KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İÇ SİSTEMLER
(Ekim/2019)

I. VERİ SAKLAMA VE İMHA TAAHHÜDÜ

1. İşbu Kişisel Veri Saklama ve İmha Politikası ("Politika"), GSD Yatırım Bankası A.Ş. ("GSD Bank") nezdinde, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 7. Maddesi uyarınca oluşturulan ilgili Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik doğrultusunda GSD Bank içerisinde ve/veya GSD Bank tarafından uyulması gereken esasları belirleyecektir.

2. GSD Bank, bünyesinde bulundurduğu, tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi sırasında işbu Politika'ya ve Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.

3. GSD Bank, işbu politika ile kişisel veri bulunan aşağıda belirtilen ortamlardaki ve belirtilen ortamlara ek ortaya çıkabilecek tüm ortamlardaki kişisel verileri kapsamayı kabul eder.

a) GSD Bank adına kullanılan bilgisayarlar/sunucular
b) Ağ cihazları,
c) Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
d) Bulut sistemleri,
e) Mobil telefonlar ve içerisindeki tüm saklama alanları,
f) Kâğıt,
g) Mikrofiş,
h) Yazıcı, Parmak izi okuyucu gibi çevre birimler,
i) Manyetik bantlar,
j) Optik diskler,
k) Flash hafızalar.

II. POLİTİKANININ KAPSAMI

1. İşbu Politika; GSD Bank'ın kişisel verileri işlediği herhangi bir sürece dâhil olan tüm departmanlarını, çalışanlarını ve 3.partileri kapsamaktadır.

2. İşbu Politika; GSD Bank'ın kişisel veriler üzerinde uygulayacağı tüm imha faaliyetlerini kapsayacak olup, her türlü imha gereksinimi sonucunda uygulanacaktır.

3. İşbu Politika kişisel veri olmayan veriler hakkında uygulanmayacaktır.

4. Konuyla alakalı yeni mevzuatlar ile belirlenmesi veya ilgili mevzuatın güncellenmesi durumunda, GSD Bank politikasını ilgili mevzuatlara uyumlu olacak şekilde güncelleyerek mevzuat gerekliliklerine uyacaktır.

5. İşbu Politika'nın GSD Bank tarafından uygulanmasında hukuki bir engel olduğuna kanaat getirildiği durumlarda, GSD Bank uygulayacağı adımları, gerek görülmesi durumunda Kurul'a da danışarak, yeniden belirleyecektir.

TANIMLAR ve KISALTMALAR

Tanımlar:

İşbu Politika'da ve ilgili yönetmelikte geçen tanımlar şu şekilde açıklanmaktadır;

Yönetmelik: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik'tir.

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 ortama verilen addır.

Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçlarını, veri kategorilerini, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve detaylandırdıkları envanterdir.

Periyodik imha: Kanunda yer alan kişisel verilerin işlenme 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 işlemidir.

Sicil: Başkanlık tarafından tutulan veri sorumluları sicilidir.

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Doğrudan tanımlayıcılar: Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır.

Dolaylı tanımlayıcılar: Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır.

İlgili kişi: Kişisel verisi işlenen gerçek kişidir.

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 gerçek veya tüzel kişilerdir.

İrtibat Kişisi Yönetim kurulu Kararı ile atanan Banka KVKK irtibat kişisini.(İç Kontrol Birim Yöneticisini

KVKK Koordinasyon Komitesi İç Sistemler kapsamında yer alan birim yöneticilerini

Kurul Kişisel Verileri Koruma Kurulu anlamına gelmektedir.

Kısaltmalar:

GSD, GsdBank'ı temsil eder.

İlgili Formlar: ***U:\Dokümanlar Veritabanı\KVKK"*** altında yer alan formlar.

III. KİŞİSEL VERİ İŞLEME ŞARTLARINI ORTADAN KALDIRAN HALLER

Kişisel verilerin işlenmesi ile ilgili hüküm ve esaslar GSD Bank'ın Kişisel Verilerin Korunması Politikası içerisinde belirtilmiş olup, tüm GSD Bank çalışanları bu politikadaki hallerden sorumludur. İşbu Veri Saklama ve İmha Politikası içerisinde Veri Saklama ve İmha dışında kalan "İşleme" konusu ilgili Kişisel Verilerin Korunması Politikası'nın bir özeti şeklindedir.

