Kişisel Verileri Saklama ve İmha Politikası

Doküman Kontrolü

Doküman Başlığı	Kişisel Verileri Saklama ve İmha Politikası	
Doküman No	GLT-KVKK-04	
İlk Yayın Tarihi	15.10.2021	
Rev No	İlk Yayın	
Son Revizyon Tarihi	15.10.2022	
Referans	6698 Kişisel Verilerin Korunması Kanunu	

Revizyon Geçmişi

Rev. No.	Revizyon Tarihi	Revizyon Yapan	Revizyon Açıklaması

Doküman Onayı

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ SORUMLUSU	İÇ KONTROL	**ÜST YÖNETİM**

İçindekiler

1. Amaç

Bu politika, Galata Menkul Değerler A.Ş Bünyesinde işletilen süreçlerde toplanan, işlenen, saklanan ve paylaşılan verilerin tespit edilmesi ve korunması için gerekli olan yöntemleri tanımlar.

2. Kapsam

Bu politikada bahsi geçen veri yönetimi faaliyetleri kuruluşun sahip olduğu, emanetçisi olduğu (kuruluş dışındaki paydaşlara ait) verilere uygulanır.

3. Tanımlar

Kurum (Kuruluş): Galata Menkul Değerler A.Ş

Paydaş: Galata Menkul Değerler A.Ş kapsamında yürütülen faaliyetlerden olumlu veya olumsuz bir şekilde doğrudan veya dolaylı bir şekilde etkilenecek gerçek veya tüzel kişiler

Üçüncü Taraf: Kuruluşa sözleşme ile hizmet sağlayan tüzel kişiler ve personelleri

Kişisel Veri İşleme Envanteri: Kurum'un iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı envanter

Personel: Kurtuluş'ta çalışan insan kaynağı

Bilgi Güvenliği: Kuruluş bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunması

Veri: Değerli olan ve sayısal/basılı olarak saklanabilen, tanımlanabilir bilgi parçası

Veri Kaybı/sızıntı önleme (DLP): Kişisel verilerin, yanlışlıkla ya da kötü niyetli kişilerce kurum dışına çıkarılmasına engel olan ya da engel olmadan işlemi raporlamaya yarayan yazılım

4. Verilerin Korunması

4.1. Verilerin Sınıflandırılması

Koruyucu önlemlerin alınabilmesi amacıyla veriler değerine, yasal gereksinimlere, hassasiyetine ve kritikliğine göre sınıflandırılır. Verinin korunması için yapılacak olan yatırımların verinin değerinden fazla olmaması için verilerin doğru şekilde sınıflandırılması önemlidir.

Veri sınıflandırma işlemi aşağıda tanımlanan dereceler kullanılarak gerçekleştirilir.

Gizli

Bilginin, müşterinin işlem yapma amacı veya talimatı ve Kurum'un aracılık fonksiyonunu ifası için zorunlu olan haller dışında, Kuruluş dışına çıkması durumunda ciddi kayıplar/zararlar oluşabilir. Bilginin, yasal zorunluluklar, müşterinin ve Kurum'un karşılıklı ve uyumlu menfaati, müşteri talimatının ifası için gerekli işlemler dışında tehlikeye atılması ilgili mevzuata uyumsuzluk sonucunu doğurabilir. Bilgiye erişim "bilmesi gereken ilkesi" ne uygun olarak kısıtlanmalıdır. Bilmesi gereken ilkesi, veriyi kullanacak kişinin, yaptığı işi ve görevi için gerekli olandan fazla veriye sahip olamamasını ifade eder.

