**GÖYNÜK BELEDİYESİ**

**Kişisel Veri**

**Saklama ve İmha Politikası**

|  |  |
| --- | --- |
| Doküman İçeriği | Bu politikanın amacı, GÖYNÜK BELEDİYESİ tarafından, kişisel verilerin saklanması ve imhasına ilişkin yöntem ve süreçlere ilişkin esasları belirlemektir. |
| Versiyon No | 1 |
| Dayanak | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| Onaylayan | GÖYNÜK BELEDİYESİ Yönetim Kurulu |

İçindekiler

[1. AMAÇ 3](#_Toc52351709)

[2. kapsam 3](#_Toc52351710)

[3. HUKUKİ DAYANAK ve yükümlülük 3](#_Toc52351711)

[4. tanımlar 3](#_Toc52351712)

[5. sorumluluk ve görev dağılımı 4](#_Toc52351713)

[6. kayıt ortamları 5](#_Toc52351714)

[6.1. Elektronik Kayıt Ortamları 5](#_Toc52351715)

[6.2. Elektronik Olmayan Kayıt Ortamları 5](#_Toc52351716)

[7. kişisel verilerin saklanmasını ve imhasını gerektiren sebepler 5](#_Toc52351717)

[7.1. Saklama ve İmhaya İlişkin Hukuki Sebepler 5](#_Toc52351718)

[7.2. Saklamayı Gerektiren Amaçlar 6](#_Toc52351719)

[7.3. İmhayı Gerektiren Sebepler 6](#_Toc52351720)

[8. İDARİ VE TEKNİK TEDBİRLER 7](#_Toc52351721)

[8.1. İdari Tedbirler 7](#_Toc52351722)

[8.2. Teknik Tedbirler 7](#_Toc52351723)

[9. saklama ve periyodik imha süreleri 8](#_Toc52351724)

[10. kişisel verilerin imha teknikleri 9](#_Toc52351725)

[10.1. Kişisel Verilerin Silinmesi 9](#_Toc52351726)

[10.2. Kişisel Verilerin Yok Edilmesi 10](#_Toc52351727)

[10.3. Kişisel Verilerin Anonim Hale Getirilmesi 12](#_Toc52351728)

[11. politikanın yürürlüğü 12](#_Toc52351729)

GÖYNÜK BELEDİYESİ VERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ

Kişisel Veri Saklama ve İmha Politikası (“Politika”) GÖYNÜK BELEDİYESİ’nin (“Kurum”) veri sorumlusu sıfatıyla elinde bulundurduğu kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

2. kapsam

Bu Politika, Kurum tarafından kişisel verileri işlenen tüm gerçek kişilere ilişkin kişisel verileri kapsar ve Kurum’un sahip olduğu ya da Kurum tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları hakkında ve tüm veri işleme faaliyetlerinde bu Politika uygulanır. İşbu Politika, Kurum’un faaliyetleri çerçevesinde düzenlenmiş, asılları ve kopyaları dahil tüm elektronik ve elektronik olmayan ortamlarda bulunan belgeleri kapsar.

3. HUKUKİ DAYANAK ve yükümlülük

Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanun (”Kanun”) ve ilgili diğer mevzuat gereğince, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in (“Yönetmelik”) 5. maddesine dayanarak ve veri sorumlusu Kurumun kişisel veri işleme envanterine uygun olarak hazırlanmıştır.

Bu kapsamda, çalışanların, çalışan adaylarının, müşterilerin ve herhangi bir nedenle Kurum nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri, Kişisel Verilerin Korunması ve İşlenmesi Politikası ile işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara ve ilgili diğer mevzuata uygun olarak yönetilmektedir.

Kurumun bütün çalışanları işbu Politika’yı tam olarak anlamak ve uygulamakla yükümlüdür. Politikanın uygulanmasından, ilgili departman yöneticileri, İrtibat Kişisi, Kişisel Verilerin Korunması Komitesi sorumludur.