Aşağıda belirtilen kapsamda bir ihlal olması durumunda Potansiyel Güvenlik İhlali Protokolü içerisindeki ihlal durumu kabul edilerek GSD Bank tarafından aksiyon alınacaktır.

1. Kanun'a Aykırılık

GSD Bank, kişisel verileri Kanun'da belirtildiği şekle aykırı olarak işlemediğini taahhüt eder.

Yani GSD Bank 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 saklamaz.
b) GSD Bank, özel nitelikli kişisel verileri sakladığı durumlarda, verileri ilgili Kanun'a bağlı kalarak GSD Bank'ın KVKK Koordinasyon Komitesi (İç Sistemler) ve Hukuk Müşavirliği bilgisi dâhilinde işler.

2. Veri İşlenme Şartlarının Ortadan Kalkması

GSD Bank, veri işlenme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu tüm çalışanları ile paylaşır. Çalışanlar, veri işlenme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez.

GSD Bank Bilgi Sistemleri ekibi, şartların ortadan kalktığı ortamları işbu Politika'ya uygun bir şekilde ortadan kaldırmakla yükümlüdür.

GSD Bank aşağıda listelenen ve Yönetmelik içinde de belirtilen durumlarda veri işlenme şartlarının ortadan kalktığını kabul eder.

a) Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
b) Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, 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 başvurunun veri sorumlusu tarafından kabul edilmesi,
g) Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi 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,
h) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

IV. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ

Kişisel verilerin imhası, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi şeklinde üç farklı şekilde sağlanabilir. İmha işlemindeki amaç, kalan veriler ile gerçek kişiye ulaşabilmenin mümkün olmamasıdır.

Kişisel verilere ilişkin olarak silme, yok etme ve imha süreçleri bu politika dokumanında açıklanan hususlar gözetilerek periyodik olarak (en az 6 ayda bir olmak üzere) yürütülür. Belirlenen periyotlarda imhaların yapılmasının takibi İmha Ekibi'nin sorumluluğundadır. İmha Ekibi'nde yer alan personel bilgilerine aşağıda yer verilmektedir. İlgili kişilerin görev tanımları ortak alanda ***"Dokümanlar Veritabanı\PERSONEL GÖREV TANIMLARI VE SORUMLULUKLAR"*** içerisinde yer almaktadır.

Unvan	Bölüm
Grup Başkanı	Bilgi Teknolojileri
Bölüm Bşk. Yard.	İç Denetim
Bölüm Başkanı	İç Kontrol
Bölüm Başkanı	Risk Yönetimi
Müdür	Muhasebe ve İnsan Kaynakları
Hukuk Müşaviri	Hukuk
Grup Başkanı	Operasyon/Finansal Raporlama
Grup Başkanı	Pazarlama
Grup Başkanı	Krediler
Müdür	Hazine

Fiziksel ortamda, kişisel bilgisayarlarda ve veri tabanında yer alan verilere ilişkin silme, yok etme ve imha çalışmasından her birim/personel envanterinde yer alan veriler kapsamında sorumludur. Dijital ortamda yer alan verinin silinmesi/yokedilmesi ve anonimleştirilmesi konusunda Bilgi Teknolojileri Grubu'ndan destek alınacaktır. Fiziksel ortamdaki verilerin silme, yok etme ve imhası ise periyodik imha sürecinde imha ekibinin koordinasyonu ile gerçekleştirilecektir.

1. Kişisel Verilerin Silinmesi

1.1. Kişisel Verilerin Silinme Süreci

Silme işlemi, GSD Bank'ın verileri tamamen veya otomatik yollarla işlediği durumlarda yapılacaktır ve GSD Bank, kişisel verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirmelidir. GSD Bank, bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti etmelidir. Bu garanti, veri sorumlusunun sorumluluğu altındadır.