- Kuruluş iş süreçlerinde kullanılan aşağıdaki müşteri verileri ve bu verilerin içerisinde bulunduğu Office Dokümanları ve E-postalar "Gizli" olarak sınıflandırılır.
    - Müşteri Telefonu

- Müşteri Adresi
- Müşteri E- postası
- Müşteri VKN
- Müşteri TCKN
- Müşteri IBAN
- Müşteri Hesap Kayıtları
- Müşteri Telefon Görüşme Kayıtları

- Kuruluşta çalışan personele ve aday personele ait aşağıda belirtilen kişisel veriler ve bu verilerin içerisinde bulunduğu Office Dokümanları ve E-postalar "Gizli" olarak sınıflandırılır.
  - TCKN
  - IBAN
  - Telefon
  - E-posta

- Kuruluşu ziyaret eden ziyaretçilere ait aşağıda belirtilen kişisel veriler ve bu verilerin içerisinde bulunduğu Office Dokümanları ve E-postalar "Gizli" olarak sınıflandırılır.
  - Telefon
  - E-posta

Hizmete Özel

Bilginin Kuruluş dışına çıkması durumunda göz ardı edilebilir düzeyde kayıp/sıkıntı yaşanabilir. Bilginin ifşası Kuruluşa ciddi bir zarar vermez, bilgiye erişim Kuruluş içerisindeki belirli birim/birimlere açıktır.

- Kuruluşta **Gizli** veri sınıfında **olmayan** verileri içeren ve Kuruluş iş süreçlerinde kullanılan tüm veriler ve bu verilerin içerisinde bulunduğu Office Dokümanları ve E-postalar "Hizmete Özel" olarak sınıflandırılır.

  - Müşteri Numarası
  - Müşterinin İşlemine Konu Sermaye Piyasası Aracının veya İşlemin Tanımı
  - Müşterinin İşlem Fiyatı
  - Müşterinin İşlem Tutarı
  - Müşterinin İşlem Maliyeti
  - Müşterinin İşlem Getirisi

Genel

Halka açık bilgilerdir. Bilgiye herhangi bir kişinin erişmesi Kuruluş için bir kayıp/zarar oluşturmaz. Genel bilgiler etiketlenmez. Örneğin, vizyon, misyon, organizasyon şeması, duyurular, temas noktaları, web sitesinde yayınlanan bilgiler vb.

- Kuruluşta oluşturulan ve web sitesi gibi halka açık alanlarda paylaşılan aşağıdaki doküman ve içerikleri Genel olarak sınıflandırılır.
  - Günlük Bülten
  - Veri Sağlayıcılardan Temin Edilen Borsa ve Piyasa Bilgileri
  - Resmî kurumların ve otoritelerin açıkladıkları her türlü veri
  - Kurum bünyesindeki verilerin istatistik veri (anonim hale getirilmiş) olarak sunulması

4.2. Verilerin Etiketlenmesi

Kuruluşta değerine, yasal gereksinimlere, hassasiyetine ve kritikliğine göre sınıflandırılan veriler aşağıdaki yöntemlere göre etiketlenir. Kuruluş personelinin etiketlendirme işlemini hatalı yaptığı durumda sistem tarafından otomatik bir mesaj ile işlediği verinin hangi sınıfa ait olduğu personele iletilir.

Veri gizlilik değeri taşıyorsa, gizlilik derecesi "Varlıkların Sınıflandırılması" başlığında tanımlanan derecelere göre aşağıdaki yöntemlere uygun olarak sınıflandırılır;

- Belge oluştururken, ilgili uygulamanın "Home" menüsünde yer alan "Manuel Classification" ikonuna tıkladıktan sonra çıkan ekrandan uygun olan sınıf seçilerek gerçekleştirilir. Uygulama, sınıflandırma işlemi yapılmadan belgenin kaydedilmesine ve çıktı alınmasına izin vermeyecektir.
- E-posta oluştururken, ilgili uygulamanın "Message" menüsünde yer alan "Manuel Classification" ikonuna tıkladıktan sonra çıkan ekrandan uygun olan sınıf seçilerek gerçekleştirilir. Uygulama, sınıflandırma işlemi yapılmadan e-postanın iletilmesine izin vermeyecektir.

4.3. Verilerin Korunması

Kuruluşa ait veriler ve gizlilik sınıfları veri envanterinde listelenir. Kuruluş verilerine yönelik uygulanacak güvenlik kontrolleri, gizlilik sınıflarına ve veri yapısına göre belirlenir. Kuruluşta uygulanacak güvenlik kontrolleri ve uyulması gereken kurallar aşağıda tanımlanmıştır.

