

**KİŞİSEL VERİLERİN
SİLİNMESİ,
YOK EDİLMESİ,
ANONİM HALE GETİRİLMESİ,
POLİTİKASI**

ÖNSÖZ

Alsancak Bilrad Emar Özel Sağlık Hizm. Tic. Ltd. Şti. (BİL RAD) ., 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun ve özel hüküm içeren sair mevzuata uygun olarak muhafaza etmekte olduğu kişisel verileri, 6698 Sayılı Kanun gereğince şartları oluştuğunda, şirket politikası gereğince veya ilgilinin talebi halinde aşağıda yer alan süreçlere uygun olarak silebilir, yok edebilir veya anonim hale getirebilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi halinde bir çelişki doğması halinde öncelikle 6698 sayılı kanun hükümleri ve Kişisel Verileri Koruma Kurumu ilke kararları tatbik edilecektir. İşbu politikada veya mevzuatta oluşabilecek revizyonlar tarih ve konu belirtilerek politikaya eklenecek, gerekli duyurular yapıldıktan sonra politikanın ayrılmaz bir parçası olarak kabul edilecektir.

-YAYIN TARİHİ 01/12/2019-

I-KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Silinen verilere, veri sorumlusu haricinde bulunan ilgili kullanıcılar tarafından ulaşılamaz ve kullanılamaz.

A-KİŞİSEL VERİLERİN SİLİNMESİ SÜRECİ

Kişisel veriler ilgilinin talebi ve kanuni bir zorunluluk bulunduğu takdirde mevzuata ve talebe uygun olarak silinir. Diğer durumlarda kişisel veriler 10 yıl süre ile saklanabilir.

Kişisel verinin varlığı sözleşmesel, ticari, hukuki, idari işlemler gereğince doğması muhtemele hak taleplerine ilişkin ise söz konusu işleme ilişkin zamanaşımı süresince veriler muhafaza edilir. Bu konuda talep ve şirket politikası arasında bir çelişki doğması halinde çelişkinin giderilmesi amacı ile Kişisel Verileri Korunma Kurumu'na yazılı başvuru yapılır ve ilke kararı doğrultusunda işlem yapılır.

Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcılar tespit edilir ve kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespiti yapılır akabinde İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılmasına ilişkin işlem gerçekleştirilir.

B-VERİ SİLME YÖNTEMLERİ

1-BULUT SİSTEMİ

Bulut sisteminde veriler silme komutu verilerek silinecektir. İlgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisi bulunmamaktadır.

2-KAĞIT ORTAMINDA BULUNAN KİŞİSEL VERİLER

Kağıt olarak basılı olan kişisel veriler karartma yöntemi kullanılarak silinecektir.

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.

3-MERKEZİ SUNUCUDA YER ALAN OFİS DOSYALARI

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

4-TAŞINABİLİR MEDYADA BULUNAN KİŞİSEL VERİLER

Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

5-VERİ TABANLARI

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

II-KİŞİSEL VERİLERİN YOK EDİLMESİ

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

KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

A-YEREL SİSTEMLER

1-DE-MANYETİZE

Manyetik medya, de manyetize etme özellikli bir cihazdan geçirilerek verilerin okunamaz biçimde bozulur. De manyetize özellikli cihaz ihtiyaç halinde temin edilecektir.

2-FİZİKSEL YOK ETME

Optik medya ve manyetik medyanın eritilerek, yakılarak veya toz haline getirilerek fiziksel olarak yok edilir.

3-ÜZERİNE YAZMA

Manyetik medya yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilir. Gerek halinde şirket tarafından bu amaçla yazılım temin edilir.

B- ÇEVRESEL SİSTEMLER

AĞ CİHAZLARI - FLASH TABANLI CİHAZLAR - MANYETİK BANT ve DİSKLER – MOBİL TELEFONLAR – SİM KARTLAR – HAFIZA KARTLARI – OPTİK DİSKLER – YAZICI – PARMAK İZİ OKUMA CİHAZLARI

Bu madde başlığı altında sayılmakta olan cihazların teknik özellikleri arasında yok etme komutu var ise yok etme komutu kullanılarak, aksi takdirde de manyetize etme, fiziksel yok etme veya üzerine yazma yöntemlerinden uygun olan seçilerek yok etme işlemi gerçekleştirilir.

C- KÂĞIT VE MİKRO FİŞLER

Kağıt ve mikro fiş olarak muhafaza edilmekte olan kişisel veriler kağıt imha veya kırma cihazları ile mümkünse yatay ve dikey olarak geri getirilemez ve birleştirilemez şekilde imha edilir. Kağıt ve mikro fişler taranarak elektronik ortama aktarılmış ise bulundukları elektronik ortam şartlarına göre de manyetize etme, fiziksel yok etme veya üzerine yazma yöntemlerinden uygun olan seçilerek yok etme işlemi gerçekleştirilir.

D-BULUT ORTAMI

Kişisel verilerin muhafaza edildiği bulut sistemi özellikleri arasında yok etme komutu bulunmakta ise bu komut ile aksi takdirde bulut sistemine ulaşılmasını sağlayan şifreleme anahtarlarının tüm kopyalarının yok edilmesi işlemi gerçekleştirilir.

E-BAKIM VE ONARIM İŞLEMLERİ

Bakım ve onarım amaçlı olarak içerisinde kişisel veri bulunan cihazların 3.kişi veya kurumlara teslim veya tevdi edilmesi halinde mümkün ise işbu politikanın yok etme başlığı altında yer alan yöntemlerden uygun olan seçilerek yok etme işlemi gerçekleştirilir. Yok etme işleminin uygun olmaması halinde ise cihaza ait veri saklama ortamı sökülür veya ilgili bölüm tarafından tercih edilen sair teknik önlemler alınır.

III-KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin farklı veriler ile eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemidir. Kişisel veriler anonim hale getirildiğinde geri döndürme veya eşleştirme yapılsa dahi veri sorumlusu ve verinin aktarıldığı kullanıcılar tarafından kime ait olduğu tespit edilemeyecek ve ilişkilendirilemeyecektir. Kişisel verilerin hangi hallerde anonimleştirileceği ve anonimleştirme işlemi için hangi yöntemin seçileceği işlemin özelliklerine göre veri sorumlusu tarafından belirlenir ve bu doğrultuda gerekli olan teknik tedbirler alınır.

Anonimleştirme yöntemi seçilirken; Verinin niteliği, Verinin büyüklüğü, Verinin fiziki ortamlarda bulunma yapısı, Verinin çeşitliliği, Veriden sağlanmak istenen fayda / işleme amacı, Verinin işlenme sıklığı, Verinin aktarılacağı tarafın güvenilirliği, Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması, Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı, Verinin dağıtıklık/merkezilik oranı, Kullanıcıların ilgili veriye erişim yetki kontrolü, Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali dikkate alınır. İşbu politikanın duyurulması ve yürütülmesi İnsan Kaynakları Departmanı tarafından gerçekleştirilecektir.