KIRŞEHİR SANAYİ VE TİCARET ODASI KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1 OCAK 2021

KIRŞEHİR TİCARET VE SANAYİ ODASI
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. BÖLÜM 1-GİRİŞ

1.1 GİRİŞ

Kişisel Verileri Saklama ve İmha Politikası ("Politika") **Kırşehir Ticaret Ve Sanayi Odası**'nın "Kurum" gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

KTSO Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Oda çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, KTSO tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir. Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım **Tanımlar Ek -1 de** gösterilmiştir.

1.2 AMAÇ

Kişisel verileri saklama ve imha politikası **Kırşehir Ticaret Ve Sanayi Odası** tarafından işlenen kişisel verilerin saklanması ve imhasına yönelik iş ve işlemler konusundaki usulleri ve esasları belirlemek amacıyla hazırlanmıştır.

1.3 KAPSAM

Kurum çalışanlarına, çalışan adaylarına, stajyerlere,üyelere, ziyaretçilere, tedarikçilere ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamındadır.

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

BÖLÜM-2 ORTAMLAR VE GÜVENLİK TEDBİRLERİ

2.1 KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

Kurum nezdinde saklanan kişisel veriler ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir ortamda saklanır.Kişisel verileriniz KTSO tarafından Elektronik Olmayan(Verilerin Kağıt Üzerinde Yazılı Veya Basılı Tutulduğu Ortam İle) ve Elektronik Ortam(Kurum Bünyesinde Yer Alan server,sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlarda*(EK TABLO: 2'de listelenen*) KTSO tarafından hukuka uygun olarak güvenli bir şekilde muhafaza edilir

2.2 ORTAM GÜVENLİĞİNİN SAĞLANMASI

Kurumun 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.

2.2.1. TEKNİK TEDBİRLER

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

a- Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında güvenlik duvarı savunma hattı kullanılarak saldırılara karşı korunur.Antivirüs kullanılarak yazılım ve donanım sistemleri düzgün bir şekilde çalışması ve alınan güvenlik tedbirlerinin yeterliliği düzenli olarak kontrol edilerek olası güvenlik açığı kapatılır.

b- Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar

c- Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolünü sağlar

d- Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar

e- Kişisel verilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanır.(Kurumda çaprazlama imha tekniğiyle çalışan İmha Makineleri kullanılmaktadır.)

f- Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur

g- Kişisel Veri İçeren Sistemlere Erişim Sınırlıdır.Bu Sistemlere Girerken Erişim Yetkisi Tanınarak Yetkililer İçin Ayrı Hesaplar Şifre Ve Parolalar oluşturularak Bilgiye Müdahale Edilmesi Engellenir.

h- Yetki Ve Kontrol Matrisleri Oluşturulur.Güçlü Şifre Ve Parola Kullanılır Hesapların Şifrelerini Her 60 Günde 1 Zorunlu Olarak Değiştirilir.Bilişim Ağlarında Hangi Yazılım Ve Servislerin Çalıştığının Kontrol Edilir.

i- Çalışanların Sistem Ve Servislerdeki Güvenlik Zafiyetlerini, Bunları Kullanan Tehditleri Bildirmesi İçin Resmi Bir Raporlama Prosedürü Oluşturularak Sistem Yönetici Tarafından En Kısa Sürede Veri Sorumlusuna Sunulur.

j- Güvenlik Açıkları Takip Edilerek Uygun Güvenlik Yamaları Yüklenmekte, Bilgi Sistemleri Güncel Halde Tutulmakta.Kişisel Veriler Kendi Yerleşkesinde Yer Alan Cihazlarda ve Kağıt Ortamlarda Saklanıyor,Bu Cihazların Ve Kağıtların Çalınması Veya Kaybolması Gibi Tehditlere Karşı Fiziksel Güvenlik Önlemlerinin Alınması Suretiyle Korunur

