BMS GERİ DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1. AMAÇ VE KAPSAM

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), BMS GERİ DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ ("Veri Sorumlusu" anılacaktır) bünyesinde gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Veri Sorumlusu olarak temel prensibimiz; Hissedar/Ortak, Çalışan, Ürün veya Hizmet Alan Kişi, Tedarikçi Yetkilisi, Tedarikçi Çalışanı, Ziyaretçi, Potansiyel Ürün veya Hizmet Alıcısı, Diğer - Santral - Telefon Çağrı Görüşmesi Tarafı , Diğer - Kamu Görevlisi, Veli / Vasi / Temsilci, Diğer - Dava, İcra Dosyası Tarafı, Stajyer, Diğer - Doktor, Çalışan Adayı, Diğer - İş Sağlığı ve Güvenliği Uzmanı ve diğer üçüncü kişiler ilgili kişilerine ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuatlara uygun olarak işlenmesidir. Bu kapsamda ilgili kişilerin hak kaybına uğramaması ve haklarını etkin bir şekilde kullanması öncelik olarak belirlenmiştir.

İşbu hazırlanan Kişisel Verileri Saklama ve İmha Politikası, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 28.10.2017 tarih ve 30224 Sayılı Resmi Gazetede yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") ve diğer mevzuat hükümlerine uyumlu şekilde hazırlanmıştır.

2. TANIMLAR

Alıcı Grubu	Alıcı Grubu Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	Açık Rıza Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Çalışan	Çalışan Veri Sorumlusu personeli.
Elektronik Ortam	Elektronik Ortam Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Hizmet Sağlayıcı	Veri Sorumlusu ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	İlgili Kişi Kişisel verisi işlenen gerçek 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.

İmha	İmha Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 ortam.
Kişisel Veri	Kişiyi belirli veya belirlenebilir kılan her türlü bilgi.
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri 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 envanter.
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kurul	Kişisel Verileri Koruma Kurulu.
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.
Periyodik İmha	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Kişisel Verileri Saklama ve İmha Politikası.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
Veri Sorumluları Sicil Bilgi Sistemi	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi.
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin

	Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

3. KAYIT ORTAMLARI

Aşağıdaki tablo, Veri Sorumlusu tarafından saklanan kişisel verilerin hangi ortamlarda kayıt altına alındığını göstermektedir. Veri Sorumlusu tarafından saklanan kişisel veriler, niteliğine ve hukuki durumuna göre en uygun kayıt ortamında saklanmaktadır.

Veri Saklama Ortamları
Bilgisayar
Kilitli Arşiv Dolabı
Arşiv Dolabı
Arşiv Odası
Kontrollü Bölgede Çift Kilitli Dolap
Kilitli Dolap
Hard Disk
Kağıt
Birim Arşivi
İşletme Sunucusu
Yurtdışı E-posta Sunucusu
Yurtiçi E-posta Sunucusu
Excel Programı
Server
Flash Bellek
Erişim Kısıtlı Dosya

4. SORUMLULUK VE GÖREV DAĞILIMLARI

Yönetmeliğin 6. maddesinin f bendi uyarınca kişisel verilerin saklanmasında ve imha süreçlerinde yer alan kişilerin unvanlarının, görevlerinin ve birimlerinin belirtilmesi gerektiği düzenleme altına alınmıştır. Bu kapsamda kişisel verilerin hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi, kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla veri güvenliği, saklama ve imha süreçlerinin yönetimi, teknik ve idari tedbirlerin alınması konularında Veri Sorumlusu bünyesinde bulunan kişilere ait unvanları, görev ve birimleri belirtilmiştir.

Unvan	Görev Tanımı

Kişisel Veri Yöneticisi	Kişisel Veri Yöneticisi Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası ve düzenlenen diğer politika ve prosedürler uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
Veri Sorumlusu Kişisel Veri Koruma Uzmanı (Teknik ve İdari)	Veri Sorumlusu Kişisel Veri Koruma Uzmanı (Teknik ve İdari) İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Yöneticisine raporlanmasından; Kişisel Veri Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Veri Sorumlusu bünyesinde, kişisel veriler Kanunun belirtmiş olduğu hususlara uygun olarak işlenmekte ve işbu Politika'da belirtilen kayıt ortamlarında saklanmakla beraber yine bu politikada belirtilen şekilde imha edilmektedir.

