

Kişisel Veri Saklama Ve İmha Politikası

1. GİRİŞ VE POLİTİKA'NIN HAZIRLANMA AMACI VE KAPSAMI

6698 sayılı Kişisel Verilerin Korunması Kanunu, 2010 yılında kişisel verilerin korunmasının Anayasal bir hak olmasının ardından 2016 yılında yürürlüğe girmiş kişisel verilerin işlenmesi aşamasında özel hayatın gizliliği ilkesini muhafaza etmek ve temel hak ve özgürlüklerin zarar görmemesi adına geliştirilmiş bu konu hakkında usul ve esasları gösteren hukuki bir koruma aygıtıdır.

6698 Sayılı Kanunun ("KVKK" ya da "Kanun") 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumlularının, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlama yükümlülüğü vardır. İşbu Kişisel Veri Saklama ve İmha Politikası, 6698 sayılı Kanun ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin GENOKS Genetik Hastalıklar Değerlendirme Merkezi ("Merkez") tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır. Merkezimiz saklama ve imha konusunda usul ve esasları, 30808 sayılı Kişisel Sağlık Verileri Hakkında Yönetmelik doğrultusunda belirlenmektedir. Kanun'un ikincil düzenlemesi olan 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca hazırlanmıştır. Merkez olarak yükümlülüklerimizi yerine getirmek için hazırlamış olduğumuz kişisel veri saklama ve imha politikası asgari olarak;

- Kişisel veri saklama ve imha politikasının hazırlanma amacına,
- Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,
- Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
- Kişisel verilerin saklanması ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,
- Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
- Saklama ve imha sürelerini gösteren tabloya,
- Periyodik imha sürelerine,
- Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe, ilişkin bilgileri kapsar.

2. TANIMLAR

Kanun/KVKK, resmi Gazetede yayınlanması ile 07/04/2019 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kurul, Kişisel Verileri Koruma Kurulu Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi Açık Rıza, belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza Kişisel Veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her tür bilgi 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 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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem İmha, Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.

- Kişisel verilerin silinmesi, ilgili kullanıcı için verinin hiçbir şekilde kullanılamaz hale getirilmesi işlemi,

Kişisel Veri Saklama Ve İmha Politikası

- Kişisel verilerin yok edilmesi, verinin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,
- Anonim Hale Getirme, kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi. Kayıt Ortamı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu ortam Elektronik Kayıt Ortamı, kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar Elektronik Olmayan Kayıt Ortamı, elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar

Kişisel veri işleme envanteri, veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 envanteri

Kişisel veri saklama ve imha politikası, veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika Periyodik imha, kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi Veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini, Kişisel Verileri Koruma Kanununun ve Yönetmeliğin Tanımladığı Özneler Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel 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 Alıcı Grubu, veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi İlgili kişi, kişisel verisi işlenen gerçek kişi 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,

3.GENEL BİLGİLENDİRME VE TEMEL İLKELER

1. Kanun'un 5 ve 6 ncı maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel veriler veri sorumlusu sıfatıyla Merkezimiz tarafından re'sen veya ilgili kişinin talebi üzerine silinip, yok edilmekte veya anonim hale getirilmektedir.
2. İlgili kişinin Kanun 'nun 11 nci maddesinde yazılı herhangi bir hakkını kullanmak adına tarafımıza iletmış olduğu talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir.
3. Merkez kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4 üncü maddesindeki genel ilkeler ile 12 nci maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket etmektedir.
4. Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Merkez tarafından kayıt altına alınmaktadır. 5. Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını veri sorumlusu sıfatıyla seçmekteyiz. Ancak, ilgili Kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilebilecektir.