Silme sırasında, silinmemesi gereken kişisel veriler de yapılan silmeden etkileniyorsa ve erişilemeyecek ve/veya kullanılamayacak hale geliyorsa GSD Bank'ın, Veri Sorumlusu ve imha ekibi ile birlikte karar alarak uygulayabileceği aşağıdaki yöntemlerin bir arada sağlanması da silme olarak değerlendirilecektir:

a) Kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek şekilde arşivlenmesi
b) Her bir kişisel veri için ilgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin kapatılması ve ortadan kaldırılması
c) Kişisel verilere yalnızca gerekli durumlarda yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması

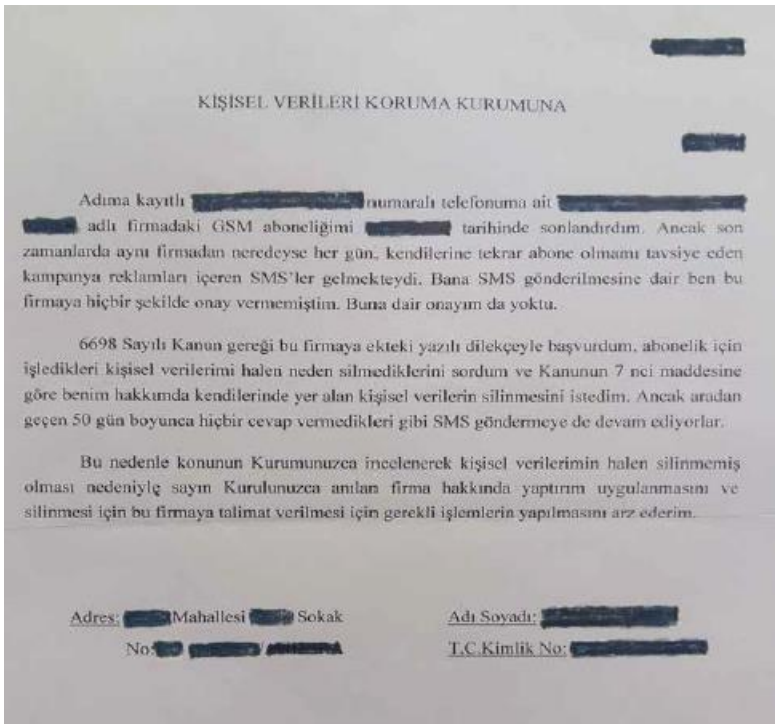
Belirtilen silme yöntemleri, Yönetmelik'e bağlı olup, ilgili durumlarda güncellenmesi Veri Sorumlusu'nun sorumluluğundadır.

1.2. Kişisel Verilerin Silinme Yöntemleri

Kişisel veriler kayıtlı oldukları ortamlara uygun yöntemlerle silinmelidir.

1.2.1. Basılı Dokümanlarda Yer Alan Kişisel Veriler

Basılı dokümanlarda bulunan kişisel veriler karartma yöntemi ile silinmelidir. 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 görünmez hale getirilmesi şeklinde yapılır.



KİŞİSEL VERİLERİ KORUMA KURUMUNA

Adıma kayıtlı [redacted] numaralı telefonuma ait [redacted] adlı firmadaki GSM aboneliğimi [redacted] tarihinde sonlandırdım. Ancak son zamanlarda aynı firmadan neredeyse her gün, kendilerine tekrar abone olmamı tavsiye eden kampanya reklamları içeren SMS'ler gelmekteydi. Bana SMS gönderilmesine dair ben bu firmaya hiçbir şekilde onay vermemiştim. Buna dair onayım da yoktu.

6698 Sayılı Kanun gereği bu firmaya ekteki yazılı dilekçeyle başvurdum, abonelik için işledikleri kişisel verilerimi halen neden silmediklerini sordum ve Kanunun 7 nci maddesine göre benim hakkımda kendilerinde yer alan kişisel verilerin silinmesini istedim. Ancak aradan geçen 50 gün boyunca hiçbir cevap vermedikleri gibi SMS göndermeye de devam ediyorlar.