2.2.2 İDARİ TEDBİRLER

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

a- Kişisel Veri İşleme Aydınlatma Metninin hazırlanarak ilgili kişileri Aydınlatma yükümlülüğü yerine getirilmektedir.
b- Kurumsal Politikalar,Sözleşmeler,Gizlilik Taahhütnameleri,Envanter Hazırlanarak KTSO'nun Kişisel Verilere Uyum Projesi yürütülmektedir.
c- Kurum İçi Periyodik ve Rastgele Denetimler,Risk Analizleri VERBİS Bildirim, Veri İşleyenler ile İlişkilerin Yönetimi,Çalışanların Niteliği Ve Teknik Bilgi/Becerisinin Geliştirilmesi,Çalışan Kişisel Verilerin Hukuka Aykırı İşlenmenin Önlenmesi, Kişisel Verilere Hukuka Aykırı Erişilmesinin Önlenmesi, Kişisel Verilerin Muhafazasının Sağlanması, İletişim Teknikleri Ve İlgili Mevzuatlar Hakkında Eğitimler Verilmektedir.
d- Çalışanlara Gizlilik Sözleşmeleri İmzalatılmaktadır.
e- Politika Ve Prosedürlerine Uymayan Çalışanlara Yönelik Uygulanacak Disiplin Prosedürü Uygulanmaktadır.
f- Kurum İçi Periyodik Ve Rastgele Denetimler Yapılmakta Ve Çalışanlara Yönelik Bilgi Güvenliği Eğitimleri Verilmektedir. Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam ederek ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri KTSO vermektedir
g- Saklanan kişisel verilere Kurum içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır.Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
h- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
i- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
j- Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

BÖLÜM 3- KİŞİSEL VERİLERİN İMHASI

3.1 SAKLAMA VE İMHA NEDENLERİ

3.1.1 SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Kurum bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız (ilgili politikaya "https://kirsehirtso.org.tr/" adresinden ulaşabilirsiniz) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır

3.1.2 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

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

a- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
b- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması
c- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla kurumun meşru menfaatleri için saklanmasının zorunlu olması

d- Kişisel verilerin kurumun herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması
e- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi
f- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması

3.1.3 İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde re'sen Kurum 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- Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:
g- Kanunlarda açıkça öngörülmesi.
h- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
i- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
j- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
k- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
l- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
m- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

3.2 İMHA YÖNTEMLERİ

Kurum Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir. KTSO tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

3.2.1 KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

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

3.2.2 KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

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

3.2.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ.

Kişisel veriler EK TABLO: 5'te belirtilen yöntemlerle yok edilir

3.3 SAKLAMA VE İMHA SÜRELERİ

3.3.1 SAKLAMA SÜRELERİ

Kurum tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir. Bütün bölümler, kendi kayıtlarının saklama ve yok etme yöntemini Yönetim Sistemlerinin belirlediği şekilde uygulamaktan sorumludur. Eğer müşteri tarafından istenen saklama süresi yasal düzenlemelerden az ise yasal düzenlemelere uyulur. Gizlilik derecesi olan dokümanlar yakılarak veya okunamayacak şekilde parçalanarak imha edilir, diğerleri ise alternatif amaçlarla kullanılır. İmha edilen kayıtların listesi tanımlanır. Kayıtların imhası dokümanın üstü çizilerek veya iptal kaşesi vurularak iptal edilir. Saklama Süreleri ise aşağıdaki listede verilmiştir. Bunun haricinde; EK TABLO: 5'te yer alan saklama ve imha süresi tablosu esas alınır.

3.3.2 İMHA SÜRELERİ

Kurum Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. İlgili kişi, Kanunun 13'ncü maddesine istinaden Kuruma başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; kurum talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Kurumun talebi almış sayılması için ilgili kişinin talebini

Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Kurum, her halde yapılan işlemle ilgili "ilgili kişiye" bilgi verir.

2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Kurum tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

3.4 PERİYODİK İMHA SÜRESİ

Kurum her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Kurum işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir. Periyodik imha süreçleri ilk kez 30.06.2018 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

BÖLÜM 4- KİŞİSEL VERİ KOMİTESİ

Kurum bünyesinde bir Kişisel Veri Komitesi kurar.Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.Kişisel Veri Komitesi bir yönetici(veya temsilcisi), bir insan kaynakları çalışanı ve bir mali işler çalışanı olmak üzere üç kişiden oluşur. Kişisel Veri Komitesinde görevli KTSO çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

UNVAN	GÖREV TANIMI
Kişisel Veri Komitesi Yöneticisi	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
KVK Uzmanı	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur

BÖLÜM 4 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 Kurum bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

BÖLÜM 5 YÜRÜRLÜK

Politika, Kurumun 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 Kurum tarafından saklanır

