# Merkezi Finans ve İhale Birimi

# Kişisel Verileri Saklama Ve İmha Politikası

**1. Amaç**

Kişisel Veri Saklama ve İmha Politikası (Politika), mevcut "Kişisel Verilerin İşlenmesi ve Korunmasına İlişkin Politika" ile "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlusu Sıfatıyla Merkezi Finans ve İhale Birimi Tarafından Alınması Gereken Yeterli Önlemlere İlişkin Politika"da yer alan şartları da göz önüne almak suretiyle, Veri Sorumlusu olarak Merkezi Finans ve İhale Birimi (MFİB) (BİRİM) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

BİRİM, misyon, vizyon ve temel ilkeler doğrultusunda, BİRİM 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 kulllanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, BİRİM tarafından bu doğrultuda hazırlanmış olan işbu Politika'ya uygun olarak gerçekleştirilir.

**2. Kapsam**

BİRİM çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup, BİRİM'in sahip olduğu ya da BİRİM'ce yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde ilgili mevzuat hükümleri saklı kalmak suretiyle işbu Politika uygulanır.

Bu Politika'da tereddüte düşülen hallerde, açık kalan hususlarda, Politika'nın yeterli olmadığı durumlarda, uygulamadaki diğer BİRİM politikaları ve ilgili mevzuat doğrultusunda hareket edilir.

Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.

**3. Tanımlar ve Kısaltmalar**

- Alıcı Grubu : Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
- Açık Rıza : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
- Anonim Hale Getirme : Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
- Çalışan : Merkezi Finans ve İhale Birimi personeli.
- 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 : Merkezi Finans ve İhale Birimi 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, 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 Verilerin İşlenmesi : Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
- Kurul : Kişisel Verileri Koruma Kurulu
- Özel Nitelikli Kişisel Veri : Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
- Periyodik İmha : Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla 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.

**4. Sorumluluk ve Görev Dağılımı**

Veri sorumlusu, Merkezi Finans ve İhale Birimi'dir (BİRİM). BİRİM'in tüm yöneticileri ve çalışanları, Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, BİRİM çalışanlarının eğitimi ve farkındalığının arttırılması, 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 aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

*Tablo 1: Saklama ve imha süreçleri görev dağılımı*

| UNVAN | BİRİM/BÖLÜM | GÖREV |
|---|---|---|
| Birim Başkanı | Merkezi Finans ve İhale Birimi | Çalışanların Politika'ya uygun hareket etmesinden sorumludur. |
| Bilgi ve Veri Yönetim Yapısı | Bilgi ve Veri Yönetim Yapısı | Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi hususlarında koordinasyondan sorumludur. |
| Diğer Tüm Bölümler | Diğer Bölümler | Görevlerine uygun olarak Politika'nın yürütülmesinden, Politika'nın gerektirdiği iş ve işlemleri yerine getirmekten sorumludur. |

**5. Kayıt Ortamları**

Kişisel veriler, BİRİM tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

*Tablo 2: Kişisel veri saklama ortamları*

| ELEKTRONİK ORTAMLAR | ELEKTRONİK OLMAYAN ORTAMLAR |
|---|---|
| - Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.)<br>- Yazılımlar (ofis yazılımları, portal, EBYS, BELGENET vb.)<br>- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.)<br>- Kişisel bilgisayarlar (Masaüstü, dizüstü vb.)<br>- Mobil cihazlar (telefon, tablet vb.)<br>- Optik diskler (CD, DVD vb.)<br>- Çıkartılabilir bellekler (USB, Hafıza Kart vb.)<br>- Yazıcı, tarayıcı, fotokopi makinesi | - Kâğıt<br>- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri vb.)<br>- Yazılı, basılı, görsel ortamlar |

**6. Saklama ve İmhaya İlişkin Açıklamalar**

BİRİM tarafından; çalışanlar, çalışan adayları, ziyaretçiler, sözleşme ve protokoller kapsamında hizmet verilen kurum ve kuruluşlara ait gerçek kişi verileri ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Anılan Yönetmelik'in 7inci maddesinin 3üncü fıkrası hükmü gereğince, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 (üç) yıl süreyle saklanır.

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

**6.1 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 verileri işleme şartları" sayılmıştır.

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

**6.1.1 Saklamayı Gerektiren Hukuki Sebepler**

BİRİM'de, 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,
- 213 sayılı Vergi Usul Kanunu,
- 193 sayılı Gelir Vergisi Kanunu,
- 5671 sayılı Merkezi Finans ve İhale Biriminin İstihdam ve Bütçe Esasları Hakkında Kanun,
- 6245 sayılı Harcırah Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 657 sayılı Devlet Memurları Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 2547 sayılı Yükseköğretim Kanunu,

- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu,
- Merkezi Finans ve İhale Birimi'nin Kurulmasına İlişkin Türkiye Cumhuriyeti ve Avrupa Birliği Komisyonu Arasındaki Mutabakat Zaptı,
- Merkezi Finans ve İhale Birimi Personel Yönetmeliği,
- 6321 sayılı Resmi Yazışmalarda Uyulacak Usül ve Esaslar Hakkında Yönetmelik,
- Devlet Memurları Yiyecek Yardımı Yönetmeliği,
- 1 Nolu Cumhurbaşkanlığı Kararnamesi,
- Bilgi Edinme Hakkı Yönetmeliği,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler,

ve gerekli hallerde ilgili diğer mevzuat çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

**6.1.2 Saklamayı Gerektiren İşleme Amaçları**

BİRİM, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar;

- İnsan kaynakları süreçlerini yürütmek
- BİRİM'de iletişimi sağlamak
- BİRİM güvenliğini sağlamak
- BİRİM faaliyetlerinin ve iş süreçlerinin ifasını sağlamak
- İstatistiksel çalışmalar yapabilmek
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
- VERBİS 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 şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
- BİRİM ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
- Yasal raporlamalar yapmak
- Çağrı merkezi süreçlerini yönetmek
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü
- Denetim/iç denetim/soruşturma/istihbarat faaliyetlerinin yürütülmesini sağlamak

**6.2 İmhayı Gerektiren Sebepler**

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren sebeplerin ve/veya 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 BİRİM tarafından kabul edilmesi,
- BİRİM'in, 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 bulunulması 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, BİRİM tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re 'sen silinir, yok edilir veya anonim hale getirilir.

**7. Teknik ve İdari Tedbirler**

BİRİM tarafından,

- Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için Kanunun 12 nci maddesi kapsamında teknik ve idari tedbirler,
- Kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 7 inci maddesi ve Yönetmelik gereği tedbirler,
- Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenecek yeterli önlemler,

alınır.

**7.1 Teknik Tedbirler**

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

- Sızma (Penetrasyon) testleri ile Birimimiz 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.
- BİRİM'in 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, yerel alan ağını oluşturan kenar anahtarların 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.

- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- BİRİM, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Birimimizde kullanılmakta olan yazılımlarda Birimimiz El Kitabı'nın PIN Q.3.4. Password Policies bölümüne göre şifre kullanılmasına izin verilmektedir.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- BİRİM internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiş olup, uygulamada anılan bu politika hükümleri de özel nitelikli kişisel verilerle ilgili işlemlerde göz önüne alınır.
- 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 elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- 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. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak 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.

**7.2 İdari Tedbirler**

BİRİM 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, 657 sayılı Kanun ve ilgili diğer mevzuat hakkındaeğitimler verilmektedir.
- BİRİM tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü 657 sayılı Devlet Memurları Kanununun sicil ve disiplin hükümleri doğrultusunda takip edilmektedir.

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

**8. Kişisel Verileri İmha Teknikleri/Yöntemi**

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, BİRİM tarafından re'sen veya ilgili kişinin başvurusu üzerine, ilgili bölümden görevlendirilen en az 1 kişi tarafından periyodik imhaya gönderilmek üzere belirlenir ve yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir. İmhaya ilişkin süreç, periyodik takip/kontrol, iş ve işlemler, BİRİM bünyesindeki her bir bölüm tarafından kendi envanterindeki bilgilerin de göz önüne alınması suretiyle bölümlerin kendi sorumluluğunda olup, takibi de yine bölümlerce gerçekleştirilir. İlgili sürecin, ihtiyaç duyulduğunda Bilgi ve Veri Yönetim Yapısı danışmanlığında yürütülmesi temin edilecektir. Bu kapsamda yapılacak işlemlerde madde 9'da belirtilen hususlar da dikkate alınır.

**8.1 Kişisel Verilerin Silinmesi**

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

*Tablo 3: Kişisel Verilerin Silinmesi*

| Veri Kayıt Ortamı | Açıklama |
|---|---|
| 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. |
| 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. |
| 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. |

**8.2 Kişisel Verilerin Yok Edilmesi**

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel veriler, BİRİM tarafından Tablo-4'te verilen yöntemlerle yok edilir.

*Tablo 4: Kişisel Verilerin Yok Edilmesi*

| Veri Kayıt Ortamı | Açıklama |
|---|---|
| Fiziksel Ortamda Yer Alan Kişisel Veriler | Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir. |
| Optik / Manyetik Medyada Yer Alan Kişisel Veriler | 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. |

**8.3 Kişisel Verilerin Anonim Hale Getirilmesi**

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

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu 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. Değişkenleri çıkartma, Bölgesel gizleme, Genelleştirme, Alt ve üst sınır kodlama, Mikro birleştirme, Veri karıştırma ve bozma uygulanan bazı anonimleştirme yöntemleridir.

Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür

**9. Saklama ve İmha Süreleri**

BİRİM, kişisel verileri işleme amacı ortadan kalktığı veya ilgili mevzuatta belirtilen süreye kadar muhafaza etmektedir. Bu doğrultuda, ilgili mevzuatın veri için saklama süresi öngörüp öngörmediği incelenmekte/takip edilmektedir. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler BİRİM tarafından verinin bulunduğu ortamlara göre en uygun yöntemle imha ( silme, yok etme veya anonim hale getirme) edilmektedir.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler her bölüm bünyesinde seçilecek imha sorumlusu tarafından belirlenir ve imha listesi yazılı olarak Bilgi ve Veri Yönetim Yapısı'na bildirilir. İmha için belirlenen liste kesinleştikten sonra re'sen silme, yok etme veya anonim hale getirme işlemi Bilgi ve Veri Yönetim Yapısı'nın gözetiminde ve ilgili Bölüm tarafından yerine getirilir.

**10. Periyodik İmha Süresi**

Yönetmeliğin 11 inci maddesi gereğince BİRİM, periyodik imha süresini, Yönetmelik'te verilen maksimum süre olan 6 ay olarak belirlemiştir. Buna göre, BİRİM'de her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

**11. Politika'nın Yayınlanması ve Saklanması**

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Bilgi ve Veri Yönetim Yapısı'nda dosyasında saklanır.

**12. Politika'nın Güncellenme Periyodu**

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

**13. Politika'nın Yürürlüğü ve Yürürlükten Kaldırılması**

Politika, 01.01.2022 tarihi itibari ile yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshası/nüshaları Başkanlık Makamı Kararı ile Bilgi ve Veri Yönetim Yapısı tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Bilgi ve Veri Yönetim Yapısı tarafından saklanır.