CİNASOĞLU GROUP MÜHENDİSLİK VE TİCARET AŞ. KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

MADDE 1- AMAÇ

Kişisel verileri saklama ve imha politikası Cinasoğlu Group Ticaret ve Mühendislik AŞ. tarafından işlenen kişisel verilerin saklanması ve imhasına yönelik iş ve işlemler konusundaki usulleri ve esasları belirlemek amacıyla hazırlanmıştır.

MADDE 2- KAPSAM

Şirket çalışanlarına, çalışan adaylarına, stajyerlere, ürün ve hizmet alanlara, potansiyel müşterilere, ortaklara, ziyaretçilere, tedarikçilere ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamındadır.

Şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

Bu 6698 sayılı Kanunun 7. maddesinin üçüncü fıkrası ile 22. maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliği'ne uygun olarak hazırlanan politikanın amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

MADDE 3- TANIMLAR

Alıcı Grubu	: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme	: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Çalışan Elektronik Ortam	: Şirket personeli **:** 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

Hizmet Sağlayıcı	: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
İlgili Kişi	: Kişisel verisi işlenen gerçek veya tüzel kişi
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
Kişisel Verilerin Silinmesi	**:** Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
Kişisel Verilerin Yok Edilmesi	**:** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
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, alıcı veya alıcı grupları tarafından geri döndürme ve 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.

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
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	: Kanunda yer alan kişisel verilerin işlenme 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
Politika	: Kişisel Verileri Saklama ve İmha Politikası
Şirket	**:** Cinasoğlu Group Mühendislik ve Ticaret AŞ.
Veri İşleyen	: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi
Veri Sorumluları Sicil Bilgi Sistemi	: Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi
VERBİS	: Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Saklamayı Gerektiren Hukuki Sebepler:

MADDE 4- SORUMLULUK VE GÖREVLER

Şirketin tüm çalışanları ve birimleri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması konusunda sorumlu birimlere tam ve aktif destek verir. Politika kapsamında alınan idari ve teknik tedbirlerin uygulanmasında, birim çalışanlarının eğitilmesinde, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesinde ve kişisel verilerin hukuka uygun olarak muhafazasında tüm çalışanlar ve birimler, sorumlu birimlere destek olur.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım EK TABLO: 1'de gösterilmiştir.

MADDE 5- KAYIT ORTAMLARI

Kişisel veriler, şirket tarafından EK TABLO: 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

MADDE 6- SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirkette, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgli mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,

Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması
Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla şirketin meşru menfaatleri için saklanmasının zorunlu olması

Kişisel verilerin şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla Saklanması

Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi

Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması

6698 sayılı Kişisel Verilerin Korunması Kanunu,

6098 sayılı Türk Borçlar Kanunu,

4734 sayılı Kamu İhale Kanunu,

657 sayılı Devlet Memurları Kanunu,

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

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,

2547 sayılı Yükseköğretim Kanunu,

5434 sayılı Emekli Sağlığı 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.

MADDE 7- SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

1. Şirket aşağıdakiler dahil olmak ancak bununla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir:
2. İnsan kaynakları süreçlerini yürütmek
3. Kurumsal iletişimi sağlamak
4. Şirket güvenliğini sağlamak
5. İstatistiksel çalışmalar yapabilmek
6. İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
7. Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
8. Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
9. Yasal raporlamalar yapmak
10. Çağrı merkezi süreçlerini yönetmek
11. İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek
12. Şirket hukuk işlerinin icrası/takibini yapmak
13. Acil Durum Yönetimi Süreçlerinin Yürütülmesi
14. Bilgi Güvenliği Süreçlerinin Yürütülmesi
15. Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
16. Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
17. Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
18. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
19. Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
20. Denetim / Etik Faaliyetlerinin Yürütülmesi
21. Eğitim Faaliyetlerinin Yürütülmesi
22. İş Sağlığı/ Güvenliği Faaliyetlerinin Yürütülmesi
23. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması ve Değerlendirilmesi
24. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
25. Lojistik Faaliyetlerinin Yürütülmesi
26. Mal/Hizmet Satın Alım Hizmetlerinin Yürütülmesi
27. Mal/Hizmet Satış Sonra<sı Destek Hizmetlerinin Yürütülmesi
28. Mal/Hizmet Satış Süreçlerinin Yürütülmesi
29. Mal/Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
30. Organizasyon ve Etkinlik Yönetimi

31. Talep/Şikayetlerin Takibi
32. Taşınır Mal ve Kaynakların Güvenliğinin Temini
33. Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
34. Ücret Politikasının Yürütülmesi
35. Ürün/Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
36. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
37. Yabancı Personel Çalışma ve Oturma İzni İşlemleri
38. Yatırım Süreçlerinin Yürütülmesi
39. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
40. Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
41. Yönetim Faaliyetlerinin Yürütülmesi
42. Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

MADDE 8- İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re'sen şirket tarafından silinir ya da yok edilir:

a- Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması
b- Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması
c- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması
d- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi
e- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması
f- İlgili kişi, Şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.
g- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.
h- Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.
i- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

MADDE 9- TEKNİK TEDBİRLER

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıdadır:

Şirketimiz tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

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 şirket 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 dönüştürülemeyecek 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
h) Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
i) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
j) Güvenlik duvarları kullanılmaktadır.
k) Sızma (Penetrasyon) Testleri İle Kurumumuz Bilişim Sistemlerine Yönelik Risk, Tehdit, Zafiyet Ve Varsa Açıklıklar Ortaya Çıkarılarak Gerekli Önlemler Alınmakta,
l) Kurumun Bilişim Sistemleri Teçhizatı, Yazılım Ve Verilerin Fiziksel Güvenliği İçin Gerekli Önlemler Alınmakta,
m) Erişimler Kayıt Altına Alınarak Uygunsuz Erişimler Kontrol Altında Tutulmakta,
n) Saklama Ve İmha Politikasına Uygun İmha Süreçleri Tanımlanmakta Ve Uygulanmakta,
o) Kişisel Verilerin İşlendiği Elektronik Ortamlarda Güçlü Parolalar Kullanılmakta, Kişisel Verilerin Güvenli Olarak Saklanmasını Sağlayan Yedekleme Programları Kullanılmaktadır.
p) Çevresel Tehditlere Karşı Bilişim Sistemleri Güvenliğinin Sağlanması İçin Donanımsal (Sistem ----Odasına Sadece Yetkili Personelin Girişini Sağlayan Erişim Kontrol Sistemi,7/24 Çalışan İzleme Sistemi, Yerel Alan Ağını Oluşturan Kenar Anahtarların Fiziksel Güvenliğinin Sağlanması, vb.) önlemler alınır.
q) Yazılımsal (Güvenlik Duvarları, Atak Önleme Sistemleri, Ağ Erişim Kontrolü, Zararlı Yazılımları Engelleyen Sistemler Vb.) Önlemler Alınmaktadır
r) Hukuka Aykırı İşlemeyi Önlemeye Yönelik Riskler Belirlenmekte, Bu Risklere Uygun Teknik Tedbirler Alınmakta,
s) Erişim Yetki Ve Rol Dağılımları İçin Prosedürler Oluşturulmakta Ve Uygulanmakta,
t) Güvenlik Açıkları Takip Edilerek Uygun Güvenlik Yamaları Yüklenmekte,
u) Bilgi Sistemleri Güncel Halde Tutulmakta,
v) Güvenli Kayıt Tutma (Loglama) Sistemleri Kullanılmakta,
w) Kişisel Verilerin Güvenli Olarak Saklanmasını Sağlayan Yedekleme Programları Kullanılmakta Ve Elektronik Olan Veya Olmayan Ortamlarda Saklanan Kişisel Verilere Erişim, Erişim Prensiplerine Göre Sınırlandırılmaktadır.

MADDE 10- İDARİ TEDBİRLER

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıdadır:

a) Çalışanlar, kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmekte ve eğitilmektedir. İlgili kişilere Aydınlatma yükümlülüğü yerine getirilmektedir.
b) Şirketimizin yürütmüş olduğu tüm faaliyetler detaylı olarak tüm iş birimleri özelinde analiz edilerek, bu analiz neticesinde ilgili iş birimlerinin gerçekleştirmiş olduğu ticari faaliyetler özelinde kişisel veri işleme faaliyetleri ortaya konulmaktadır.
c) Şirketimizin iş birimlerinin yürütmüş olduğu kişisel veri işleme faaliyetleri; bu faaliyetlerin 6698 Sayılı Kanun'un aradığı kişisel veri işleme şartlarına uygunluğun sağlanması için yerine getirilecek olan gereklilikler her bir iş birimi ve yürütmüş olduğu detay faaliyet özelinde belirlenmektedir.
d) İş birimlerimiz belirlenen hukuksal uyum gerekliliklerinin sağlanması için ilgili iş birimleri özelinde farkındalık yaratılmakta ve uygulama kuralları belirlenmekte; bu hususların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler Şirket içi politikalar ve eğitimler yoluyla hayata geçirilmektedir.
e) Şirketimiz ile çalışanlar arasındaki hukuki ilişkiyi yöneten sözleşme ve belgelere, Şirketin talimatları ve kanunla getirilen istisnalar dışında, kişisel verileri işlememe, ifşa etmeme ve kullanmama yükümlülüğü getiren kayıtlar konulmakta ve bu konuda çalışanların farkındalığı yaratılmakta ve denetimler yürütülmektedir.
f) Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
g) İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
h) Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin bilgilendirme yapar veya mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar. Güvenlik Politika Ve Prosedürlerine Uymayan Çalışanlara Yönelik Uygulanacak Disiplin Yönetmeliği Uygulanır.
i) Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
j) Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.
k) Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
l) Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel, hırsızlık vb.) karşı güvenliği sağlanmaktadır. Fiziksel kişisel veriler kilitli dolaplarda muhafaza edilir.
m) Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

f) n) Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
o) Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
p) Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
r) Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
s) Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve info@cinasoglu.com hesabı kullanılarak gönderilmektedir.
t) Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
u) Sızma testi uygulanmaktadır.
v) Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
y) Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

MADDE 11- KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 3'te belirtilen yöntemlerle silinir.