TANIMLAR-EK 1

TANIM	AÇIKLAMA
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	İlgili kişinin kendisiyle ilgili veri işlenmesine,özgürce,konuyla ilgili yeterli bilgi sahibi olarak ve sadece o işlemle sınırlı olarak verdiği onay beyanıdır.
Anonim Hale Getirme	Verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli ya da belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesini ifade eder.
Arşiv	Her türlü dokümanın belli bir düzen içinde saklama koşulları yerine getirilerek korunması ve değerlendirilmesidir.
Çalışan	Kırşehir Ticaret Ve Sanayi Odası Personeli
Çalışan Adayı	Kurumumuza herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ile ilgili bilgilerini kurumumuza açmış olan gerçek kişiler.

Doğrudan Tanımlayıcılar	Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları
Dolaylı Tanımlayıcılar	Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,
EBYS	Elektronik Belge Yönetim Sistemi
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.
Hizmet Sağlayıcı	Kırşehir Ticaret Ve Sanayi Odası ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	Kişisel verisi işlenen gerçek 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

Kayıt	Yürütülen faaliyetlerin sonuçlarını gösteren, gerçekleştirilen faaliyetler ve elde edilen sonuçlar için objektif delil sağlayan dokümanlar.
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 İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Kişisel Verilerin İşlenmesi	Kişisel verilerin kısmen veya tamamen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi,kaydedilmesi,depolanması,muhafaza edilmesi değiştirilmesi,yeniden düzenlenmesi,açıklanması,aktarılması,devralınması,elde edilebilir hale getirilmesi,sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.
Kişisel Verilerin İşlenmesi ve Korunması Politikası	"https://kirsehirtso.org.tr/" ulaşılabilecek Kurum da bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politika
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
KTSO	Kırşehir Ticaret Ve Sanayi Odası
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 re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Saynology	Otomatik Yedekleme Ünitesi
Politika	Kişisel Verileri Saklama Politikası
Veri İşleyen	Veri sorumlusu adına kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen gerçek ve tüzel kişilerdir.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade etmektedir.Bu sistemler elektronik ya da fiziki ortamda oluşturulabilir.
Veri Sorumlusu	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen,veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olanlardır.
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.

Yedekleme	Elektronik ortamdaki kayıtların düzenli aralıklarla, bulunduğu elektronik ortamdan başka bir elektronik/manyetik ortama yedeklenmesi.
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
Üçüncü Kişiler	Kurumumuzun taraflarla arasındaki ticari işlem güvenliğini sağlamak veya bahsi geçen kişilerin haklarını korumak ve menfaat temin etmek üzere bu kişilerle ilişkili olan üçüncü taraf gerçek kişiler veya bu politika kurum çalışanları kişisel verilerin korunması ve işlenmesi politikası kapsamına girmeyen gerçek kişiler
Ziyaretçi	Kurumun sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler

KİŞİSEL VERİ SAKLAMA ORTAMLARI-EK 2

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

KİŞİSEL VERİLERİ SİLME YÖNTEMLERİ-EK 3

Veri Kayıt Ortamı	**Silme Yöntemi**
Sunucularda yer alan kişisel veriler	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 veriler	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.(EBYS ortamında oluşturulan kayıtların (gelen evrak – giden evrak) yedeklenmesi TOBB

	tarafından yapıldığından birimler EBYS de oluşturdukları kayıtlar için yedekleme yapmazlar.)
Fiziksel ortamda yer alan kişisel veriler	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.
Karatma	Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir.Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde kalemle karalanarak görünemez hale getirilmesi şeklinde yapılır
Taşınabilir medyada bulunan kişisel veriler	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.
Yazılımdan güvenli olarak silme	Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken;bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler uygulanır.

KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ –EK 4

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel olarak yok etme	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medyada yer alan verilerin yok edilmesi	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