Bu nedenle konunun Kurumunuzca incelenerek kişisel verilerimin halen silinmemiş olması nedeniyle sayın Kurulunuzca anılan firma hakkında yaptırım uygulanmasını ve silinmesi için bu firmaya talimat verilmesi için gerekli işlemlerin yapılmasını arz ederim.

Adres: [redacted] Mahallesi [redacted] Sokak
No: [redacted]

Adı Soyadı: [redacted]
T.C.Kimlik No: [redacted]

Kişisel Verilen Karartılması Örneği

1.2.2. Merkezi Sunucuda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir.

1.2.3. Taşınabilir Disk Üzerinde Bulunan Kişisel Veriler

Taşınabilir (harici) disk üzerinde bulunan kişisel veriler, şifreli olarak saklanmalı ve disk özelliğine uygun yazılımlar kullanılarak silinmelidir.

1.2.4. Veri Tabanları Üzerinde Bulunan Kişisel Veriler

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir.

2. Kişisel Verilerin Yok Edilmesi

Yok etme işlemi, GSD Bank'ın verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve GSD Bank bu verileri tekrar geri getirilmesi ve tekrar kullanılması mümkün olmayacak hale getirmekle yükümlüdür. Bu işlemler sırasında GSD Bank çalışanları ve ilgili departmanlar Veri Sorumlusu'na yok edilecek ilgili verileri bildirmekle yükümlüdür, sonrasında ise Veri Sorumlusu gerekli her türlü teknik ve idari tedbiri alacaktır.

2.1. Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespiti ve verilerin tutulduğu sistemlere göre aşağıdaki yöntemlerden bir veya birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir.

2.1.1. Yerel Sistemler Üzerindeki Kişisel Veriler

2.1.1.1. De-manyetize Etme

Manyetik medyanın özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

2.1.1.2. Fiziksel Yok Etme

Optik medya ve manyetik medyanın eritilmesi, yakılması, toz haline getirilmesi veya metal öğütücüden geçirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Katı hal diskler (SSD) gibi de-manyetize edilemeyen cihazlar için fiziksel yok etme işlemleri uygulanmalıdır.

2.1.1.3. Üzerine Yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kere 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir.

2.1.2. Çevresel Sistemler Üzerindeki Kişisel Veriler

2.1.2.1. Ağ cihazları (switch, router vb.)

Söz konusu cihazların silme komutları vardır ama yok etme özelliği bulunmamaktadır. (2.1.1)'de belirtilen uygun yöntemlerin bir ya da birkaçı kullanılarak yok edilmesi gerekir.

2.1.2.2. Flash tabanlı diskler

Flash tabanlı sabit disklerin ATA (SATA, PATA, vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yöntem ya da (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi gerekir.

2.1.2.3. Manyetik bant ve manyetik disk üniteleri

Manyetik bantları ve manyetik disk ünitelerini güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok etmek gerekir.

2.1.2.4. Mobil telefonlar (Sim kart ve sabit hafıza alanları)

Mobil telefonlardaki sabit hafıza alanlarının (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi gerekir.

2.1.2.5. Optik diskler (CD, DVD vb.)

Optik disklerin yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleri ile yok edilmesi gerekir.

2.1.2.6. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri

Tüm veri kayıt ortamlarının söküldüğü doğrulanarak (2.1.1)'de belirtilen uygun yöntemlerin kullanılıp yok edilmesi gerekir.

2.1.2.7. Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri

Söz konusu sistemler için (2.1.1)'de belirtilen uygun yöntemler kullanılarak yok edilme işlemi gerçekleştirilmelidir.

2.1.3. Kâğıt ve Mikrofiş Ortamları

Kalıcı ve fiziksel ortam üzerine yazılı olan kişisel verilerin yok edilmesi için ortamın kâğıt imha veya kırpma makineleri ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünmesi gerekir.

2.1.4. Bulut Ortamı

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve mümkünse kişisel verilerin depolandığı her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Kişisel verilerin yok edilmesi için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

Yukarıda yer alan 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 (2.1.1)'de belirtilen uygun yöntemleri kullanarak yok edilmesi,
ii. Yok etmenin mümkün 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 gerekir.