Tüm personel Verilerin Etiketlenmesi başlığı altında belirtilen yöntem ile verilerini etiketlemek ile yükümlüdür. Etiketleme yapılmayan veriler ile ilgili aşağıda belirtilen kurallar uygulanacaktır.

- Etiketleme yapılmayan dokümanlar kaydedilemez.
- Etiketleme yapılmayan dokümanlar e-posta ile gönderilmez.
- Etiketleme yapılmayan dokümanların çıktısı alınmaz.
- Etiketleme yapılmayan e-postalar gönderilmez.
- Etiketleme yapılmayan dokümanlar USB, CD/DVD vb. medya cihazlarına kopyalanmaz.
- Etiketleme yapılmayan görseller (ekran görüntüleri, resim dosyaları vb.) e-posta ile paylaşılmaz, USB, CD/DVD vb. medya cihazlarına kopyalanmaz, çıktısı alınmaz.

Gizli

Gizli olarak nitelendirilen verileri içeren e-posta, dokümanlar (tüm dosya formatları), görseller vb. veriler Gizli sınıfı kurallarına göre değerlendirilir. Ayrıca Gizli veri içeren tüm dokümanlar, e-postalar, görseller vb. veriler Gizli olarak etiketlendirilmediği sürece işlem yapılamaz. Gizli etiketli veriler için aşağıda belirtilen kurallar uygulanacaktır.

- Alınan tüm ekran görüntüleri otomatik olarak Gizli sınıfında etiketlendirilir.
- Gizli etiketli verilerin Kuruluş içerisinde paylaşımı kayıt altına alınır.
- Gizli etiketli veriler (Sorumlu Birim Yöneticisi)'ne paydaş (kurum e-posta adresi, firma e-posta adresi vb.) iletmediği sürece Kurum dışı e-posta ile paylaşılamaz/aktarılamaz.
- Gizli etiketli veriler (Sorumlu Birim Yöneticisi)'ne paydaş (kişi, birim, grup vb.) belirtilmediği sürece çıktı alınamaz.
- Gizli etiketli veriler (Sorumlu Birim Yöneticisi)'ne paydaş belirtilmediği sürece web ara yüzü (cloud, web uygulamaları vb.) kullanılarak paylaşılamaz/aktarılamaz.
- Gizli etiketli veriler USB, CD/DVD vb. medya cihazlarına kopyalanmaz.

Hizmete Özel

Hizmete Özel olarak sınıflandırılan verileri içeren e-posta, sayısal dokümanlar (tüm dosya formatları), görseller vb. veriler Hizmete Özel sınıfı kurallarına göre değerlendirilir. Hizmete Özel etiketli veriler için aşağıda belirtilen kurallar uygulanacaktır.

- Gizli sınıfındaki verileri içeren Hizmete Özel etiketli veriler Gizli sınıfı kuralları ile değerlendirilir.
- Hizmete Özel etiketli verilerin Kuruluş içi paylaşımları kayıt altına alınır.
- Hizmete Özel etiketli veriler (Sorumlu Birim Yöneticisi)'ne paydaş (kurum e-posta adresi, firma e-posta adresi vb.) belirtilmediği sürece Kuruluş dışına e-posta ile paylaşılmaz.
- Hizmete Özel etiketli veriler USB, CD/DVD vb. medya cihazlarına kopyalanmaz.

Genel

- Gizli veya Hizmete Özel olarak sınıflandırılan verileri içeren Genel etiketli veriler ilgili sınıflandırma kuralları ile değerlendirilir.

5. Verilerin Saklanması ve İmhası

5.1. Kişisel Verilerin İmhasını Gerektiren Durumlar

5.1.1 Kanuna Aykırılık

Kurum, kişisel verileri Kanun'da belirtildiği şekle aykırı olarak işlemeyeceğini taahhüt eder.

