TAKIM TEZGAHLARI SANAYİCİ VE İŞ İNSANLARI DERNEĞİ
(TİAD)

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

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

1. GİRİŞ

Kişisel Veri Saklama ve İmha Politikası (Politika), Takım Tezgahları Sanayici ve İş İnsanları Derneği (TİAD) ve iktisadi işletmeleri tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda uygulamaları belirlemek amacıyla hazırlanmıştır.

Üye firmalar, mevcut personel, çalışan adayları, hizmet sağlayıcılar, TİAD ve iktisadi işletmelerine ait web sitesi ve web portallarının kullanıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve diğer ilgili mevzuata uygun olarak işlenmesi ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanması TİAD tarafından öncelik olarak belirlenmiştir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, TİAD tarafından bu doğrultuda hazırlanmış olan Politika ve yayımlanmış olan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası çerçevesinde gerçekleştirilir.

2. KISALTMALAR

Alıcılar	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi(ler)
Açık Rıza	Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve hür iradeyle beyan edilen rıza
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Dijital Ortam	Kişisel bilgilerin oluşturulduğu, düzenlendiği ve saklandığı veritabanları dahil dijital ortamlar
Dijital Olmayan Ortam	Dijital arşiv haricinde kalan, basılı, görsel, vb. ortamlar
İmha	Kişisel verilerin silinmesi, imha edilmesi veya anonim hale getirilmesi
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kişi	Kişisel verisi işlenen gerçek kişi
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Veri İşleme Envanteri	İş süreçlerine bağlı olarak gerçekleştirilmekte olan kişisel verileri işleme faaliyetlerinin, veri işleme amaçları, hukuki sebebi, kategorisi, aktarılan alıcılar ve veri konusu kişi grubuyla ilişkilendirildiği, azami saklama süresinin belirtildiği envanter (KİVİEN)

Kişisel Verilerin İşlenmesi	Kişisel verilerin, tamamen veya kısmen 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
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, ceza mahkumiyeti, adli sicil verileri, biyometrik ve genetik verileri
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda, kişisel verileri saklama ve imha politikasında belirtilen aralıklarla uygulanacak silme veya anonim hale getirme işlemi
Personel	TİAD ve iktisadi işlemelerinde çalışan kişiler
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

3. VERİ KAYIT ORTAMLARI

Kişisel veriler, TİAD tarafından aşağıdaki tabloda belirtilen ortamlarda mevzuata uygun olarak güvenli bir şekilde saklanır.

Dijital Ortamlar	**Dijital Olmayan Ortamlar**
Fiziki Server (Etki alanı, e-posta, veritabanı, dosya paylaşım, vb.)	Kağıt (resmi yazı, gelen/giden evrak, vb.)
Web Sitesi Sunucuları	Manuel veri kayıt sistemleri (Üye bilgi kayıt defteri, anket formları, gelen/giden evrak defteri, üye kayıt klasörleri, yeterlilik sınav kayıt klasörleri, vb.)
Yazılımlar (CRM, UYS, DERBİS, VOC-Tester, Ofis Programları, Veri Yedekleme ve İmaj Yazılımı, vb.)	Basılı ortamlar (dergi, rapor, gazete, vb.)
Veri Güvenliği Donanımı (Güvenlik Duvarı, Antivirüs, 5651 Loglama, Güvenlik Kamerası Kayıt Cihazı, Veri Yedekleme Cihazı (NAS), vb.)	
Kişisel bilgisayarlar (Masaüstü, dizüstü)	
Mobil cihazlar (telefon, tablet vb.)	
Taşınabilir Veri Depoları (USB bellek, hafıza kartı, harici HDD, CD, DVD, vb.)	
Yazıcı, tarayıcı, fotokopi makinesi	

4. VERİ SAKLAMA

Kanun'un dördüncü 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, beşinci ve altıncı maddelerinde ise kişisel verilerin işleme şartları tanımlanmıştır. Kanun'un ilgili maddeleri doğrultusunda TİAD ve iktisadi işletmelerinin faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süre kadar saklanır.

4.1. Veri Saklama'nın Hukuki Dayanakları

TİAD ve iktisadi işletmelerinin faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler aşağıda yer alan kanun ve yönetmeliklerde öngörülen saklama süreleri kadar saklanır.

a. Türkiye Cumhuriyeti Anayasası
b. 4721 sayılı Türk Medeni Kanunu
c. 6698 sayılı Kişisel Verilerin Korunması Kanunu
d. 6098 sayılı Türk Borçlar Kanunu
e. 6102 sayılı Türk Ticaret Kanunu
f. 213 sayılı Vergi Usul Kanunu
g. 5253 sayılı Dernekler Kanunu
h. 5072 sayılı Dernek ve Vakıfların Kamu Kurum ve Kuruluşları ile İlişkilerine Dair Kanun
i. 1606 sayılı Bazı Dernek ve Kurumların Bazı Vergilerden, Bütün Harç ve Resimlerden Muaf Tutulmasına İlişkin Kanun
j. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
k. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
l. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
m. 4982 Sayılı Bilgi Edinme Kanunu
n. 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun
o. 4857 sayılı İş Kanunu
p. 5544 sayılı Mesleki Yeterlilik Kanunu
q. Dernek, Vakıf, Birlik, Kurum, Kuruluş, Sandık ve Benzeri Teşükküllere Genel Yönetim Kapsamındaki Kamu İdarelerinin Bütçelerinden Yardım Yapılması Hakkında Yönetmelik
r. Makine Emniyeti Yönetmeliği
s. Türkiye Yeterlilikler Çerçevesinin Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik
t. Bilim, Sanayi ve Teknoloji Bakanlığı Piyasa Gözetimi ve Denetimi Yönetmeliği
u. İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik
v. Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

