alan çalışanların unvanları, birimleri ve görev tanımları aşağıdaki liste’de verilmiştir.

1. UNVAN:
2. BİRİM :
3. GÖREV:

 1) UNVAN:

 2) BİRİM :

 3) GÖREV:

**KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI**

 Referans Grup, iş faaliyetlerini yerine getirirken elde ettiği kişisel verileri kanuni sürelere uygun olarak saklamak amacıyla aşağıda yer alan kayıt ortamlarını kullanmaktadır.

Kişisel veriler, Referans Grup tarafından aşağıda listelenen ortamlarda hukuka uygun olarak güvenli şekilde saklanır.

**KAYIT ORTAMLARI**

1. **Fiziksel Ortamlar:**Kağıt,Manuel veri kayıt sistemleri,Yazılı, basılı, görsel ortamlar
2. **Elektronik Ortamlar** Sunucular (yedekleme, web, dosya paylaşım, hizmet paylaşımı),Yazılımlar (ZİRVE,MİCROSOFT OFFİCE) Bilgi güvenliği cihazları, antivirüs (Windows Defender,Norton),Kişisel bilgisayarlar (Masaüstü, dizüstü) ,Mobil cihazlar (telefon, tablet ) ,Optik diskler (CD, DVD) ,Çıkartılabilir bellekler (USB, Hafıza Kart) ,yazıcı, tarayıcı, fotokopi makinesi

**SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR**

 Referans Grup tarafından, **Çalışan Adayı, Veli / Vasi / Temsilci, Çalışan, Hissedar/Ortak,Tedarikçi Yetkilisi, Ürün veya Hizmet Alan Kişi,Potansiyel Ürün Veya Hizmet Alan Kişi, Ziyaretçi** gibi ilgili kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

**Saklamayı Gerektiren Hukuki Sebepler**

 Kurumda, iş faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

* 6698 sayılı Kişisel Verilerin Korunması Kanunu,
* 6098 sayılı Türk Borçlar Kanunu,
* 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
* 5018 sayılı Kamu Mali Yönetimi Kanunu,
* 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
* 4982 Sayılı Bilgi Edinme Kanunu,
* 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
* 4857 sayılı İş Kanunu,
* 2828 sayılı Sosyal Hizmetler Kanunu
* İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
* Arşiv Hizmetleri Hakkında Yönetmelik
* Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

**Saklamayı Gerektiren İşleme Amaçları**

 Referans Grup,faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

* 1. Acil Durum Yönetimi Süreçlerinin Yürütülmesi
	2. Bilgi Güvenliği Süreçlerinin Yürütülmesi
	3. Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
	4. Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
	5. Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
	6. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
	7. Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
	8. Denetim / Etik Faaliyetlerinin Yürütülmesi
	9. Eğitim Faaliyetlerinin Yürütülmesi
	10. Erişim Yetkilerinin Yürütülmesi
	11. Faaliyetlerin Mevzuata Uygun Yürütülmesi
	12. Finans Ve Muhasebe İşlerinin Yürütülmesi
	13. Fiziksel Mekan Güvenliğinin Temini
	14. Görevlendirme Süreçlerinin Yürütülmesi
	15. Hukuk İşlerinin Takibi Ve Yürütülmesi
	16. İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
	17. İletişim Faaliyetlerinin Yürütülmesi
	18. İnsan Kaynakları Süreçlerinin Planlanması
	19. İş Faaliyetlerinin Yürütülmesi / Denetimi
	20. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
	21. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
	22. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
	23. Lojistik Faaliyetlerinin Yürütülmesi
	24. Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
	25. Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
	26. Mal / Hizmet Satış Süreçlerinin Yürütülmesi
	27. Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
	28. Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
	29. Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
	30. Pazarlama Analiz Çalışmalarının Yürütülmesi
	31. Performans Değerlendirme Süreçlerinin Yürütülmesi
	32. Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
	33. Risk Yönetimi Süreçlerinin Yürütülmesi
	34. Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
	35. Sözleşme Süreçlerinin Yürütülmesi
	36. Stratejik Planlama Faaliyetlerinin Yürütülmesi
	37. Talep / Şikayetlerin Takibi
	38. Taşınır Mal Ve Kaynakların Güvenliğinin Temini
	39. Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
	40. Ücret Politikasının Yürütülmesi
	41. Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
	42. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
	43. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
	44. Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
	45. Yönetim Faaliyetlerinin Yürütülmesi
	46. Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

**Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Hukuki ve Teknik Nedenler**

Kişisel veriler ilgili mevzuatta öngörülen süre boyunca veya böyle bir süre öngörülmemişse, kişisel verilerin işlenme amaçları için gerekli olan süre kadar saklanmaktadır.

 Kişisel veriler;

* İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
* İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
* Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
* Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
* Referans Grup tarafından, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap verilmemesi hallerinde; ilgili kişinin KVK Kurula’na şikâyette 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, durumlarında, Referans Grup tarafından silinir, yok edilir veya anonim hale getirilir.

**KİŞİSEL VERİLERİN GÜVENLİĞİNE YÖNELİK TEKNİK VE İDARİ TEDBİRLER**

 Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi süreçlerinde kullanılan mevcut teknolojiler göz önüne alınarak, aşağıdakilerle sınırlı olmamak üzere, her türlü teknik ve idari tedbir alınmaktadır.

**Kişisel Verilerin Güvenliğine Yönelik Teknik ve İdari Tedbirler**

1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

2. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

3. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

4. Çalışanlar için yetki matrisi oluşturulmuştur.

5. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar

hazırlanmış ve uygulamaya başlanmıştır.

6. Gerektiğinde veri maskeleme önlemi uygulanmaktadır

7. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

8. Güncel anti-virüs sistemleri kullanılmaktadır.(Windows Defander,Norton)

9. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

10. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

11. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

12. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

13. Kişisel veri güvenliğinin takibi yapılmaktadır.

14. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri

alınmaktadır.

15. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği

sağlanmaktadır.

16. Kişisel veri içeren ortamların güvenliği sağlanmaktadır

17. Kişisel veriler mümkün olduğunca azaltılmaktadır.

18. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

19. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

20. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve

uygulanmaktadır.

21. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir

22. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

23. Şifreleme yapılmaktadır.

24. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

26. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

**Basılı Ortamda Saklanan Kişisel Verilerin Silinmesine Yönelik Yöntemler**

Kağıt üzerinde bulunan kişisel veriler karartma (maskeleme) yöntemi kullanılarak veya belgenin ilgili kullanıcıların erişemeyeceği bir ortamda güvenli olarak saklanması sureti ile silinmektedir.

**Elektronik Ortamda Saklanan Kişisel Verilerin Yok Edilmesine Yönelik Yöntemler**

Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde

erişilemez ve tekrar kullanılamaz hale getirilir

**Basılı Ortamda Saklanan Kişisel Verilerin Yok Edilmesine Yönelik Yöntemler**

 Kişisel veri içeren belgeler Geri Dönüştürülemez Şekilde (karmaşık sitillerle) Yırtma, Yakma gibi yöntemler ile yok edilmektedir.

**Elektronik Ortamda Saklanan Kişisel Verilerin Yok Edilmesine Yönelik Yöntemler**

 Kişisel veriler, bulunduğu sistemlerin türüne göre aşağıda yer alan yöntemlerden bir veya birkaçı kullanılarak yok edilmektedir.

1. **Kişisel Verilerin Anonim Hale Getirilmesi**

 Kişisel veriler, hukuka uygun olarak işlenmesini gerektiren sebeplerin ortadan kalkması halinde veri sorumlusu tarafından anonim hale getirilebilir. Bu kapsamda, Kişisel Verileri Koruma Kurumu yayınlarında ifade edilmiş olanlarla sınırlı olmamak üzere çeşitli anonim hale getirme teknikleri Referans Grup tarafından kullanılmaktadır.

1. **Maskeleme**

 Bu yöntem, kişisel veri niteliğindeki bir bilginin, belirli alanlarının kaldırılarak veya değiştirilerek ilgili kişi ile bağının kesilmesini ifade eder.

 Referans Grup amaçlarını gerçekleştirebilmek amacıyla yürüttüğümüz faaliyetlerimiz esnasında hukuka uygun şekilde saklanan verilerin saklama sürelerinin dolması durumunda veri ile kişi arasındaki bağı koparmak amacıyla maskeleme yapılacaktır.

**Elektronik Ortamda Saklanan Kişisel Verilerin Yok Edilmesine Yönelik Yöntemler**

**SAKLAMA VE İMHA SÜRELERİ**

 Kanunlarda yer alan kişisel verileri işleme şartlarının ortadan kalkması bu verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi sonucunu doğurmaktadır. Bu sebeple Yönetmelik’in 12’nci maddesi ile veri sorumlusu; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, işleme şartları ortadan kalkan kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğü altına girmektedir. Referans Grup tüm kişisel verilere dair imha işlemini belirtilen işleme sürelerine uygun olarak altı aylık aralıklar içerisinde gerçekleştirmektedir.

 Kişisel verilerin imhasına ilişkin bütün işlemler kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanmaktadır.

 Kişisel verilerin saklanması için belirlenen sürelere, Saklama Süreleri Listesi’nden ulaşabilirsiniz.

 Söz konusu saklama süreleri üzerinde, gerekmesi halinde Referans Grup tarafından güncellemeler yapılır.

 Referans Grup bu sürelere uyulmasını takip eder ve her altı ayda Referans Grup Yönetim Kurulunu bilgilendirir.

**1-Kimlik-Hukuki İlişki Süresi + 15 Yıl**

**2-İletişim-Hukuki İlişki Süresi + 15 Yıl**

**3-Lokasyon-6 Ay**

**4-Özlük-Hukuki İlişki Süresi + 15 Yıl**

**5-Hukuki İşlem-Hukuki İlişki Süresi + 10 Yıl**

**6-Müşteri-Hukuki İlişki Süresi + 10 Yıl**

**7-Fiziksel Mekan-1 Ay**

**9-Risk Yönetimi-Hukuki İlişki Süresi + 10 Yıl**

**10-Finans-Hukuki İlişki Süresi + 10 Yıl**

**11-Mesleki Deneyim-Hukuki İlişki Süresi + 10 Yıl**

**12-Görsel Ve İşitsel Kayıtlar-Hukuki İlişki Süresi + 10 Yıl**

**GÜNCELLEME PERİYODU**

 İşbu Politika en az yılda iki kez gözden geçirilir ve ihtiyaç̧ halinde güncellenir.

|  |  |
| --- | --- |
| **Güncelleme Tarihi** | **Güncelleme Kapsamı** |
|  |  |
|  |  |

**YÜRÜRLÜK**

 İşbu Politika Referans Grup Yönetim Kurulu onayı ile \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ tarihinde yürürlüğe girecektir.