Kurum, Kanun'un 5 ve 6. maddelerindeki kişisel verilerin işlenmesi şartlarındaki istisnalar mevcut olmadığı sürece;

a) Kanun'da belirtilen istisnalar dışında açık rızasını almadığı kişilerin kişisel verilerini saklamayacaktır.

b) İstisna kapsamında veya açık rıza kapsamında işlenen verilerin işleme amacının ortadan kalkması ve/veya yasal saklama sürelerinin dolması halinde Kurum bu kişisel verileri saklamayacak ve imha edecektir.

5.1.2 Kişisel Veri İşleme Şartlarının Ortadan Kalkması

Kurum, veri işlenme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu kişisel veri işleyen ilgili tüm çalışanları ile paylaşır.

Çalışanlar, veri işlenme şartlarının ortadan kalktığı durumlarda veri işlemeye devam etmeyecektir. Bu durumların tespiti ilgili iş biriminin önerisi ile İç Kontrol, Uyum ve Hukuk bölümü tarafından yapılır ve işbu Politika 'ya uygun şekilde imha işlemi gerçekleştirir.

Kurum aşağıda listelenen ve Yönetmelik içinde de belirtilen ilgili durumlarda veri işlenme şartlarının ortadan kalktığını kabul eder:

a) İlgili mevzuatın kişisel verileri işlemeye esas teşkil eden hükümlerinin değiştirilmesi veya yürürlükten kaldırılması;

b) Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçersiz olması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,

c) Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,

d) Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,

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

f) İlgili kişinin, Kanunun 11 inci maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı usule uygun başvurunun Kurum tarafından kabulü,

g) Kurum, ilgili kişi tarafından kişisel verilerinin imhası talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,

Kişisel verilerin saklanmasını gerektiren azami süre geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

6. KİŞİSEL VERİLERİN İMHASI

Kişisel verilerin imhası, aşağıda detaylıca açıklanan verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde üç farklı şekilde yapılabilir.

Kurum bünyesinde ilgili iş birimleri, söz konusu kişisel verilerin bulunduğu bilgi sistemleri ve uygulama sahipleri, İç Kontrol, Uyum ve Hukuk bölümü ve konuyla ilgili olabilecek diğer kişi ya da bölümler kişisel verilerin imhası için uygulanacak yönteme bu imhanın nedenine bağlı olarak yazılı karar verir. Bu yazılı karar gereğince işbu Politikanın G) maddesindeki imha yöntemlerinden biri Kurul'un yayınladığı Kişisel Verilerin Silinmesi Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi'ne bağlı olarak uygulanır.

Kişisel verilerin saklanması ve imhası için kullanılacak yöntemlerle ilgili Kurum ayrıca teknik kılavuzlar oluşturur ve bunların uygulanmasını sağlar.

Kişisel verilerin imhasının takibi Kurum içerisindeki ilgili veri sahibi iş biriminin sorumluluğundadır. Veri sahibi iş birimi, verilerin imhası için denetimi kendisi tarafından yapılmak kaydıyla Kurum'un farklı birimlerinden destek alır.

6.1. Kişisel Verilerin Silinmesi

Tamamen veya kısmen otomatik yollarla işlenen kişisel verilerin silinmesi; söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Herhangi bir veri kayıt sisteminin parçasını teşkil eden ve otomatik olmayan yollarla işlenen kişisel verilerin silinmesi sürecinde, yasal saklama süreleri göz önünde bulundurularak silme işlemine konu olacak kişisel veriler belirlenir. Kurum kişisel verilere erişim ve yetkilendirme anlamında Kurum'un mevcut durumda bilgi sistemleri ve uygulamaları üzerinde yürütmekte olduğu rol ve yetki matrisleri dahilinde güncellemelerini yapar ve ilgili kullanıcıları tespit eder. İlgili Kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkileri ve yöntemleri bu kapsamda tespit edilir.

Kurum, kişisel verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirir. Kurum, bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti eder.

6.2. Kişisel Verilerin Yok Edilmesi

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

Yok etme işlemi, Kurum'un verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve Kurum bu verileri tekrar geri getirilmesi mümkün olmayacak hale getirmekle yükümlüdür.

Kâğıt ve mikro fiş ortamları için bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta geri birleştirilemeyecek şekilde küçük parçalara bölünerek yok edilecektir. Ayrıca, Kurum bu kapsamda Üçüncü Taraflardan imha hizmeti alabilir.

6.3. Kişisel Verilerin Anonimleştirilmesi

Anonim hale getirme işlemi, Kurum'un kişisel verileri tamamen veya kısmen otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kurum, ilgili veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıları çıkartarak ya da değiştirerek, ilgili kişinin kimliğinin saptanabilmesini engelleyerek bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesini sağlar.

Verilerin anonimleştirilmesi sırasında Kurum, tek yönlü fonksiyonlar ile şifreleme gibi yöntemler kullanabilir.

7. Kişisel Verilerin İmha Süreci ve Yöntemleri

Kişisel verilerin imhası için Kurum, imha sırasında kullanılabilecek tüm yöntemleri İşbu Politika ve eklerinde tanımlar. Veri sahibi iş birimi, işbu Politika içerisindeki uygun yöntemi uygun duruma göre belirleyerek uygulamakla yükümlüdür.

Kişisel verilerin imhası sırasında Kurum vereceği yazılı karara göre aşağıdaki yöntemlerden uygun olanı seçerek imhayı gerçekleştirir:

7.1. Üzerine Yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine yazılımlarla en az 7 kez 0 ve 1'lerden oluşan sayısal veriler yazılarak eski verinin okunamaz hale getirilmesi işlemidir.

7.2. Manyetize Etme

Manyetik medyanın yüksek değerde manyetik alanda fiziksel değişime sokularak üzerindeki verinin okunamaz hale getirilmesi işlemidir.

7.3. Fiziksel Yok Etme

Optik medya veya manyetik medyanın eritme, toz haline getirme, öğütme ve benzeri işlemlerle fiziksel olarak yok edilmesi işlemidir. Manyetize etme veya üzerine yazma metotlarının başarısız olduğu durumlarda uygulanabilir.

7.4. Bulut İmhası

Bulut sistemler üzerinde tutulan kişisel verilerin imha bildiriminin anlaşmalı servis sağlayıcıya yapılmasının ardından kişisel verilerin şifreleme anahtarlarının tüm kopyalarının imha edilmesi işlemidir.

7.5. Çevresel Sistemlerde Yer Alan Kişisel Verilerin İmhası

Yazıcı, parmak izi ünitesi, kapı giriş turnikesi gibi sistemler içerisinde yer alan kişisel verileri barındıran mevcut ise iç ünite, mevcut değil ise tüm cihaz üzerinde üzerine yazma, manyetize etme veya fiziksel yok etme uygulanarak yapılması gereken imha işlemidir. Bu tip imhaların, cihazların yedekleme, bakım ve benzeri işlemlere tabi olmasından önce uygulanması zorunludur.

8. Saklama ve İmha Süreleri

8.1. Periyodik İmha ve Yasal Saklama Süreleri

Kurum 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.

Yasal saklama ve imha sürelerini dolduran fiziksel ve elektronik veriler, periyodik olarak imha edilir. Kurum, imha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri imha eder.

Periyodik imha, tüm kişisel veriler için 6 aylık zaman aralıklarında gerçekleştirilir. Periyodik imha sırasında baz alınacak yasal saklama süreleri, Kurumun Kişisel Veri Envanterinde belirlenmiştir (EK). İmha işlemi, imha yükümlülüğünün doğmasını takiben ilk Periyodik imha sırasında uygulanır.

İmha edilen kişisel verilere ilişkin tüm işlemler kayıt altına alınır ve bu kayıtlar 3 yıl süre ile saklanır.

Kurum'un müşterilerine ait veriler, düzenleyici kurum Sermaye Piyasası Kurulu'nun düzenlemelerine uygunluk sağlamak amacıyla, SPK düzenlemelerinde ve Türk Ticaret Kanunu'nda belirtilen saklama sürelerinden az olmamak üzere ve muhtemel müşteri ihtilaflarının çözümünde mahkemelere ya da tahkim heyetine sunulmak üzere durumun gerekli kıldığı ek sürelerde saklanır.