Kişisel Veri Saklama Ve İmha Politikası

4.KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler, tarafından aşağıda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır: Merkezde tutulan kayıt defterleri, elektronik ortamda da tutulabilir. Hastaların sağlık bilgilerine ait gerekli kayıtların elektronik ortamda saklanması, değiştirilmesinin ve silinmesinin önlenmesi ve gizliliğin ihlal edilmemesi için fiziki, manyetik veya elektronik müdahalelere ve olası suistimallere karşı gerekli idari ve teknik tedbirler alınır. Merkez tarafından fiziki ortamda tutulan kayıtların her türlü suistimale karşı korunmasına yönelik gerekli idari ve teknik tedbirler alınır. Bu konudaki gerekli idari ve teknik tedbirlerin alınmasından ve periyodik olarak denetlenmesinden mesul müdür sorumludur. Elektronik ortamdaki veriler, güvenli yedekleme sistemiyle düzenli olarak yedeklenir.

A.ELEKTRONİK ORTAMLAR: 1. Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) 2. Yazılımlar (ofis yazılımları, muhasebe yazılımları) 3. Kişisel bilgisayarlar (Masaüstü, dizüstü) 4. Mobil cihazlar (telefon,tablet .) 5. Optik diskler (CD, DVD vb.) 6. Çıkartılabilir bellekler (USB, Hafıza Kart vb.) 7. Yazıcı, tarayıcı, fotokopi makinesi 8. Pos Makinaları 9. Ödeme Kaydedici Cihazlar 10. Laboratuvar Cihazları

B.ELEKTRONİK OLMAYAN ORTAMLAR: 1. Kağıt 2. Manuel veri kayıt sistemleri 3. Yazılı, basılı, görsel ortamlar

5.KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

İşlenen kişisel veriler, Merkezdeki ürün ve hizmetlerinin türü ve niteliğine göre değişebilmektedir. İlgili kişilere ait kişisel veriler, veri sorumlusu sıfatıyla merkezimiz tarafından kanunlarda açıkça öngörülmesi, verilen sağlık hizmetinin gerektirdiği ölçüde işlenmesi, sözleşme kurulması ve ifası , ticari ve iş stratejilerinin belirlenmesi; iş akdi, satış ve hizmet sözleşmeleri gibi karşılıklı edimlerin ifası için gerekli olan çalışan ve hastalara ait verileri fiziki veyahut elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır. Daha açık bir ifadeyle saklamayı gerektiren hukuki amaç ve sebepler aşağıdaki gibidir: Amaçlar; 1. Faaliyet konusu sağlık hizmetinin kanunlarda öngörüldüğü şekilde verilebilmesi, 2. Ticari faaliyetlerin sürdürülebilmesi, 3. Hukuki yükümlülüklerin yerine getirilebilmesi, 4. Çalışan haklarının ve yan haklarının planlanması ve ifası, 5. Çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi, 6. Hasta ilişkilerinin yönetebilmesi, 7. Hastalara ait bir hakkın tesisi, kullanılması veya korunması, 8. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaati için veri işlemenin zorunlu olması, 9. İlgili Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi, 10. KVKK Madde 5/2'de sayılan şartlardan birinin varlığından söz edilemeyecek durumlarda, saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması , Hukuki Dayanaklar ; 1. 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2. 6102 sayılı Türk Ticaret Kanunu, 3. 6098 sayılı Türk Borçlar Kanunu, 4. 213 Sayılı Vergi Usul Kanunu, 5. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 6. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 7. 4857 sayılı İş Kanunu, 3308 sayılı Mesleki Eğitim Kanunu, 8. 2547 sayılı Yükseköğretim Kanunu, 5434 sayılı Emekli Sandığı Kanunu, 9. 2828 sayılı Sosyal Hizmetler Kanunu , 10. İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik, 11. 3359 sayılı Sağlık Hizmetleri Temel Kanunu, 12. Genetik Hastalıklar Değerlendirme Merkezleri Yönetmeliği, 13. Kişisel Sağlık Verileri Hakkında Yönetmelik Sayı : 30808, 14. İnsan Doku ve Hücreleri ile Bunlarla İlgili Merkezlerin Kalite ve Güvenliği Hakkında Yönetmelik, 15. 29.05.1979 tarihli ve 2238 sayılı Organ ve Doku Alınması, Saklanması ve Nakli Hakkında Kanun, 16. Ayakta Teşhis Ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik, Yönetmelik ve kanunun çizdiği sınırlar çerçevesinde, aşağıda sayılan hallerde talep ile veya re'sen Merkezimiz tarafından; 1. İlgili kişinin, Kanun'un 11 inci maddesindeki haklarını kullanmak suretiyle