KİŞİSEL VERİLERİ ANONİM HALE GETİRME YÖNTEMLERİ-EK 5

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

SAKLAMA VE İMHA SÜRESİ TABLOSU –EK 6

VERİ SAHİBİ	SÜREÇ	VERİ SAKLAMA SÜRESİ	İMHA SÜRESİ
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	İş görüşmesi olumlu sonuçlanan adaylar için iş sözleşmesinin sona ermesinden itibaren 10 yıl; olumsuz sonuçlanan adaylar için adayın Kuruma başvuru tarihinden itibaren 6 ay ve her halükarda adayın verdiği izni geri aldığı tarihe kadar	Saklama süresinin bitimini takiben 180 gün
Çalışan Adayı,Çalışan,Ziyaretçiler	Kamera görüntüleri	15 gün saklanır	Saklama süresinin bitimini takiben 180 gün
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük veriler	İş Sözleşmesi Süresi Boyunca Ve İş Sözleşmesinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takiben 180 gün
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	İş Sözleşmesi Süresi Boyunca Ve İş Sözleşmesinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takiben 180 gün
Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	İş Sözleşmesi Süresi Boyunca Ve İş Sözleşmesinin Sona Ermesinden İtibaren 15 Yıl	Saklama süresinin bitimini takiben 180 gün

Çalışan	Kurumumuz Tarafından Yapılan Mesleki Yeterlilik Sınavları	Hukuki İlişkinin bitiminden itibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Kurumun İşbirliği İçinde Olduğu Kurum/Firmalar (Tedarikçi vb)	Kurumun İşbirliği İçinde Olduğu Kurum/Firmalar ile Kurum arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler,Kurumun İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri	Kurumun işbirliği içinde olduğu Kurum/ Firmaların, Kurum ile olan iş/ticari ilişkisi süresince ve ilişkinin sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır	Saklama süresinin bitimini takiben 180 gün
Tarihi Değere Sahip Olan Bilgiler	Faaliyetlerin Mevzuata Uygun Yürütülmesi/İş Sürekliliğinin Sağlanması	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Saklama süresinin bitimini takiben 180 gün
Üye	Üye kayıt işlemlerinin yapılması	Hukuki İlişkinin Bitiminden İtibaren 10 yıl	Saklama süresinin bitimini takiben 180 gün
Üye	Kurum ve İlgili Kuruluşlarla yapılan eğitimler ve sınavlar	Eğitimin Tamamlanmasından İtibaren 5Yıl(TOBB AKREDİTASYON SİSTEMİ)	Saklama süresinin bitimini takiben 180 gün
Üye	Üye Memnuniyet Anketleri ve Üye Talep Formları Dikkate Alınarak Üye Eğitim Planını Hazırlanması/	Anketin doldurulduğu yılın sona ermesine müteakiben 5 Yıl(TOBB AKREDİTASYON SİSTEMİ)	Saklama süresinin bitimini takiben 180 gün
Stajyer	Stajyerin Dosyası	Stajın Bitiminden İtibaren 1Yıl	Saklama süresinin bitimini takiben 180 gün
Stajyer	Oryantasyon Eğitimi	Stajın Bitiminden İtibaren 1Yıl	Saklama süresinin bitimini takiben 180 gün
Şirket Kurmak İsteyen Gerçek Kişiler/ Ortaklar/	Kuruluş belgesi	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Saklama süresinin bitimini takiben 180 gün

İşletme Yetkilisi			
Çalışanlar ve İlgili kişiler	Muhasebe Kayıtları	Hukuki ilişkinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
Çalışanlar ve İlgili kişiler	Gelen ve giden evrak defterleri	Tamamen dolduğu ve bütün kayıtların kapandığı tarihten itibaren on yıl	Saklama süresinin bitimini takiben 180 gün
Çalışanlar ve İlgili kişiler	Her türlü yazışmaya ait gelen ve giden evrak	10 yıl	Saklama süresinin bitimini takiben 180 gün
Çalışanlar ve İlgili kişiler	Bilirkişi, eksper ve kapasite raporları	10 yıl	Saklama süresinin bitimini takiben 180 gün
Çalışanlar ve İlgili kişiler	Para cezaları ile disiplin soruşturma ve cezalarına konu her türlü evrak belge ve dosya;	10 yıl	Saklama süresinin bitimini takiben 180 gün
Çalışanlar ve İlgili kişiler	Diğer arşiv malzemeleri	5 yıl	Saklama süresinin bitimini takiben 180 gün

SAKLAMA VE İMHA SÜREÇLERİNİN GÖREV DAĞILIMI-EK 7

UNVAN	VERİ	SAKLAMA SÜRESİ	MUHAFAZA SÜRESİ
Yönetim Sistemleri Yöneticisi	Yönetim Sistemleri El Kitabının ve İlgili Dokümanların Dağıtımı ile ilgili Kayıtlar	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Elektronik Ortam(Server)
Yönetim Sistemleri Yöneticisi	Yönetimin Gözden Geçirme Toplantısı Kayıtları	Yönetim Dönemi(4 Yıl)(PR02.KAYITLARIN	Hard Copy