8.2. Veri Sahiplerinin Talep Etmesi Durumunda İmha Süreci

Veri sahiplerinin Kurum'a başvurarak kendisine ait kişisel verilerin imhasını talep ettiği durumlarda Kurum, kişisel verileri işleme şartlarının mevcut durumunu kontrol eder.

Söz konusu kontrol sonucunda;

- Kişisel verileri işleme şartlarının tamamının ortadan kalktığı anlaşılırsa, talebe konu kişisel veriler işbu Politika 'da belirtilen karar ve yöntemlere uygun olarak en geç otuz gün içinde imha edilir ve ilgili kişiye bilgi verilir.

- Kişisel verileri işleme şartlarının ortadan kalktığı ve talebe konu olan kişisel verilerin üçüncü kişilere aktarıldığı anlaşılmışsa Kurum bu durumu ilgili üçüncü kişiye bildirir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Kurum ilgili veri sahibine gerekçesini açıklayarak talebi reddedebilir ve ret cevabını ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

Veri sahiplerinden gelecek taleplerin karşılanması ve yanıtlanması amacıyla Kurum bünyesinde Kişisel Veri Sahiplerinden Gelen Talep ve Şikayetlerin Yönetimi Süreci oluşturulur.

8.3. Saklama ve İmha Süreçlerinde Yetkilendirme

Kurum'un kişisel verileri saklama ve imha süreçlerinde görev alanlar ve iş tanımları aşağıdaki gibidir;

KVKK Çalışma Grubu: Komite ve Üst Kurul olmak üzere 2 bileşenli bir yapıdadır. Kişisel verilerin saklanması ve imhası konusunda Kurum'un ilgili iş birimleriyle beraber çalışarak politika ve yöntemler hakkında karar verir, Politika ve eklerinin güncel tutulmasını sağlar, gerekli durumlarda Kurum'un ilgili birimleri ile yakın çalışarak Politikanın Kanun ve Yönetmeliğe uygun ve doğru şekilde yürütülmesini temin eder.

İç Kontrol, Uyum ve Hukuk: Kişisel verilerin saklanması ve imhası ile ilgili hukuki konularda danışmanlık yapar, Kanun, Yönetmelik ve ilgili mevzuat değişikliği halinde ilgili iş birimlerine gerekli bilgilendirmeyi yapar. Politikanın Kanun ve Yönetmeliğe uygun olarak yürütülmesini temin eder.

Bilgi teknolojileri: Politika ‘da belirtilen karar ve yöntemler ışığında ilgili imha ve saklama süreçlerinin Kanun ve Yönetmeliğe uygun şekilde gerçekleştirilmesini sağlar.

Kurum’un ilgili iş birimleri: Kişisel verilerin saklanması ve imhası konusunda politika ve yöntemlerin belirlenmesi için görüş ve gerekçelerini belirtir ve bu Politika nezdinde yürütülmesi aksiyonlarının takibini yapar.

9. POLİTİKA’DA YAPILACAK DEĞİŞİKLİKLER

9.1. Kanun, Yönetmelik veya sair mevzuatın kısmen veya tamamen değiştirilmesi, tadil edilmesi, güncellenmesi veya yürürlükten kaldırılması durumunda, Kurum Politikayı yeni Kanun, Yönetmelik veya mevzuata uyumlu olacak şekilde güncelleyerek değiştirecektir.

9.2. Kurum, Politika üzerinde yaptığı değişiklikler incelenebilecek olacak şekilde güncellenen Politikayı e-posta yolu ile çalışanlarıyla paylaşacak ve kurumsal intranet üzerinden çalışanlarının erişimine sunacaktır.

10. Uyumluluk

Tüm personel ve üçüncü taraflar bu politikaya uygun davranmaktan sorumludur. [Bilgi Güvenliği Yönetişim ve Uyum ekibi] bu politikanın uygulanmasından, uygulamanın denetlenmesinden ve politika dokümanının güncel tutulmasından sorumludur.

11. Gözden Geçirme ve Revizyon

Bu politika, [Bilgi Güvenliği Yönetişim ve Uyum ekibi] tarafından periyodik olarak yılda bir kez gözden geçirilir.