

# TDUB KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

## 1- POLİTİKANIN AMACI

Kişisel Verileri Saklama ve İmha Politikası ("Politika") Türkiye Değerleme Uzmanları Birliği ("Birlik") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Birlik; Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Birlik 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, Birlik tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

Birlik çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Birliğin sahip olduğu ya da Birlik tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

## 2- 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.

**ÜYS:** Birliğin "Üye Yönetim Sistemi" yazılımı.

**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:** Birlik 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.

**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.

**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 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 işlemi.

**Politika:** Kişisel Verileri Saklama ve İmha Politikası

**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.

### 3- SORUMLULUK VE GÖREV DAĞILIMLARI

Birliğin tüm birimleri ve çalışanları, sorumlu birimlerce 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 saklanmasıyla sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına aşağıda yer verilmiştir.

Saklama ve imha süreçleri görev dağılımı

Veri Koruma Görevlisi; İdari ve Teknik tedbirlerin uygulanması Çalışanların politikaya uygun hareket etmesinden ve Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.

Birlik veri silme işlemi için Veri Koruma Görevlisi tarafından münhasıran bir veya daha fazla personel görevlendirebilir. Silme işlemine konu teşkil edecek kişisel veriler Veri Koruma Görevlisi tarafından belirlenir. Silme işlemleri önceden belirlenmiş personel vasıtasıyla yerine getirilir. Bu personelin yetkileri özel olarak düzenlenir.

İç veya dış ağ ortamlarındaki dijital verilerin (dosya sunucusu, kullanılan yazılımlar, dijital arşiv ve yedekler) silinmesinden Bilgi Sistemleri Birimi sorumludur.

Fiziksel (elektronik olmayan) ortamda saklanan İnsan Kaynakları, Muhasebe ve Muhaberat verilerinin silinmesinden Mali ve İdari İşler Müdürü sorumludur.

Kişisel cihazlarda (bilgisayar, telefon, mobil telefon, tablet, bellek vb.) saklanan verilerin silinmesinden ilgili personel sorumlu olup, hangi dosyaların kişisel cihazlarda nasıl tutulacağına dair iç prosedür kapsamında hareket edilir. Kişisel cihazlarda saklanan verilerin silinmesi talimatı ve silinme kontrolünden Bilgi Sistemleri Birimi sorumludur.

İlgili kişilerin yetkilendirilmesine Bilgi Güvenlik Komitesi görev tanımın da yer verilmiştir.

Silinmesi gereken verilerin silme, yok etme veya anonimleştirilmesinin, kanun, yönetmelik ve Birlik politika ve prosedürlerine uygun olarak yapıldığının ve işlemlere ilişkin oluşturulan bilgi kaydı doğruluğunun kontrolü Veri Koruma Görevlisi tarafından yapılır.

Silinen verilerin kimlere ait olduğu konusunda Bilgi Sistemleri Birimi tarafından bilgi kaydı oluşturulur. Bu kayıtlar diğer hukuki yükümlülükler hariç olmak üzere en az üç (3) yıl süreyle saklanır.

#### **4- KAYIT ORTAMLARI**

Kişisel veriler, Birlik tarafından listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Kişisel veri saklama ortamları

Elektronik Ortamlar, Elektronik Olmayan Ortamlar, Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.), Yazılımlar (ofis yazılımları, portal, muhasebe yazılımı, ÜYS, VERBİS), Bilgi güvenliği cihazları (güvenlik duvarı, antivirüs vb.), Kamera sistemleri (görüntü ve ses kaydı), Kişisel bilgisayarlar (masaüstü, dizüstü), Mobil cihazlar (telefon, tablet vb.), Optik diskler (CD, DVD vb.), Çıkarılabilir bellekler (USB, Hafıza Kart, Sabit harici disk vb.), Yazıcı, tarayıcı, fotokopi makinesi, faks makinesi, kağıt, manuel veri kayıt sistemleri (anket formları), yazılı, basılı, görsel ortamlar.