		KONTROLÜ PROSEDÜRÜ)	
Genel Sekreterlik	Üye Hizmet Talep Kayıtları	Üyelik İlişkisinin Bitmesinden İtibaren 10 yıl	Hard Copy
Eğitim-Araştırma Bilgi İşlem	Hizmet Geliştirme ile İlgili Her Türlü Çalışma (Araştırma, Eğitim vb.)	Eğitimin bitmesinden itibaren 1 yıl	Hard Copy
Arşiv	Hizmet Faaliyetleri Dokümanları	10 Yıl	Hard Copy
Yönetim Sistemleri Yöneticisi	Dış Kaynaklı Dokümanlar (Yasa, (Yasa, Yönetmelik ve Standartlar)	Güncellenene kadar, sonraki aşamada arşivde 10 yıl tutulur.	Elektronik Ortam
Genel Sekreterlik	Tedarikçi Değerlendirme/Performans Sonuçları	Yönetim Dönemi(4 Yıl)	Hard Copy
Genel Sekreterlik	Tedarikçi Sözleşmeleri ve Giriş Kontrol Sonuçları	10 Yıl	Hard Copy
Genel Sekreterlik	Tedarikçi Uyarıları	5 Yıl	Hard Copy
İlgili Bölüm Arşivi	Hizmet kontrolü ve uygun olmayan ürün kayıtları	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy
Yönetim Sistemleri Yöneticisi	İş Akışları, Proses Kartları	Güncellenene kadar, sonraki aşamada arşivde 10 yıl tutulur.	Hard Copy
Oda Sicil Memurluğu	Oda günlük faaliyet kayıtları (Evrak Kayıt Defteri)	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Elektronik Ortam + Hard Copy
Ticaret Sicil Müdürlüğü Üye Dosyaları	Ticaret Sicil Müdürlüğü	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy + Elektronik Ortam
Genel Sekreterlik	Muhasebe Kayıtları	10 yıl	Hard Copy + Elektronik Ortam

Genel Sekreterlik	Üye Tahakkuk Takip Müfredat Defteri	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy + Elektronik Ortam
Genel Sekreterlik	Yönetim Kurulu Karar Defteri	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy
Genel Sekreterlik	Meclis Karar Defteri	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy
Oda Sicil Memurluğu	Oda Üye Dosyaları	Üyelik İlişkisinin Bitiminden İtibaren 10 yıl	Hard Copy + Elektronik Ortam
Ticaret Sicil Müdürlüğü	Ticaret Sicil Müdürlüğü Üye Dosyaları	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy + Elektronik Ortam
Genel Sekreterlik	Personel Özlük Dosyaları	Hukuki İlişkinin Bitiminden İtibaren 10 yıl	Hard Copy
Genel Sekreterlik	Toplantı Çağrıları, Hazirun Cetvelleri	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Hard Copy
Yönetim Sistemleri Yöneticisi	Odada uygulanan Yönetim Sistemleri (çevre, kalite, müşteri memnuniyeti, bilgi güvenliği, akreditasyon sistemi) dokümanları	Devlet Arşiv Hizmetleri Yönetmeliğinde Öngörülen Süreler Boyunca	Elektronik Ortam
Yönetim Sistemleri Yöneticisi	Personel Eğitim Kayıtları	Görev süresi tamamlanana kadar	Hard Copy
Genel Sekreterlik	Üye Eğitim Kayıtları	Üyelik İlişkisinin Bitmesinden İtibaren 1Yıl	Hard Copy
Bilgi	Bilgi Yedekleri	Devlet Arşiv Hizmetleri Yönetmeliğinde	Elektronik Ortam

Güveliği Yönetim Sistemleri Yöneticisi		Öngörülen Süreler Boyunca	(Server), Taşınabilir Bellek Kırşehir Ticaret Borsası kasası
Yönetim Sistemleri Yöneticisi	Dokümanların elektronik ortamda dağıtımları için kullanılan e-postalar	5 Yıl	Elektronik Ortam
Yönetim Sistemleri Yöneticisi	İptal edilen dokümanların asılları	5 Yıl	Elektronik Ortam