Kişisel Veri Saklama Ve İmha Politikası

verilerinin silinmesini, yok edilmesini veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabulü, 2. Veri sorumlusunun, ilgili kişinin Kanun'un 11 inci maddesindeki haklarını kullanarak başvurmasına karşın cevap vermemesi, başvuruyu reddetmesi ya da cevabın yetersiz olması sebepleriyle ilgili kişinin Kurul'a şikayette bulunması ve Kurul tarafından uygun bulunması, 3. Kişisel verinin açık rıza ile işlenmiş bulunup, ilgili kişinin bu açık rızasını geri alması, 4. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, 5. Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası, 6. Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması, 7. Kanun'un 5. Ve 6. Maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması hallerinde SİLİNİR, YOK EDİLİR, ANONİM HALE GETİRİLİR. 6. TEKNİK VE İDARİ TEDBİRLER 1 İlgili kişinin hakları MADDE 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir. Kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi; hukuka uygun olarak imha edilmesi için veri sorumlusu Merkezimiz tarafından alınmış idari ve teknik tedbirler aşağıda sayılmıştır.

6.1 MERKEZİMİZ TARAFINDAN ALINAN TEKNİK VE İDARİ TEDBİRLER

1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır. 2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır. 3. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur. 4. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır. 5. Çalışanlar için yetki matrisi oluşturulmuştur. 6. Erişim logları düzenli olarak tutulmaktadır. 7. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır. 8. Gerektiğinde veri maskeleyme önlemi uygulanmaktadır. 9. Gizlilik taahhütnameleri yapılmaktadır. 10. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır. 11. Güncel anti-virüs sistemleri kullanılmaktadır. 12. Güvenlik duvarları kullanılmaktadır. 13. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir. 14. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir. 15. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir. 16. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır. 17. Kişisel veri güvenliğinin takibi yapılmaktadır. 18. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır. 19. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır. 20. Kişisel veri içeren ortamların güvenliği sağlanmaktadır. 21. Kişisel veriler mümkün olduğunca azaltılmaktadır. 22. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır. 23. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır. 24. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır. 25. Mevcut risk ve tehditler belirlenmiştir. 26. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve 27. uygulanmaktadır. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal

Kişisel Veri Saklama Ve İmha Politikası

posta hesabı kullanılarak gönderilmektedir. 28. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir. 29. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir. 30. Şifreleme yapılmaktadır. 31. Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır. 32. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır. 33. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır. 34. Veri kaybı önleme yazılımları kullanılmaktadır.

7. SAKLAMA VE İMHA SÜRELERİ

Veri sorumlusu Merkezimiz tarafından Kanun ve ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin saklama ve imha sürelerinin tespitinde aşağıda belirtilen ölçütlerden yararlanılmaktadır: 1. Kanun veya yönetmeliklerde, kişisel verinin saklanmasına ve imhasına ilişkin öngörülmüş olan süreye uyulmaktadır. Anılan sürenin sona ermesi akabinde veri hakkında 2 nci bent kapsamında işlem yapılır. 2. Söz konusu kişisel verinin saklanmasına ilişkin olarak kanunda veya yönetmeliklerde öngörülen sürenin sona ermesi veya ilgili söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla; • Kanun'un 6 ncı maddesine göre özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının şirket açısından önem derecesine göre belirlenir. • Verinin saklanmasının Kanun 'nun 4 üncü maddesinde belirtilen ilkelere uygunluğu sorgulanır. Saklanmasının Kanun 'nun 4 üncü maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir. • Verinin saklanmasının Kanun'nun 5 ve 6 ncı maddelerinde öngörülmüş olan istisnalardan hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.