4. tanımlar

Bu Politika kapsamında kullanılan terimler aşağıdaki anlamları ifade eder.

|  |  |
| --- | --- |
| Aktif Kayıtlar | Kurum’un işleyişi, idaresi ve yönetimi için halen kullanılmakta olan kayıtlardır. |
| Aktif Olmayan Kayıtlar | Kullanılmayan; ancak işlenmesi sonradan gerekebileceği için saklama süreleri sona ermemiş kayıtlardır. |
| Elektronik Ortam | Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlardır. |
| Elektronik Olmayan Ortam | Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlardır. |
| Fiziksel Yok Etme | Optik veya manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesidir. |
| İkincil Mevzuat | Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüşü ifade eder. |
| İmha | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir. |
| Karartma/Maskeleme | Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması, buzlanması, yıldızlanması gibi işlemleridir. |
| 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 ortamdır. |
| Periyodik İmha | Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda bu Politikada belirtilen ve tekrar eden aralıklarla re’sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir. |
| Silme | Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. |
| Veri Kayıt Sistemi | Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. |
| VERBİS | Veri Sorumluları Sicil Bilgi Sistemidir. |

Burada yer verilmeyen terimlerin, Kanun, Yönetmelik ve diğer ikincil mevzuatta yer alan anlamda kullanıldığı kabul edilir.

5. sorumluluk ve görev dağılımı

Kurum’un tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim 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 sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımları aşağıdaki şekildedir:

|  |  |  |
| --- | --- | --- |
| ÜNVANI | BİRİMİ | GÖREVİ |
| Üst Yönetim | - | Çalışanların Politika’ya uygun hareket etmesinin sağlanmasından sorumludur. |
| Veri Sorumlusu İrtibat Kişisi | - | Kurum nezdinde Politika’nın yürütülmesinden sorumludur. |
| Kişisel Verilerin Korunması Komitesi | - | Politika’nın hazırlanması, yürütülmesi, yayınlanması, geliştirilmesi ve güncellenmesinden sorumludur. |
| İnsan Kaynakları Yetkilisi | - | Görev alanı çerçevesinde Politika’nın uygulanmasından sorumludur. |
| Bilgi Sistemleri Yetkilisi | - | Politika’nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve gerekli yatırımların sağlanması için yönetimin bilgilendirilmesinden sorumludur. |
| Finans-Muhasebe İşleri Yetkilisi | - | Görev alanı çerçevesinde Politika’nın uygulanmasından sorumludur. |
| İlgili Kullanıcılar ve Veri İşleyenler | - | Veri işleme ve saklanması ile ilgili işlemlerin usul ve yasaya uygun olmasından sorumludur. |

6. kayıt ortamları

Kurum bünyesinde kişisel verilerin kayıt ortamları aşağıda belirtilmiştir:

6.1. Elektronik Kayıt Ortamları

Ses kayıtları, fotoğraflar, videolar ve görsel ve işitsel ortamlar dahil birçok ortamda yer alan kişisel veriler; doğru, güncel ve kişisel verileri işlemesi gereken kişilerce erişilebilir olacak şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli elektronik ortamlarda saklanabilir.

Elektronik ortamlar, sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.), yazılımlar (ofis yazılımları, portal vb.), bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit, engelleme, günlük kayıt dosyası, anti virüs vb.), yedekleme kartuşları, kişisel bilgisayarlar (masaüstü, dizüstü), mobil cihazlar (telefon, tablet vb.), optik diskler (CD, DVD vb.), çıkartılabilir bellekler (USB, hafıza kartı vb.) ve yazıcı, tarayıcı, fotokopi makinesi vb. diğer elektronik veri kayıt ortamlarıdır.

6.2. Elektronik Olmayan Kayıt Ortamları

* Yazılı, basılı ortamlar ve manuel veri kayıt sistemleri gibi elektronik olmayan kayıt ortamları, fiziksel kayıtlar, kâğıt üzerindeki kayıtlar, fotoğraflar ve sözleşmeler gibi kağıt, mikro fiş ve benzeri ortamlarda bulunan kayıtlardan oluşur.
* Aktif kayıtlar ve kolayca erişilmesi gereken kayıtlar Kurum’un ofis ortamında depolanabilir.
* Aktif olmayan kayıtlar Kurum’un arşivlerine gönderilir.