3. Kişisel Verilerin Anonimleştirilmesi

Anonim hale getirme işlemi, GSD Bank'ın kişisel verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin doğrudan ve/veya dolaylı tanımlayıcılarının çıkartılarak ya da değiştirilerek, başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Verilerin anonimleştirilmesi sırasında GSD Bank geri dönülemez şekilde maskeleme, tek yönlü fonksiyonlar ile şifreleme gibi yöntemler kullanılabilir. Uygulanacak yöntemin doğruluğu, Veri Sorumlusu tarafından onaylanamıyorsa kurula danışılmalıdır.

3.1. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Alt ve Üst Sınır Kodlama • Bölgesel Gizleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme

3.1.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

3.1.1.1. Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Bu yöntem değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin hassas bir veri olması gibi sebeplerle kullanılabilir.

Yaş	Cinsiyet	Posta Kodu	Gelir	Din
20	K	S017	20,000	~~Budist~~
28	E	S018	22,000	~~Müslüman~~
29	E	S016	32,000	~~Hristiyan~~

3.1.1.2. Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.

Yaş	Cinsiyet	Doğum Y.	Sektör	Derece
31	K	İstanbul	Mimarlık	3.22
31	E	İstanbul	Mimarlık	3.04
31	E	Ankara	Sanayi	3.22
43	K	Ankara	Sanayi	3.40
~~51~~	~~E~~	~~Eskişehir~~	~~Sanat~~	~~2.45~~

3.1.1.3. Bölgesel Gizleme

Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görünebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine sebep olacaksa istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

Yaş	Cinsiyet	Meslek	HIV Durumu
52	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
64	E	Mühendis	Pozitif
30	K	-	Pozitif

Orijinal Veri Kümesi

Yaş	Cinsiyet	Meslek	HIV Durumu
52	K	Öğretmen	Pozitif
28	E	Mimar	Negatif
64	E	Mühendis	Pozitif
Bilinmiyor	K	-	Pozitif

Bölgesel Gizleme Sonrası Veri Kümesi

3.1.1.4. Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

3.1.1.5. Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir.

Yaş	Cinsiyet	Meslek	Gelir Yıllık	Test Sonucu	Harcamalar
3*	K	Mühendis	92,000	Negatif	8,000
4*	E	Mimar	110.000	Negatif	9.600
4*	E	Doktor	149.000	Negatif	10.000
5*	E	Doktor	125.000	Pozitif	11.100

Orijinal Veri Kümesi

Tablodaki Gelir ve Harcamalar değişkenleri kendi içlerinde sınıflanarak aşağıdaki tabloda anonim halini almıştır.

Yaş	Cinsiyet	Meslek	Gelir Yıllık	Test Sonucu	Harcamalar
3*	K	Mühendis	Düşük	Negatif	Düşük
4*	E	Mimar	Orta	Negatif	Düşük
4*	E	Doktor	Yüksek	Negatif	Orta
5*	E	Doktor	Yüksek	Pozitif	Yüksek

Alt ve üst sınır kodlama sonrası veri kümesi

3.1.1.6. Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir.

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar	Çankaya	Evli
K	Mühendis	Çankaya	Bekar
K	Mimar	Çankaya	Boşanmış
K	Mühendis	Çankaya	Evli

Orijinal Veri Kümesi

Cinsiyet	Meslek	İlçe	Medeni Durum
K	Mimar veya Mühendis	Çankaya	Evli
K	Mimar veya Mühendis	Çankaya	Bekar
K	Mimar veya Mühendis	Çankaya	Boşanmış
K	Mimar veya Mühendis	Çankaya	Evli

Global kodlama sonrası veri kümesi

3.1.1.7. Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur.

3.1.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan yöntemlerle mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

3.1.2.1. Mikro Birleştirme

Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

Aşağıdaki tabloda "Gelir" sütunundaki değerlerine göre birbirine yakın olan üçerli gruplara ayrılmıştır. Her grup, içindeki değerlerin aritmetik ortalaması alınmış ve bulunan yeni değerler orijinal değerlerin yerine yazılmıştır.