8. KİŞİSEL VERİLERİN İMHA USULLERİ

1. Kişisel Verilerin Silinmesi Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, şirketimiz, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmiştir. Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır: 1.1. Hizmet Olarak Uygulama Türü Bulut Çözümleri Bulut sisteminde veriler silme komutu verilerek silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisi bulunmamaktadır. 1.2. Kağıt Ortamında Bulunan Kişisel Veriler 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 yapılmaktadır. 1.3. Merkezi Sunucuda Yer Alan Ofis Dosyaları Dosyanın işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir. 1.4. Taşınabilir Medyada Bulunan Kişisel Veriler Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir. 1.5. Veri Tabanları Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmektedir. 1.6. Şirketimiz Tarafından Kullanılan Yöntemler 1.6.1. Kağıt Ortamında Bulunan Kişisel Veriler İçin: Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri

Kişisel Veri Saklama Ve İmha Politikası

döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılmaktadır. 1.6.2. Merkezi Sunucuda Yer Alan Ofis Dosyaları İçin: Dosyanın işletim sistemindeki silme komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir. 1.6.3. Taşınabilir Medyada Bulunan Kişisel Veriler İçin: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir. 1.6.4. Veri Tabanlarında Bulunan Kişisel Veriler İçin: Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile (DELETE vb.) silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmektedir. 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 Şirketimiz kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmiştir. Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilir ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmektedir: 2.1. Yerel Sistemler Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılmaktadır. 2.1.1. De-manyetize Etme Manyetik medyanın özel bir cihazdan geçirilerek yüksek değerde bir manyetik alana maruz bırakılarak üzerindeki veriler okunamaz biçimde bozulmaktadır. 2.1.2. 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 erişilemez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medya da fiziksel olarak yok edilmektedir. 2.1.3. 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. 2.2. Çevresel Sistemler Ortam türüne bağlı olarak kullanılan yok etme yöntemleri aşağıda yer almaktadır: 2.2.1. Ağ cihazları (switch, router vb.) Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. 2.2.2. Flash tabanlı ortamlar Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa 'block erase' komutunu, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini ya da yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. 2.2.3. Manyetik bant Verileri esnek bant 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 edilmektedir. 2.2.4. 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 edilmektedir. 2.2.5. Mobil telefonlar (Sim kart ve sabit hafıza alanları) Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yerel belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. 2.2.6. Optik diskler CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir. 2.2.7. Veri kayıt ortamı Çıkarılabilir yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre yerel sistemlerde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. 2.2.8. Veri kayıt ortamı sabit yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri Söz konusu sistemlerin çoğunda silme komutu bulunmakta,

Kişisel Veri Saklama Ve İmha Politikası

ancak yok etme komutu bulunmamaktadır. Yerel belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir. 2.3. Kağıt ve Mikrofiş Ortamları Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılabilir boyutta, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre yerel sistemlerde belirtilen yöntemlerin bir ya da birkaçı kullanılarak yok edilmektedir. 2.4. Bulut Ortamı 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 kullanılmaktadır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilmektedir. Yukarıdaki ortamlara ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir: i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin yerel sistemlerde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi, ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi, iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması, yöntemlerinden biri kullanılmaktadır. 2.5.Şirketimiz Tarafından Kullanılan Yöntemler 2.5.1. Optik diskler: Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir. 2.5.2. Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma usulleri ile anlaşılabilir boyutta, geri birleştirilemeyecek şekilde küçük parçalara bölünmektedir. 3. Kişisel Verilerin Anonim Hale Getirme 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. Veri Sorumlusu olarak, halihazırda kişisel verilerin anonimleştirilmesi yöntemini kullanmamaktayız. Söz konusu imha yönteminin Merkezimizde kullanılması halinde, Saklama ve İmha Politikamızda gerekli güncellemeler tarafımızca yapılacaktır.