7. kişisel verilerin saklanmasını ve imhasını gerektiren sebepler

7.1. Saklama ve İmhaya İlişkin Hukuki Sebepler

Kurum kişisel verileri;

* 213 sayılı Vergi Usul Kanunu,
* 2004 sayılı İcra İflas Kanunu,
* 4857 sayılı İş Kanunu,
* 5237 sayılı Türk Ceza 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,
* 6102 sayılı Türk Ticaret Kanunu,
* 6098 sayılı Türk Borçlar Kanunu,
* 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
* 6698 Sayılı Kişisel Verilerin Korunması Kanun’u, ilgili yönetmelikleri gereği ve bunlarla sınırlı olmamak üzere yayınlanan diğer mevzuat hükümleri,

Gereğince işlemekte, saklamakta ve ilgili şartların gerçekleşmesi durumunda imha yöntemlerini kullanarak silmekte, yok etmekte veya anonim hale getirmektedir.

7.2. Saklamayı Gerektiren Amaçlar

Kurum, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklamaktadır:

* 5393 Sayılı Belediye Kanunu ve 2464 Sayılı Belediye Gelirleri Kanunu kapsamındaki yükümlülüklerin yerine getirilmesi,
* 1319 Sayılı Emlak Vergisi Kanunu, 2886 Sayılı Devlet İhale Kanunu, 657 Sayılı Devlet Memurları Kanunu, 4734 Sayılı Kamu İhale Kanunu, 3071 Sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun, 3194 Sayılı İmar Kanunu, 5326 Sayılı Kabahatler Kanunu, 4982 Sayılı Bilgi Edinme Hakkı Kanunu, 213 Sayılı Vergi Usul Kanunu ve diğer vergi kanunları çerçevesinde iş ve işlemlerin yürütülmesi,
* İş Kanunu ve Türk Borçlar Kanunu kapsamında çalışanlara ilişkin sorumlulukların yerine getirilmesi,
* Acil durum yönetimi süreçlerinin yürütülmesi,
* Bilgi Güvenliği süreçlerinin yürütülmesi,
* Çalışan adaylarının başvuru süreçlerinin yürütülmesi,
* Çalışanlar için iş sözleşmesi ve ilgili mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesi,
* Denetim faaliyetlerinin yürütülmesi,
* Erişim yetkilerinin yürütülmesi,
* Faaliyetlerin mevzuata uygun sürdürülmesi,
* Fiziksel mekân güvenliğinin temini ve ziyaretçi kaydının tutulması,
* Görevlendirme süreçlerinin yürütülmesi,
* Hukuk işlerinin takibi ve yürütülmesi,
* İç Denetim, disiplin ve soruşturmalara ilişkin faaliyetlerin yönetilmesi,
* İletişim faaliyetlerinin yürütülmesi,
* İnsan kaynakları süreçlerinin planlanması ve yürütülmesi,
* İş faaliyetlerinin yürütülmesi ve denetlenmesi,
* İş Sağlığı/Güvenliği faaliyetlerinin yürütülmesi,
* İş Süreçlerinin iyileştirilmesine yönelik önerilerin alınması ve değerlendirilmesi,
* İş sürekliliğinin sağlanmasına yönelik faaliyetlerin yönetilmesi,
* Performans değerlendirme süreçlerinin yönetilmesi,
* Veri saklama ve arşiv faaliyetlerinin yürütülmesi,
* Talep ve şikâyetlerin takibi,
* Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi,
* Yönetim faaliyetlerinin yürütülmesi.

7.3. İmhayı Gerektiren Sebepler

Kişisel veriler aşağıda belirtilen hallerde Kurum tarafından resen veya ilgili kişinin talebi üzerine imha yöntemleri kullanılarak silinir, yok edilir veya anonim hale getirilir:

* İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
* İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
* Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
* Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
* Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verilen cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kuruluna 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.

8. İDARİ VE TEKNİK TEDBİRLER

8.1. İdari Tedbirler

Kurum, işlediği kişisel verilerin hukuka uygun olarak işlenmesi ve muhafazasının sağlanması ile kişisel verilere hukuka aykırı erişimin engellenmesi için aşağıdaki idari tedbirleri almaktadır:

* Kişisel verilerin korunması ve işlenmesi ile kişisel verilerin saklanması ve imhası konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
* Kişisel veri işleme envanteri hazırlanmıştır.
* Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması hakkında eğitimler verilmektedir.
* Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
* Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
* Sözleşme ve diğer belgelerine kendileri ile paylaşılan kişisel verilerin gizliliğine, bu verilerin ne şekilde işleneceğine ve saklanacağına ilişkin veri güvenliği hükümleri konulmaktadır.