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	25.000
37	K	1559	28.000
41	E	1559	37.000
25	K	1557	49.000
34	E	1558	56.000
48	E	1556	60.000

Orijinal Veri Kümesi

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	30.000
37	K	1559	30.000
41	E	1559	30.000
25	K	1557	55.000
34	E	1558	55.000
48	E	1556	55.000

Mikro Birleştirme sonrası veri kümesi

3.1.2.2. Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır.

Yaş	Cinsiyet	İl	Gelir
23	K	İstanbul	20.000
37	K	Ankara	30.000
41	E	İzmir	30.000
25	K	İstanbul	25.000
34	E	Ankara	55.000
48	E	İzmir	15.000

Orijinal Veri Kümesi

Yaş	Cinsiyet	İl	Gelir
23	K	İstanbul	25.000
37	K	Ankara	55.000
41	E	İzmir	15.000
25	K	İstanbul	20.000
34	E	İzmir	30.000
48	E	İzmir	30.000

Veri değiş tokuş sonrası veri kümesi

3.1.2.3. Gürültü Ekleme

Bu yöntem ile seçilen değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bozulma her değerde eşit ölçüde uygulanır.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	45.000
35	E	Ankara	123.000
45	E	Ankara	18.000

Orijinal veri kümesi

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	50.000
35	E	Ankara	128.000
45	E	Ankara	23.000

Gürültü sonrası veri kümesi

3.2. Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya Kişisel Verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir.

Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirerek veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

i. Anonimlik

Anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için

ii. Çeşitlilik

Anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

iii. Yakınlık

Kişisel Verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine yakınlık yöntemi denmektedir

V. SAKLAMA VE İMHA SÜRELERİ

1. Periyodik İmha ve Yasal Saklama Süreleri

Yasal saklama ve imha sürelerini dolduran fiziksel ve dijital veriler, periyodik olarak imha edilir. GSD Bank, Kişisel Verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, Kişisel Verileri siler, yok eder veya anonim hale getirir. Periyodik imha, tüm Kişisel Veriler için 6 aylık zaman aralıklarında gerçekleştirilir. Periyodik imha sırasında baz alınacak yasal saklama ve imha süreleri, GSD Bank Kişisel Veri İşleme Envanteri'nde (**U:\Dokümanlar Veritabanı\KVKK-**

Excel) belirlenmiştir. GSD Bank, Yönetmelik madde 11(4) kapsamında Kurul'un süreleri kısaltması durumunda, yeni sürelere uyum sağlayacağını taahhüt eder.

Süreç	Saklama Süresi
Bankacılık Kanunu ve BDDK Düzenlemeleri Gereği	10 yıl
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (sağlık raporları vs.)	15 yıl
İlgili kişisel verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması veya bir suç ile ilişkili olması durumunda Türk Ceza Kanunu'nun 66. ve 68. maddeleri gereği	Dava zamanaşımı ve Ceza Zamanaşımı müddetince
Sair ilgili mevzuat gereği	ilgili mevzuatta öngörülen süre kadar

Silinen, yok edilen ve anonim hale getirilen verilere ilişkin işlemlerin diğer hukuki yükümlülüklerden ayri en az 3 yıl süre ile saklanır. GSD Bank'ın diğer hukuki yükümlülüklerden kaynaklanan Kişisel Veri saklama hakları saklıdır.

Veri Sahiplerinin Talep Etmesi Durumunda Silme ve Yok Etme Süreci

Veri sahiplerinin GSD Bank'a başvurarak kendisine ait Kişisel Verilerin silinmesini veya yok edilmesini talep ettiği durumlarda Kişisel Verileri işleme şartlarının mevcut durumunu kontrol eder ve buna bağlı ilgili aksiyonları alır.