9. PERSONEL (KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASINDA YER ALAN) UNVAN, BİRİM VE GÖREV LİSTESİ

Veri Sorumlusunun 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 saklanması 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 ait dağılım aşağıdaki tabloda verilmiştir.

BİLGİ İŞLEM MÜDÜRÜ, BİLGİ İŞLEM BİLGİ İŞLEM DEPERTMANI KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI UYGULAMA

Kişisel Veri Saklama Ve İmha Politikası

SORUMLUSU,
VERİLERİN SAKLAMA SÜRESİNE UYGUNLUĞUNU SAĞLAMA VE PERİYODİK İMHA SÜRESİ
İÇİNDE İMHA SÜRECİNİ YÖNETMEK.

MUHASEBE MÜDÜRÜ, MUHASEBE
MALİ İŞLER DEPARTMANI KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI UYGULAMA
SORUMLUSU,
VERİLERİN SAKLAMA SÜRESİNE UYGUNLUĞUNU SAĞLAMA VE PERİYODİK İMHA SÜRESİ
İÇİNDE İMHA SÜRECİNİ YÖNETMEK.

10. SAKLAMA VE İMHA SÜRELERİ TABLOSU Merkez tarafından, faaliyetler kapsamında işlenmekte olan kişisel verilerle ilgili olarak; • Departmanlara bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde (anılan Envanter'e <http://www.GENOKS.com.tr/> linki üzerinden erişilebilecektir); • Veri kategorileri bazında saklama süreleri VERBİS'e kayıta yer almaktadır. Aşağıda ise süreçler bazında oluşturulan Saklama ve İmha Tablosu bulunmaktadır.

SAĞLIK HİZMETİ SÜREÇLERİ Hukuki İlişki Süresi + 30 Yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde KAMERA KAYDI 3 Ay Saklama süresinin bitimini takip eden ilk periyodik imha süresinde İNSAN KAYNAKLARI SÜREÇLERİNİN YÜRÜTÜLMESİ Hukuki İlişki Süresi + 10 Yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde VERGİ VE SGK İŞLEMLERİ Hukuki İlişki Süresi + 10 Yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde BORDRO Hukuki İlişki Süresi + 10 Yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde İŞE ALIM FAALİYETİ Saklama süresinin bitimini takip eden ilk periyodik imha süresinde HASTA AÇIK RIZA SÜREÇLERİ 10 Yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde ELEKTRONİK ORTAMDA TUTULAN SAĞLIK HİZMET SÜREÇ VERİLERİ Süresiz

11. GÜNCELLEMELER İşbu politikada, kanun ve yönetmeliklere ve veri sorumlusu sıfatına haiz Merkezimizin aldığı kararlara göre yapılan değişiklikler aşağıdaki tablodadır.

GÜNCELLEME TARİHİ DAYANAK DEĞİŞİKLİĞİN KAPSAMI FAALİYET SAKLAMA SÜRESİ İMHA SÜRESİ

12.PERİYODİK İMHA SÜRESİ Yönetmeliğin 11 inci maddesi gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, veri sorumlusu tarafından her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

13. POLİTİKA'NIN YAYINLANMASI, SAKLANMASI VE GÜNCELLENMESİ: Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda saklanır ve sitesinde yayınlanır. İhtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. İşbu politika imza tarihinden itibaren yürürlüğe girmiş kabul edilir. 14. REFERANS DÖKÜMANLAR -6698 Sayılı Kişisel Verilerin Korunması Kanunu -30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Kişisel Veri Saklama Ve İmha Politikası

14. REFERANS DÖKÜMANLAR

-6698 Sayılı Kişisel Verilerin Korunması Kanunu

-30224 Sayılı 28.10.2018 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik