

ITHINKA İNOVASYON YAZILIM DANIŞMANLIK SANAYİ VE TİCARET ANONİM ŞİRKETİ

Veri Saklama ve İmha Politikası

AMAÇ

Madde 1 – Kişisel Verileri Saklama ve İmha Politikası (“Politika”) Ithinka İnovasyon Yazılım Danışmanlık Sanayi ve Ticaret Anonim Şirketi (“Şirket”) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirket tarafından; ürün veya hizmet alan firmanın temsilcisi, ürün veya hizmet alan kişi, tedarikçi temsilcisi, gerçek kişi tedarikçi, tedarikçi çalışanı, tedarikçi yetkilisi, Şirket çalışanları ve çalışan adaylarına ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) ve diğer ilgili mevzuata uygun olarak işlenmesine ve işleme şartlarının tamamının ortadan kalkması durumunda silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek amacıyla işbu politika hazırlanmıştır.

Kişisel verilerin korunması ve kişisel verileri toplanan gerçek kişilerin temel hak ve hürriyetlerinin gözetilmesi kişisel verilerin işlenmesinde gözetilen en temel prensiptir.

Şirket, kişisel verilerin saklanması ve imhasına ilişkin faaliyetleri sayılan ilkeler doğrultusunda hazırlanmış olan işbu Politikaya uygun olarak gerçekleştirmektedir.

KAPSAM

Madde 2 –; Ürün veya hizmet alan firmanın temsilcisi, ürün veya hizmet alan kişi, tedarikçi temsilcisi, gerçek kişi tedarikçi, tedarikçi çalışanı, tedarikçi yetkilisi, Şirket çalışanları ve çalışan adaylarına ait kişisel verilerin saklanması ve imhasına ilişkin usul ve esaslar işbu Politika kapsamında düzenlenmiş olup; Şirketin uhdesinde bulunan ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ile kişisel veri işlenmesine, saklanmasına ve imha edilmesine yönelik faaliyetlerde işbu Politika uygulanacaktır.

TANIMLAR

Madde 3 – İşbu Politikanın uygulanmasında;

- a) **Açık rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- b) **Alıcı Grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- c) **Anonim hâle getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

- d) **Elektronik Ortam:** Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,
- e) **Elektronik Olmayan Ortam:** Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamları,
- f) **İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,
- g) **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- h) **Kanun:** 6698 Sayılı Kişisel Verilerin Korunması Kanununu,
- i) **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 ortamını,
- j) **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- k) **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 envanterini,
- l) **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 işlemi,
- m) **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,
- n) **Periyodik İmha:** Kanunda 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 işlemini,
- o) **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- p) **Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
- q) **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

KAYIT ORTAMLARI

Madde 4 – Kişisel veriler Şirket bünyesinde elektronik ve elektronik olmayan ortamlarda kanuna uygun olarak saklanmaktadır.

a) Elektronik Ortamlar

- **SUNUCULAR:** 2 Ad fiziksel 2 adet sanal sunucu bulunmaktadır. Serverlar üzerinde Microsoft Server 2012 bulunmaktadır. PAF muhasebe ve personel programı kuruludur. Yedekleme için Veem yazılımı kullanılmakta yedekleme her akşam yapılmakta ve network içindeki NAS diske kaydedilmektedir. Antivirüs olarak Kaspersky Total Security yazılımı hem serverlarda hemde terminal PC lerde virüs koruması sağlamaktadır. Firewall olarak ZYXEL kullanılmaktadır.
- **VERİ TABANLARI:** Microsoft SQL
- **MAİLLER :** E-mail hizmeti dışardaki bir sunucuda muhafaza edilmekte Zimbra mail server kullanılmakta erişim ise IMAP/POP3 protokolleri ile sağlanmaktadır. Zimbra Mail sunucuda e-mailler max 90 gün tutulmaktadır.
- **KAMERA KAYITLARI:** Ofis bina yönetimince bulunan 2 adet kamera 1 adet DVR cihazına kayıt yapmaktadır, DVR cihazının disk kapasitesine göre 14/21 gün arası kayıt tutulmakta yer durumuna göre 14/21 gün önceki kayıtlar otomatik olarak silinmektedir.
- **MASAÜSTÜ VE DİZÜSTÜ BİLGİSAYARLAR:** Kullanılmakta olan masaüstü ve dizüstü bilgisayarlar kullanıcı adı ve şifreleriyle Networke erişebilmekte haricinde herhangi bir erişim verilmemektedir.
- **MOBİL CİHAZLAR :** Networkte Mobil cihazlarla erişim yetkisi verilmemektedir.
- **YAZICI, FOTOKOPİ VE FAKS MAKİNALARI:** Yazıcı, fotokopi ve faks makinalarında veri saklanmamakta bilgisayarlardan gönderilen çıktıları basacak şekilde çalıştırılmaktadır.