8.2. Teknik Tedbirler

Kurum, işlediği kişisel verilerin hukuka uygun olarak işlenmesi ve muhafazasının sağlanması ile kişisel verilere hukuka aykırı erişimin engellenmesi için aşağıdaki teknik tedbirleri almaktadır:

* Kurum, kişisel verilere erişimi, veri işleme konusunda açıkça yetkilendirilmiş çalışanları ile sınırlandırmaktadır. Kurum çalışanlarının görevleri gereği kullanmadıkları kişisel verilere erişimleri sınırlandırılmaktadır.
* Kişisel verilerin saklandığı sisteme ve konumlara ilgilisinin dışındaki erişimin engellenmesi için gerekli teknik önlemler alınmakta ve alınan önlemler dönemsel olarak güncellenmektedir.
* Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
* Kişisel verilerin korunmasını sağlamaya yönelik gerekli olan virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar, yazılım ve sistemler Kurum tarafından kurulmaktadır.
* Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
* Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

9. saklama ve periyodik imha süreleri

Kurum, kişisel verileri ilgili mevzuatta belirtilen süre boyunca saklamaktadır. Mevzuatta kişisel verilerin saklanmasına ilişkin herhangi bir süre öngörülmemiş ise, kişisel veriler ticari hayatın teamülleri gereğince işlenmesinin gerektiği ya da işlendikleri amaç için gerekli olan süre kadar işlenmektedir. Bu çerçevede öncelikle ilgili mevzuatta kişisel verinin saklanması için bir süre öngörülüp öngörülmediği tespit edilmekte, mevzuatta bir süre öngörülmüşse bu süre kadar, yoksa kişisel verinin işlendiği amaç için gereken süre kadar ilgili kişisel veri saklanmaktadır. Saklama sürelerinin sonunda kişisel veri, periyodik imha sürelerine veya veri sahibinin başvurusuna göre ve belirlenmiş olan imha yöntemlerine göre silinmekte, yok edilmekte ya da anonim hale getirilmektedir.

Kurum tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

* Süreçler ve departmanlara bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
* Veri kategorileri bazında saklama süreleri VERBİS’e kayıtta yer alır.

Kişisel verilerin saklanma ve imha süreleri aşağıdaki tabloda gösterilmiştir.

|  |  |  |
| --- | --- | --- |
| VERİ TÜRÜ | SAKLAMA SÜRESİ | İMHA SÜRESİ |
| İnsan Kaynakları Verisi-İş Başvurusu | Başvurunun yapıldığı tarihten itibaren 1 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İnsan Kaynakları Verisi- Özlük Dosyası | İşten Ayrılmasını Takip Eden Yıldan İtibaren 30 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İnsan Kaynakları-Özel Nitelikli Kişisel Veriler | Veri konusu kişi grubu ve verinin niteliğine göre 1, 10 ve 30 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Finans/Muhasebe Verileri | Mali Takvim Yılını Takip Eden Yıldan İtibaren 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Mal ve Hizmet Satın Alınan Gerçek Kişiler ile Tüzel Kişilerin Çalışanları ve Yetkilileri Verileri | İş ilişkisinin sona ermesinden itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sözleşmelere İlişkin ve Sözleşme Kapsamında Yer Verilen Veriler ile Sözleşmeden Kaynaklı İlişkilerde İşlenen Kişisel Veriler | Sözleşmenin sona ermesinden itibaren 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Görsel ve İşitsel Veriler | Veri konusu kişi grubuna göre 1 yıl veya 10 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Ziyaretçi Kayıtları | Kayıt tarihinden itibaren 1 yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Kamera Kayıtları | Kayıt tarihinden itibaren 2 ay | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

Kurum, Yönetmelik gereğince periyodik imha süresini 6 ay olarak belirlemiştir. Politika bağlamında, saklama takvimi kaydın oluşturulduğu takvim yılının sonunda başlar. Saklama süresi dolmuş kayıtlar Kurumda her yıl Haziran ve Aralık aylarında olmak üzere iki kez gerçekleştirilen periyodik imhaya tabi tutulur. Bir kişisel verinin işleme amacının ortadan kalktığı tarih bu iki dönemden hangisine daha yakınsa o dönemde İmha edilir.