#### **5- SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR**

Birlik tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

##### **5.1 Saklamaya İlişkin Açıklamalar**

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü 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 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Birlik faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

##### **5.1.1 Saklamayı Gerektiren Hukuki Sebepler**

Birlik'te, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

6698 sayılı Kişisel Verilerin Korunması Kanunu, 6098 sayılı Türk Borçlar Kanunu, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 4982 Sayılı Bilgi Edinme Kanunu, 4857 sayılı İş Kanunu, İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik.

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen hukuki süreler ve amaçla ilgili olarak tespit edilmiş saklama süreleri kadar saklanmaktadır.

##### **5.2 İmhayı Gerektiren Sebepler**

Kişisel veriler; İşlenmesine esas teşkil gerektiren ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası

İşlenmesini veya saklanmasını amacın ortadan kalkması

Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,

Kanununun 11.nci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Birlik tarafından kabul edilmesi,

Birliğin, 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 şikâyetinde bulunması ve bu talebin Kurul tarafından uygun bulunması

Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılabilecek herhangi bir şartın mevcut olmaması, durumlarında, Birlik tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

## **6- TEKNİK VE İDARİ TEDBİRLER**

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanununun 12.nci maddesiyle Kanununun 6.ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Birlik tarafından teknik ve idari tedbirler alınır.

### **6.1 Teknik Tedbirler**

Birlik tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

Birlik risk analizi ile bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır. Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır. Birliğin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler 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.

Birlik içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.

Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

Birlik, 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 Kurula bildirmek için Birlik 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) sistemleri kullanılmaktadır.

Kişisel verilerin güvenli olarak saklanması sağlayan veri yedekleme programları kullanılmaktadır. Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

Birlik internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak şifrelenmektedir.

Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, 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.

Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak, SSH veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

## 6.2 İdari Tedbirler

Birlik tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, hakkında eğitimler verilmektedir.

Yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.

Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.

Kişisel veri işlemeye başlamadan önce Birlik tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir. Kişisel veri işleme envanteri hazırlanmıştır. Birlik içi periyodik ve rastgele denetimler yapılmaktadır. Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

## 7- KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Birlik tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

### 7.1 Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda yer verilen yöntemlerle silinir.

Sunucularda yer alan Kişisel Veriler. Saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır. Elektronik ortamda yer alan kişisel veriler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Fiziksel ortamda bulunan verilerden saklanmasını gerektiren süre sona erenler için arşivden sorumlu yönetici hariç çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Fiziksel ortamda yer alan verilerden süresi sona erenler kağıt kırma makinelerinde geri dönülmeyecek şekilde yok edilir.

### 7.2 Kişisel Verilerin Anonim Hale Getirilmesi

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. Kişisel Verileri Anonim Hale Getirme Teknikleri;

Anonim hale getirme; bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Birlik, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirilmektedir.

Kişisel verilerin anonim hale getirilmesi tekniklerinden hangisinin uygulanacağına dair karar, teknik detaylarda Bilgi İşlem Birimi ve yazılım ekibinin görüşü alınmak koşulu ile Veri Koruma Görevlisi tarafından verilir.

## 8- SAKLAMA VE İMHA SÜRELERİ

Birlik 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.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi tarafından yerine getirilir. İmha süreleri Periyodik silme dönemlerinde süresi dolan verileri tespit için kullanılmaktadır.

Kişisel Verilerin Saklama Sürelerinin Yer Aldığı Tablo bilgileri aşağıda yer almaktadır. İşlenen veri kategorileri ve işlenen süreçler bazında saklama sürelerinin tespitinde bu tablo bilgilerinden faydalanılmaktadır.

- Muhasebe ve Finansal İşlemlere İlişkin tüm Kayıtlar / 10 Yıl 6102 Sayılı Kanun, 213 Sayılı Kanun
- Çerezler ve Log Kayıtları / 6 Ay – En Fazla 2 Yıl 5651 Sayılı İnternet Kanunu
- Ticari Elektronik Mail Onay Kayıtları / Onayın geri alındığı tarihten itibaren 1 Yıl 6563 Sayılı Kanun ve İlgili Mevzuat
- Çevrim içi Ziyaretçilere İlişkin Trafik Bilgileri / 2 Yıl 5651 Sayılı Kanun
- Müşterilere İlişkin Kişisel Veriler / 6563 Sayılı Kanun ve ilgili mevzuat çerçevesinde ise 3 yıl , Hukuki ilişki son erdikten sonra 10 Yıl. 6563 Sayılı Kanun, 6102 Sayılı Kanun, 6098 Sayılı Kanun, 213 Sayılı Kanun, 6502 Sayılı Kanun
- Tedarikçilere İlişkin Kişisel Veriler / Hukuki ilişki sona erdikten sonra 10 Yıl 6102 Sayılı Kanun, 6098 Sayılı Kanun ve 213 Sayılı Kanun
- Sözleşmeler / Sözleşmenin Sona Ermesinden İtibaren 10 Yıl KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
- İnsan Kaynakları Süreçleri / Faaliyetin Sona Ermesinden İtibaren 10 Yıl KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
- Donanım ve Yazılıma Erişim Süreçleri / 2 Yıl KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
- Ziyaretçi ve Toplantı Kullanıcıların Kaydı / Etkinliğin Sona ermesinden İtibaren 2 Yıl KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
- Kamera Kayıtları (Etkinlik, eğitim vb.) / 2 Yıl KVKK Tarafından Yayınlanan Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama Ve İmha Politikası
- İş Kanunu Kapsamında Saklanan Veriler (Örn. Kıdem tazminatı, ihbar tazminatı, kötüniyet tazminatı, eşit davranma ilkesine aykırılık tazminatına konu olabilecek bilgiler, bordro kayıtları, yıllık izin gün sayısı vb.) / İş İlişkinin sona ermesinden itibaren 5 Yıl 4857 Sayılı İş Kanunu ve İlgili Mevzuat
- İş Kanunu Kapsamında Saklanan Özlük Dosyasına İlişkin Veriler / İş İlişkinin sona ermesinden itibaren 10 Yıl 4857 Sayılı İş Kanunu ve İlgili Mevzuat / 6098 Sayılı Türk Borçlar Kanunu
- İş Kanunu Kapsamında Saklanan Verilerden Sendikal Tazminata Konu Olabilecek Veriler (Örn: Performans kayıtları, disiplin cezaları, fesih evrakları vb.) / İş İlişkinin sona ermesinden itibaren 10 Yıl 6098 Sayılı Türk Borçlar Kanunu
- İş Sağlığı ve Güvenliği Mevzuatı Kapsamında Toplanan Veriler (Örn: İşe giriş sağlık testleri, sağlık raporları, İSG Eğitimleri, İş Sağlığı ve Güvenliği faaliyetlerine ilişkin kayıtlar vb.) / İş İlişkinin sona ermesinden itibaren 15 Yıl 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği
- SGK Mevzuatı kapsamında tutulan veriler (Örn: İşe giriş bildireleri, pirim/hizmet belgeleri vb.) / İş İlişkinin sona ermesinden itibaren 10 Yıl 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve İlgili Mevzuat
- İş Kanunu Uyarınca: Çalışan ile ilgili Mahkeme/icra bilgi taleplerinin cevaplanması / İş İlişkinin sona ermesinden itibaren 10 Yıl 4857 Sayılı İş Kanunu ve İlgili Mevzuat
- Çalışan Erişim Kısıtlamaları (Active Directory İşlemleri vb.) / İş İlişkinin sona ermesinden itibaren 10 Yıl 4857 Sayılı İş Kanunu ve İlgili Mevzuat
- Birlik Ortakları ve Yönetim Kurulu Üyelerine ait Bilgiler (Örn: Huzur hakkı ve Kar payı ödemeleri vb.) / 10 Yıl 6102 Sayılı Türk Ticaret Kanunu
- Birlik Ortakları ve Yönetim Kurulu Üyelerine ait Bilgiler (Pay defterinde yer alan kişisel veriler) / Pay Defterinin Saklanma Zorunluluğu Sebebiyle Süresiz 6102 Sayılı Türk Ticaret Kanunu
- Burs Ödemesi, Çalışan Avans Ödemesi / 10 Yıl 6102 Sayılı Türk Ticaret Kanunu