MADDE 12- KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 4'te belirtilen yöntemlerle yok edilir.

MADDE 13- SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bunun haricinde; EK TABLO: 5'te yer alan saklama ve imha süresi tablosu esas alınır.

MADDE 14- PERİYODİK İMHA SÜRESİ

Şirket her yılın kasım ayında periyodik imha işlemi gerçekleştirilir.

MADDE 15- POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuoyuna ilan edilir. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

MADDE 16- YÜRÜRLÜK

Politika, şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile şirket tarafından saklanır.

MADDE 17- KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARINA, BİRİMLERİ VE GÖREV TANIMLARI

Bilgi İşlem Birimi Yöneticisi; Şirketin tüm Bilgi İşlem süreçlerini yönetir.

Hukuk Birimi Yöneticisi, Şirketin tüm hukuki işlem süreçlerini yönetir.

İnsan Kaynakları Yöneticisi (Personel ile ilgili konularda), Şirketin tüm personel süreçlerini yönetir.

Temin ve Tedarik Yöneticisi (Müşteri bilgileri ile ilgili konularda); Şirketin tüm satış pazarlama süreçlerini yönetir.

EK TABLO: 1 Saklama ve imha süreçleri görev dağılımı

UNVANI	BİRİMİ	GÖREVİ
Şirket Müdürü	Şirket	Çalışanların politikaya uygun davranmasından sorumludur.
	….	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi İşlem Müdürü	Bilgi İşlem Müdürlüğü	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
	Diğer Tüm Birimler	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

EK TABLO: 2 Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel bilgisayarlar Mobil Cihazlar Optik diskler Yazıcılar, tarayıcılar, fotokopi makineleri Çıkarılabilir ve taşınabilir bellekler Sunucular Yazılımlar Bilgi güvenliği cihazları	Kâğıtlar Yazılı ve basılı ortamlar Görsel kayıtlar Manuel veri kayıt sistemleri

EK TABLO: 3 Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortam	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 ortam	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu 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.
Taşınabilir medya	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.

EK TABLO: 4 Kişisel Verilerin Yok Edilmesi Yöntemleri

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel ortam	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medya	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir

EK TABLO: 5 Saklama ve İmha Süresi Tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş sağlığı ve güvenliği uygulamalar	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Bordrolama	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Personel mahkeme/adliye taleplerinin cevaplandırılması	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Eğitim kayıtlarının dosyalanması	Eğitimin düzenlenmesinin ardından 10 yıl	Saklama süresinin bitimini takiben 180 gün
Acil durum hazırlıkları	Hazırlığın yapılmasını takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Log kayıt takip sistemleri	Oluşturulmasından itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Kamera kayıtları	Kaydedilmesinden itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün

Ayrıca;

NO	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
1	Kimlik	10 YIL
2	İletişim	5 YIL
3	Lokasyon	2 YIL
4	Özlük	10 YIL
5	Hukuki İşlem	10 YIL
6	Müşteri İşlem	5 YIL
7	Fiziksel Mekân Güvenliği	2 YIL
8	İşlem Güvenliği	2 YIL
9	Risk Yönetimi	5 YIL
10	Finans	10 YIL
11	Mesleki Deneyim	5 YIL
12	Görsel ve İşitsel Kayıtlar	1 YIL
13	Felsefi İnanç, Din, Mezhep ve Diğer İnançlar	10 YIL
14	Kılık ve Kıyafet	5 YIL
15	Dernek Üyeliği	5 YIL
16	Sağlık Bilgileri	15 YIL
17	Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	10 YIL
18	Biyometrik Veri	2 YIL
19	Güvenlik Kamerası Kaydı	30 GÜN

Yukarıda ayrıca belirtilen süreler, çalışanlar için iş sözleşmesinin feshi tarihinden, tedarikçi ve müşteriler için sözleşmenin sona erme tarihinden veya sözleşme yoksa son işlemin yapıldığı tarihten, diğer ilgili kişiler için kişisel verilerin elde edilme tarihinden itibaren başlar ve sürenin sona ermesinden itibaren 180 gün içerisinde imha edilir.

Veri Sorumlusu Unvan : Cinasoğlu Group Mühendislik ve Ticaret AŞ.

Mersis no : 0210044884200001

E-posta adresi : info@cinasoglu.com

Kayıtlı Elektronik Posta Adresi : @cinasoglu.com

Fiziki Posta Adresi : Finanskent Mah. Finans Cad. Sarphan Finans Merkezi 5/C No:109 Ümraniye/İstanbul