10. kişisel verilerin imha teknikleri

Kurum tarafından KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenen kişisel veriler, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, Kurum tarafından resen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak silinerek, yok edilerek veya anonim hale getirilerek imha edilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde;

* İlgili mevzuatta kişisel verilerin işlenmesinde uyulması gerekli görülen genel ilkelere,
* Veri sorumlularının veri güvenliğine ilişkin yükümlülükleri kapsamında alınması gereken idari ve teknik tedbirlere,
* Kişisel Verileri Koruma Kurulu kararlarına,
* Kişisel verilerin saklanması ve imhası politikasına uygun hareket edilmektedir.

10.1. Kişisel Verilerin Silinmesi

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

Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Silme işlemi için öncelikle silme işlemine konu teşkil edecek kişisel veriler belirlenmekte ve her bir kişisel veri için ilgili kullanıcılar tespit edilmektedir. Bunu takiben ilgili kullanıcıların erişim, geri getirme ve tekrar kullanma gibi yetkileri ve kullandıkları yöntemler tespit edilerek işbu yetkiler ortadan kaldırılmaktadır.

Verilerin silinmesi ile ilgili aşağıdaki yöntemler kullanılır:

1. **Hizmet Olarak Uygulama Türü Bulut Çözümleri**

Bulut sisteminde veriler silme komutu verilerek silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilir.

1. **Kâğıt Ortamında Bulunan Kişisel Veriler**

Kâğıt ortamında 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 sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

1. **Merkezi Sunucuda Yer Alan Kişisel Veriler**

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması sağlanır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına da dikkat edilir.

1. **Taşınabilir Medyada Bulunan Kişisel Veriler**

Taşınabilir medyalarda taşınan veriler şifreli olarak saklanmakta ve bu araçlarda gizli seviyede hiçbir veri taşınmamaktadır. Taşınabilir ortamda olan kişisel veriler, söz konusu donanıma uygun yazılımlar ile silinir.

1. **Veri Tabanları**

Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

10.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kurum, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel veriler, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilir.

1. **Yerel Sistemler**

Yerel sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılır.

● **De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

● **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi sağlanır.

● **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1’lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

1. **Çevresel Sistemler**

Ortam türüne bağlı olarak kullanılan yok etme yöntemleri aşağıda yer almaktadır:

● **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanlarının, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da Yukarıda ‘Yerel Sistemler’ için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.

● **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yukarıda ‘Yerel Sistemler’ için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.

● **Veri kayıt ortamı çıkartılabilir olan yazıcı çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göreYukarıda ‘Yerel Sistemler’ için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

● **Veri kayıt ortamı sabit olan yazıcı gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Yukarıda ‘Yerel Sistemler’ için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Bulut Sistemler:** Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi sağlanır.

10.3. 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 alıcı grupları 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. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiyi işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Kurum, kişisel verilerin silinmesi veya yok edilmesi yerine anonim hale getirilmesi sürecinde gerekli her türlü teknik ve idari tedbirleri alır. Kişisel verilerin anonim hale getirilmesi, Kişisel Verilerin Silinmesi Yok edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte belirtilen esaslara ve Kişisel Verilerin Korunması Kurumunun konuya ilişkin yayınladığı rehberdeki yöntemlere uygun olarak yapılır.

Kurum, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmek için aşağıdaki şartların yerine getirilmesini arar ve işbu şartların yerine getirilmiş olmasını sağlar:

● Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulmaması,

● Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturmaması,

● Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

11. politikanın yürürlüğü

Kurum tarafından kişisel verilerin saklanması ve imhasında uygulanmak üzere yürürlükteki mevzuatla uyumlu olarak hazırlanan bu Politika, Kurum Yönetim Kurulunun kararı ile yürürlüğe konulmuştur.

Bu politika Kurumun internet sayfasında yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur. Bu Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.