- Komite Başvurusu, İş Başvurusu, Staj Başvurusu, Başvuru Kabul Edilmediği Takdirde Aday Başvurularına İlişkin Veriler (Örn: CV, Özgeçmiş, Cover Letter, Başvuru Formu vb.) / 1 Yıl Sektörel teamüller geçerli.
- Sendikal Faaliyetler Uyarınca İşlenen ve Sendika ile Paylaşılan Kişisel Veriler / 10 Yıl 6356 Sayılı Sendikalar ve Toplu İş Sözleşmesi
- Çalışanlara Yönelik Kurumsal İletişim Faaliyetleri Uyarınca İşlenen Veriler (Örn: Katılımcı Listesi vb.) / İş İlişkisinin sona ermesinden itibaren 10 Yıl Sektörel Teamül
- Çalışan Memnuniyet Anketlerine İlişkin Veriler / Anketin doldurulduğu yılın sona ermesine müteakiben 1 Yıl Sektörel Teamül
- Birlik Faaliyetleri Uyarınca, Saklanması Gereken Ticari Defterler, Ticari Defterlerde Yer Alan Kayıtlara Dayanarak Oluşturulan Belgeler, Finansal Tablolar vb. İşlenen Kişisel Veriler / 10 Yıl 6102 sayılı Türk Ticaret Kanunu
- Genel Kurul İşlemleri Uyarınca İşlenen Veriler / 10 Yıl 6102 sayılı Türk Ticaret Kanunu
- Birliğin Taraf Olduğu Sözleşmelerin Kurulması ve İçeriğine İlişkin Kişisel Veriler / 10 Yıl 6102 sayılı Türk Ticaret Kanunu
- Tüketicinin Bilgilendirilmesine ve Cayma Hakkını Kullanabilmesine İlişkin Sesli Veya Elektronik Ortamdaki Bilgiler / 3 Yıl 27866 Sayılı Resmi Gazetede Yayınlanan Mesafeli Sözleşmelere Dair Yönetmelik
- Mal ve Hizmetleri Tanıtmak, Pazarlamak, İşletmesini Tanıtmak ya da Kutlama ve Temenni gibi İçeriklerle Tanınırlığı Artırmak Amacıyla Alıcıların Elektronik İletişim Adreslerine Gönderilen Ticari Elektronik İletilere İlişkin Onay Kayıtları / 1 Yıl 29417 Sayılı 15.07.2015 Tarihli Resmi Gazetede Yayınlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında yönetmelik
- Sözleşmeden Kaynaklı İlişkilerde İşlenen Kişisel Veriler (Örn: Birlik Yetkilisi, Ad Soyad, imza sirküleri vb.) / Sözleşmenin Sona Ermesine Müteakip 10 Yıl 6098 Sayılı Türk Borçlar Kanunu
- Vergisel Kayıtlara İlişkin Kişisel Veriler / 5 Yıl 213 Sayılı Vergi Usul Kanunu
- Fatura, Gider Pusulası, Makbuz gibi Vergi Usul Kanunu Uyarınca Tutulması gereken Belgelerle İşlenen Kişisel Veriler / 5 Yıl 213 Sayılı Vergi Usul Kanunu
- Ziyaretçilerin Kişisel Verileri / 2 Yıl 5651 Sayılı Kanun (Birliğin Wi-Fi Ağına Erişim Sağlayan Ziyaretçiler İçin)
- CCTV Kameraları Uyarınca Güvenlik Amaçlı Olarak İşlenen Kişisel Veriler (Kamera Kayıtları) / 90 Gün Sektörel Teamül
- Çalışanların Kişisel Verilerinin Yer Aldığı Ortamlara İlişkin Yaptığı Erişimlerin Log Kayıtları / En Az 2 Yıl Olmak Suretiyle İş Davalarına Konu Olabilmesi Sebebiyle 10 Yıl 5651 Sayılı Kanun Gereği ve TİB (Telekomünikasyon İletişim Başkanlığı) Yönetmelikleri