b) Elektronik Olmayan Ortamlar

- **KAĞITLAR:** Sözleşmeler, taahhütnameler, formlar, tutanaklar, faturalar vb. gibi.
- **DOSYALAR:** Özlük Dosyaları vb. gibi.
- **MANUEL VERİ KAYIT SİSTEMLERİ:** Muhasebe defterleri, İş yeri Hekimi Muayene defteri, personel izin defteri vb. gibi

KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN HUKUKİ VE TEKNİK SEBEPLERE İLİŞKİN AÇIKLAMALAR

Madde 5 – Şirket tarafından işlenen kişisel veriler Kanuna uygun olarak saklanır ve imha edilir. Kanunun 7. maddesi uyarınca işlenmesini gerektiren sebepler ortadan kalktığı takdirde kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda yer verilmektedir.

SAKLAMAYA İLİŞKİN AÇIKLAMALAR

Madde 6 – Kanunun 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6. maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Şirket faaliyetleri çerçevesinde ve işleme amaçları doğrultusunda saklanması gereken kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süreler kadar saklanmaktadır.

SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Madde 7- Şirket faaliyetleri, iş ve işleyiş süreçleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süreler kadar muhafaza edilmektedir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4857 sayılı İş Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

ile bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır. Mevzuatta herhangi bir süre öngörülmemiş ise; kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması anına kadar saklanmaktadır.

İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Madde 8 – Şirket tarafından işlenen 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,
- Şirketin, 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 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, Şirket tarafından re'sen ya da ilgili kişinin talebi üzerine silinmektedir, yok edilmektedir ya da anonim hale getirilmektedir.

KİŞİSEL VERİLERİN HUKUKA UYGUN SAKLANMASI VE İMHA EDİLMESİ İÇİN ŞİRKET NEZDİNDE ALINAN TEKNİK VE İDARİ TEDBİRLER

Madde 9 – Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12. maddesiyle Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından 31.01.2018 tarihli ve 2018/10 sayılı Kurul Kararı ile belirlenmiş yeterli önlemler kapsamında Şirket tarafından teknik ve idari tedbirler alınmaktadır.

TEKNİK VE İDARİ TEDBİRLER

Madde 10 – Şirket tarafından alınan teknik ve idari tedbirler aşağıda sayılmaktadır.

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerektiğinde veri maskeleyme önlemi uygulanmaktadır.

- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- 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.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ İÇİN UYGULANAN İMHA TEKNİKLERİ

Madde 11- İmha sürecinde yer alan kişiler imha listeleri oluşturulur. Yönetimden imha oluru alınır. Yapılan imha bilgisayar ortamına yansıtılarak kayıt altına alınır. İmha ile ilgili dokümanlar saklanır.

a) Elektronik Ortamlar

- **SUNUCULAR - VERİ TABANLARI:** Sunucularda saklanan kişisel veriler veri tabanlarında tutulmaktadır, bu veri tabanlarında süresi dolan veriler bilgi işlem uzmanı tarafından süresi dolduğunda program üzerinden silinmektedir.