4.2. Saklamayı Gerektiren Veri işleme Amaçları

- İnsan kaynakları ve personel yönetim süreçlerini yürütmek
- Üye firmalar ile iletişimi sürdürmek
- İlişkili kurum ve firmalar ile kurumsal iletişimi sağlamak
- TİAD ve iktisadi işletmelerinin işleyiş güvenliğini sağlamak
- İstatistiksel çalışmalar yapabilmek
- İmzalanan sözleşmeler doğrultusunda gerekli çalışmaları sürdürebilmek
- İlgili mevzuat kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı hukuki yükümlülüklerin yerine getirilmesini sağlamak

- TİAD ile iş ilişkisinde bulunan gerçek/tüzel kişilerle irtibat sağlamak
- İlgili mevzuatın gerektirdiği raporlamaları yapmak
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü sürdürmek

5. VERİ İMHA

Kişisel veriler;

- Veri işlenmesine ve saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya yürürlükten kaldırılması
- Veri işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması
- Sadece açık rıza şartına istinaden kişisel veri işlemenin gerçekleştiği hallerde, ilgili kişinin açık rızasını iptal etmesi
- Kanun'un 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun TİAD tarafından kabul edilmesi
- TİAD'ın, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; KVK Kurulu'na şikayette bulunulması ve bu talebin KVK Kurulu 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, TİAD ve iktisadi işletmeleri tarafından ilgili kişinin talebi üzerine silinir ya da anonim hale getirilir.

6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli şekilde saklanması, hukuka aykırı olarak işlenmesi/erişilmesinin önlenmesi ve hukuka uygun olarak imha edilmesi için Kanun'un 6'ncı ve 12'nci maddesi gereği özel nitelikli kişisel veriler için KVK Kurulu tarafından belirlenen ve ilan edilen yeterli önlemler çerçevesinde TİAD tarafından teknik ve idari tedbirler alınır.

6.1. Teknik Tedbirler

TİAD tarafından işlenen kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sıralanmıştır.

- Sızma (Penetrasyon) testleri ile TİAD bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Firewall (güvenlik duvarı) olay yönetimi ile gerçek zamanlı yapılan izlemeler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların server etki alanında yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal dizin (Active Directory) üzerinden güvenlik ayarları aracılığı ile yapılmaktadır.
- TİAD'ın bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, 7/24 kamera kayıt sistemi, yangın söndürme sistemi, su baskını uyarı sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, ağ erişim kontrolü, antivirüs/antispam sistemleri, vb.) önlemler alınmaktadır.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak (loglama) uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- TİAD, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve KVK Kurulu'na bildirmek için TİAD tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemi kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, prosedür ve talimatlara göre sınırlandırılmaktadır.
- TİAD ve iktisadi işletmelerinin internet sayfalarına erişim güvenli protokol (HTTPS) kullanılarak gerçekleştirilmektedir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- 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.
- Sunuculara TİAD dışından erişim sağlanması gerektiğinde, SSL VPN kurularak veri aktarımı gerçekleştirilmekte ve log kayıtları tutulmaktadır.

6.2. İdari Tedbirler

TİAD tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sıralanmıştır.

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Kişisel veri işlemeye başlamadan önce TİAD tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik veya rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

7. KİŞİSEL VERİLERİN İMHA EDİLMESİ

İlgili mevzuatta öngörülen süre veya işlendikleri amaç için belirlenen olan saklama süresinin sonunda kişisel veriler, TİAD tarafından veya ilgili kişinin başvurusu üzerine, ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

7.1. Kişisel Verilerin Silinmesi

Veri Ortamı	Yapılacak İşlem
Dosya paylaşım serverlarında (sunucular) yer alan kişisel veriler	Sunucularda yer alan kişisel verilerden, saklama süresi sona erenler için sistem yöneticisi tarafından ilgili kullanıcının erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklama süresi sona erenler, ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklama süresi sona erenler, hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ya da, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanabilir.
Taşınabilir Cihazlarda Bulunan Kişisel Veriler	Taşınabilir HDD, SSD, hafıza kartı veya USB bellek şeklindeki saklama ortamlarında tutulan kişisel verilerden saklama süresi sona erenler, hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

7.2. Kişisel Verilerin Yok Edilmesi

Veri Ortamı	Yapılacak İşlem
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kağıt ortamda yer alan kişisel verilerden saklama süresi sona erenler, kağıt öğütücülerde geri döndürülemeyecek şekilde yok edilir.
Silinemeyen Optik/Manyetik Medyada Yer Alan Kişisel Veriler	Optik veya manyetik medyada yer alan kişisel verilerden saklama süresi sona erenler için kağıt/plastik öğütücülerde (agromel) parçalama veya yakma gibi fiziksel olarak yok edilme işlemi uygulanır.

7.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, tekil kişisel verilerin başka verilerle eşleştirilse dahi gerçek kişi kimliğini belli etmeyecek hale getirilmesidir. Kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla, tekil ve gerçek kişi ile eşleştirilemeyecek verilerin kullanılması için bu yöntem uygulanabilir.

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.

8. VERİ SAKLAMA VE İMHA SÜRELERİ

TİAD'ın ISO 9001:2015 Kalite Yönetim Sistemi'nin bir parçası olan "YN-F-02-04 Kalite Kayıtları Listesi"nde belirtilmiş olan süreler takip edilerek imha işlemleri gerçekleştirilir.