- Birlik İnternet Ağının Kullanılması, İnternet Giriş ve Uzaktan Bağlantı Esnasında İşlenen Trafik Bilgileri (Örn: IP adres, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri vb.) / 2 Yıl 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6502 Sayılı Tüketicinin Korunması Hakkında Kanun Gereğince Satış Sonrası Hizmet Verilmesinin Zorunlu Olması Sebebiyle İşlenen Kişisel Veriler (Örn: Ürün kurulum tarihi, müşteri iletişim bilgileri) / 2 Yıl 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6502 Sayılı Tüketicinin Korunması Hakkında Kanun Gereğince Satış Sonrası Hizmet Verilmesinin Zorunlu Olması Sebebiyle İşlenen Kişisel Veriler (Örn: Ürün kurulum tarihi, müşteri iletişim bilgileri) / 15 Yıl 6502 Sayılı Tüketicinin Korunması Hakkında Kanun, 13.06.2014 Tarih ve 29029 Sayılı Resmi Gazetede Yayınlanan Satış Sonrası Hizmetler Yönetmeliği
- Müşteri Bilgilerinden, TTK 82. Maddesi Uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesine ilişkin kişisel veriler / 10 Yıl 6102 Sayılı Türk Ticaret Kanunu
- Müşteri İşlem Bilgileri (Müşterilerin Talep/Şikayet/önerilerine İlişkin Çağrı Kayıtları vb.) / 10 Yıl 6098 Sayılı Türk Borçlar Kanunu
- Potansiyel Müşterilere İlişkin Veriler (Örn: cookies, çerezler, linkedin üzerinden profillemeye ilişkin veriler / 13 Ay Avrupa Birliği-Sektörel Teamül Uygulaması
- Üyelik başvuru belgelerindeki kişisel veriler / Üyelik işlemlerinin tamamlanmadığı veya onaylanmadığı durumlarda 1 yıl
- Eğitim başvuru belgelerindeki kişisel veriler / Eğitimin gerçekleşmemesi veya katılımcının başvuruyu iptal ettiği durumlarda ise verileriniz 1 yıl, eğitimin gerçekleşmesi durumunda 213 sayılı Vergi Usul Kanuna göre 5 yıl
- İletişim amaçlı işlenen veriler / Açık rıza alınamaması durumunda iletildiği tarihten sonra 2 ay saklanır.

Amacı sona eren ve hukuki saklama süresine tabi olmayan kayıtlar Birlikçe tespit edilen makul süre sonunda silme yok etme veya anonimleştirme işlemine tabi tutulur.

## **9- PERİYODİK İMHA SÜRESİ**

Yönetmeliğin 11 maddesi gereğince Birlik periyodik imha süresini altı (6) ay olarak belirlemiştir. Birlik Mayıs ayında ve Kasım ayında periyodik imha işlemi gerçekleştirir.

Bu Politika da yapılacak her türlü değişiklik Veri Koruma Görevlisi onayına tabidir. Yapılan değişiklikler Yönetim Kurulu /üst Yönetim imzasıyla revizyon tarihi ve numarası verilerek uygulamaya girecek ve arşivlenecektir.