- MAİLLER: Süresi dolan kişisel veriler bilgi işlem uzmanı tarafından manuel olarak ZIMBRA mail server üzerinden silinir.
- KİŞİSEL BİLGİSAYARLAR (MASAÜSTÜ, DİZÜSTÜ): Bilgisayarlar şirkete aittir ve personel ayrıldığında formatlanır ve cihaz üzerindeki tüm data temizlenir.
- MOBİL CİHAZLAR: Mobil cihazlar network erişimine kapalıdır.
- KAMERA KAYITLARI: DVR cihazının disk kapasitesine göre 14/21 gün kayıt tutulmakta 14/21 gün önceden başlamak üzere eski kayıtlar otomatik olarak silinmektedir.

b) Elektronik Olmayan Ortamlar

- KAĞIT : Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler yakılarak, yırtılarak geri döndürülemeyecek şekilde geri dönüşüme gönderilerek yok edilir.
- DOSYALAR: Dosyalanmış şekilde tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler yakılarak, yırtılarak geri döndürülemeyecek şekilde geri dönüşüme gönderilerek yok edilir.
- MANUEL VERİ KAYIT SİSTEMLERİ: Saklanmasını gerektiren süre sona erenler, yakılarak, yırtılarak geri döndürülemeyecek şekilde geri dönüşüme gönderilerek yok edilir.

KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRECİNDE YER ALAN KİŞİLER

Madde 12 - Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce işbu Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

UNVAN	BİRİM	GÖREV
Yönetici	Yönetim	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur. Şirket içerisindeki herkesin politikaya uygun hareket

			etmesinden sorumludur. Periyodik imha süreçlerinde oluşturulan imha listelerine olur verir.
Bilgi Uzmanı	Teknolojileri	Bilgi Teknolojileri	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur. Periyodik imha süreçlerinde imha listeleri oluşturur.
İnsan Müdürü/Muhasebe Müdürü	Kaynakları	İnsan Kaynakları/Muhasebe	Politikanın yürütülmesinden sorumludur. Periyodik imha süreçlerinde imha listeleri oluşturur.

SAKLAMA VE İMHA SÜRELERİ TABLOSU

Madde 13 –Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak; Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde; Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır. Gerekmesi halinde söz konusu saklama süreleri üzerinde güncellemeler yapılır.

Saklama ve İmha Süreleri aşağıdaki tabloda gösterilmektedir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
ÇALIŞAN ADAYLARININ İŞ BAŞVURULARININ DEĞERLENDİRİLMESİ VE İŞE ALIM SÜREÇLERİNİN YÜRÜTÜLMESİ KAPSAMINDAKİ BELGELER	DEĞERLENDİRME SÜRECİNİN SONA ERMESİNDEN İTİBAREN 2 YIL	SAKLAMA SÜRESİNİN BİTİMİNİ TAKİP EDEN İLK PERİYODİK İMHA SÜRESİNDE

ÇALIŞANLARA AİT PERSONEL İŞ SÖZLEŞMELERİ VE ÖZLÜK DOSYALARI KAPSAMINDAKİ BELGELER	İŞ İLİŞKİSİNİN SONA ERMESİNDEN İTİBAREN 10 YIL	SAKLAMA SÜRESİNİN BİTİMİNİ TAKİP EDEN İLK PERİYODİK İMHA SÜRESİNDE
SÖZLEŞMESEL İLİŞKİ GEREĞİ ÜRÜN/HİZMET ALAN GERÇEK KİŞİLER, ÜRÜN/HİZMET ALAN FİRMA TEMSİLCİLERİ VE GERÇEK KİŞİ TEDARİKÇİLER İLE TEDARİKÇİ FİRMA YETKİLİLERİ VE TEMSİLCİLERİNE AİT VERİLER	SÖZLEŞMESEL İLİŞKİNİN SONA ERMESİNDEN İTİBAREN 10 YIL	SAKLAMA SÜRESİNİN BİTİMİNİ TAKİP EDEN İLK PERİYODİK İMHA SÜRESİNDE

PERİYODİK İMHA SÜRELERİ

Madde 13 - Yönetmeliğin 11. maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirkette her yıl Nisan ve Ekim aylarında periyodik imha işlemi gerçekleştirilmektedir.

POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Madde 14 – İşbu Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayınlanmaktadır. Ayrıca Şirkete ait internet sitesinde kamuya açıklanmaktadır. Basılı kâğıt nüshası yönetimde saklanmaktadır.

POLİTİKANIN GÜNCELLENME PERİYODU

Madde 15 - Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.