Kişisel Verileri işleme şartlarının tamamı ortadan kalkmışsa talebe konu Kişisel Verileri siler, yok eder veya anonim hale getirir. GSD Bank ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. **U:\Dokümanlar Veritabanı\KVKK> Formlar**

Kişisel Verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan Kişisel Veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

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

VI. KİŞİSEL VERİLERİN SAKLANMASI, İŞLENMESİ VE İMHASI İÇİN ALINAN TEDBİRLER

GSD Bank, Kişisel Verilerin hukuka uygun şekilde saklanması, işlenmesi ve erişimini sağlamak için korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetlerine göre teknik ve idari tedbirler almaktadır.

a. Teknik Tedbirler

GSD Bank tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Teknolojideki gelişmelere uygun teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmekte ve yenilenmektedir.
- İş birimi bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak yetki matrisi oluşturulmuş, kişisel hesap yönetimi sistemi kurulmuş ve şifreleme sistemleri aktive edilmiştir.
- Bu kapsamda virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılım ve donanımlar kurulmakta, log kayıtları tutulmakta, düzenli yedeklemeler yapılmaktadır.
- Bu kapsamda güvenlik duvarları ve saldırı tespit ve önleme sistemleri kullanılmakta yetki kontrolleri ve sızma testleri gerçekleştirilmektedir.
- Teknik konularda bilgili personel istihdam edilmekte ve bu kişiler kurulmuş olan imha ekibinin daimi üyesi yapılmaktadır.

b. İdari Tedbirler

GSD Bank tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- GSD Bank çalışanlarına Kişisel Verileri Koruma mevzuatı kapsamında bilgilendirmiş ve bu konuda gerekli eğitimlerden geçirmiştir. Eğitimler kapsamında, çalışanlara rolleri ve sorumlulukları anlatılmış, "yasaklanmadıkça her şey serbest" değil "izin verilmedikçe her şey yasak" prensibi hakkında bilgilendirme yapılmıştır. Çalışanlar ile öğrendikleri Kişisel Verileri ilgili mevzuat hükümlerine aykırı olarak başkasına açıklayamayacağı, işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda gizlilik sözleşmesi imzalanarak Kişisel Verilerin Korunması adına

gerekli taahhütler alınmıştır. Bu kapsamda İş Sözleşmeleri ve disiplin yönetmeliklere Kanun'a uygun hükümler eklenmiştir. GSD Bank içi organizasyonlarında, bu taahhütlere ve sair gizlilik yükümlülüklerine uyulmaması durumunda işletilecek disiplin süreçlerini hazırlamıştır.

- Veri Sorumluları Sicil Bilgi Sistemine bildirim yapılabilmesi için gerekli hazırlıklarını tamamlamıştır.
- İş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak GSD Bank içinde Kişisel Verilere erişim ve yetkilendirme süreçleri yetki matrisleri tasarlanmış ve uygulanmaktadır.
- GSD Bank tarafından Kişisel Verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; Kişisel Verilerin aktarıldığı kişilerin, Kişisel Verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.
- Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha konularında işbu Politika kapsamında gerekli düzenlemeleri yapmıştır
- Kişisel Veri İşleme Envanteri hazırlanmış ve Kişisel Verilerin işlenmesi, muhafazası ve aktarılmasına ilişkin sözleşmelerde gerekli hükümlere yer vermiş,
- Kurum İçi Periyodik ve/veya Rastgele Denetimler için gerekli hazırlıklar yapılmıştır. Risk Analizleri gerçekleştirilerek gerekli önlemler alınmıştır.
- İhlal durumunda kurumsal iletişim prosedürleri ve bilgilendirme süreçleri işbu Politika'da belirleniştir.

VII. KVKK KOORDİNASYON KOMİTESİ GÖREVLERİ

GSD Bank kendi bünyesinde, işbu Politika ve bu Politika ile ilişkili diğer politikaları yönetmek üzere GSD Bank Yönetim Kurulu kararı gereğince "GSD Bank KVKK Koordinasyon Komitesi" kurmuştur. Bu komitenin görevleri aşağıda belirtilmektedir. Komite en az yılda bir olmak üzere KVKK kapsamındaki mevzuatsal değişikliklerin ve banka içi uygulamaların değerlendirilmesi amacıyla toplanır.

- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili temel politikaları hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu'nun onayına sunmak.

- Kişisel Verilerin Korunması ve İşlenmesine ilişkin politikaların uygulanması ve denetiminin ne şekilde yerine getirileceğine karar vermek ve bu çerçevede GSD Bank içi görevlendirmede bulunmak ve koordinasyonu sağlamak hususlarını Yönetim Kurulu'nun onayına sunmak.
- Kanun ve ilgili mevzuata uyumun sağlanması için yapılması gereken hususları tespit etmek ve yapılması gerekenleri Yönetim Kurulu'nun onayına sunmak; uygulanmasını gözetmek ve koordinasyonunu sağlamak.
- Kişisel Verilerin Korunması ve İşlenmesi konusunda GSD Bank nezdinde farkındalığı arttırmak.
- GSD Bank'ın Kişisel Veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini Yönetim Kurulu'nun onayını sunmak.
- Kişisel Veri sahiplerinin başvurularını Hukuk Müşavirliği ve Genel Müdür görüş ve uygunluğu dahilince karara bağlamak.
- Kişisel Verilerin Korunması ve İşlenmesi ile ilgili temel politikalardaki değişiklikleri hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu'nun onayına sunmak.
- Kişisel Verilerin Korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak GSD Bank içinde yapılması gerekenler konusunda Yönetim Kurulu'na tavsiyelerde bulunmak.
- Kişisel Verilerin Korunması Kurulu ve Kurumu ile olan ilişkileri koordine etmek.
- Yönetim Kurulu'nun Kişisel Verilerin korunması konusunda vereceği diğer görevleri icra etmek.

VIII. POLİTİKA'DA YAPILACAK DEĞİŞİKLİKLER

1. İlgili mevzuatta yapılacak her türlü resmi değişikliğin ardından bu değişiklerle uyumlu olacak şekilde GSD Bank tarafından işbu Politika'da değişiklik yapılabilir.

2. GSD Bank, Politika üzerinde yaptığı değişiklikler izlenebilecek şekilde, güncellenen Politika'yı e-posta yolu ile çalışanlarıyla paylaşacak ve aşağıdaki web adresi üzerinden çalışanlarının erişimine sunacaktır.

U:\Dokümanlar Veritabanı\KVKK

YETKİ VE SORUMLULUK

YETKİ

Bu Politika kapsamındaki personel belirlenen görevlerin yerine getirilmesi konusunda; yasalar, Banka iç mevzuatı ile belirlenen ve kendilerine delege edilen yetkilere sahiptirler.

SORUMLULUKLAR

Bu politika dokümanı kapsamındaki personel, yönetmelik ve diğer talimatlarla belirlenen görevlerin Banka politikası ve mevzuatına, yasalara uygun olarak yerine getirilmesinden, bu yönetmelikte belirtilen işlerin doğru ve zamanında yapılmasından, Banka'nın üçüncü kişilere karşı iyi bir şekilde temsil edilmesinden, suistimal içeren işlemin bilinmesi ya da tespit edilmesi durumunda bunu yönetimine gerekirse de Üst Yönetime bildirmekten, işi gereği edindiği bilgi ve belgeleri üçüncü şahıslarla paylaşmamaktan, genel ahlak kurallarına uygun davranmaktan, Banka menfaatlerini daima ön planda tutmaktan, verilen yetkileri gereği gibi kullanmaktan ve bu uygulama talimatının güncel tutulmasını sağlamak üzere GSD Bank KVKK Koordinasyon Komitesi'ne (İç Sistemler) değişen bilgilerin akışını sağlamaktan sorumludurlar. İç Sistemler Bölümleri dokümanın güncel tutulmasından sorumludur.

YÜRÜRLÜK VE DENETİM

YÜRÜRLÜK

Bu doküman Yönetim Kurulu'nun 01.10.2018 tarih ve 59 sayılı kararı ile yürürlüğe girmiştir.

DENETİM

İlgili çalışanlar; bu uygulama talimatı maddelerine göre Banka denetçileri tarafından denetlenir.