Kişisel Veriler, Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartlarından birine veya birkaçına dayalı olarak ve bu kapsamda, kişisel verilerin işlenmesi için belirtilen şartların geçerliliği süresince kişisel veriler saklanmakta, söz konusu işleme şartları sona erdiğinde veya ilgili kişinin Veri Sorumlusu'na başvurusu üzerine, (Veri Sorumlusu'nun riayet etmesi gereken diğer hukuki yükümlülükleri kontrol edildikten sonra) uygun görülmesi halinde ilgili kişinin talebi üzerine saklanmakta olan kişisel veriler silinmekte, imha edilmekte veya anonim hale getirilmektedir.

5.1. Saklamayı Gerektiren Hukuki Sebepler

Veri Sorumlusu, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 4857 sayılı İş Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun,
- 3308 sayılı Mesleki Eğitim Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
- İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği,
- Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik,
- 1774 sayılı Kimlik Bildirme Kanunu
- 4904 sayılı Türkiye İş Kurumu Kanunu

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

5.2. Saklamayı Gerektiren İşleme Amaçları

Veri Sorumlusu, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri belirli amaçlar doğrultusunda saklamaktadır. Bu kapsamda amaçlar aşağıda sayılmıştır:

İşleme Amaçları
İş Faaliyetlerinin Yürütülmesi / Denetimi
Finans Ve Muhasebe İşlerinin Yürütülmesi
Yönetim Faaliyetlerinin Yürütülmesi
Hukuk İşlerinin Takibi Ve Yürütülmesi
Denetim / Etik Faaliyetlerinin Yürütülmesi
İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
Taşınır Mal Ve Kaynakların Güvenliğinin Temini
Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi
Fiziksel Mekan Güvenliğinin Temini
Lojistik Faaliyetlerinin Yürütülmesi
İletişim Faaliyetlerinin Yürütülmesi
Mal / Hizmet Satış Süreçlerinin Yürütülmesi
İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi

Sözleşme Süreçlerinin Yürütülmesi
İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
Faaliyetlerin Mevzuata Uygun Yürütülmesi
Risk Yönetimi Süreçlerinin Yürütülmesi
Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
Talep / Şikayetlerin Takibi
İnsan Kaynakları Süreçlerinin Planlanması
İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
Ücret Politikasının Yürütülmesi
Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
Görevlendirme Süreçlerinin Yürütülmesi
Eğitim Faaliyetlerinin Yürütülmesi
Diğer - Fesih İşlemlerinin Yürütülmesi
Diğer - İnsan Kaynakları Süreçlerinin Yürütülmesi
Acil Durum Yönetimi Süreçlerinin Yürütülmesi
Bilgi Güvenliği Süreçlerinin Yürütülmesi
Erişim Yetkilerinin Yürütülmesi
Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
Pazarlama Analiz Çalışmalarının Yürütülmesi

5.3. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11'inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Veri Sorumlusu tarafından kabul edilmesi,
- Veri Sorumlusu'nun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği

cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kurumuna şikâyette bulunması ve bu talebin Kurum tarafından uygun bulunması,

- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

- İlgili mevzuatlarda yer alan saklama sürelerinin sona ermesi,

6. KİŞİSEL VERİLERİN GÜVENLİ ŞEKİLDE SAKLANMASI, HUKUKA AYKIRI İŞLENMESİ VE ERİŞİMİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Veri Sorumlusu, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır. Ayrıca Veri Sorumlusu Kanun'un 12. maddesiyle Kanunun 6'ncı maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kişisel Verileri Koruma Kurumu tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde teknik ve idari tedbirler de almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

6.1. Teknik Tedbirler

Veri Sorumlusu, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

Teknik Tedbirler
Ağ güvenliği ve uygulama güvenliği sağlanmaktadır
Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır
Anahtar yönetimi uygulanmaktadır
Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır
Erişim logları düzenli olarak tutulmaktadır
Gerektiğinde veri maskeleme önlemi uygulanmaktadır
Güncel anti-virüs sistemleri kullanılmaktadır
Güvenlik duvarları kullanılmaktadır
Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır
Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır
Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır
Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir
Şifreleme yapılmaktadır

6.2 İdari Tedbirler

Veri Sorumlusu, kişisel verilerin saklandığı tüm ortamların, ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

İdari Tedbirler
Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur
Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır
Çalışanlar için yetki matrisi oluşturulmuştur
Gizlilik taahhütnameleri yapılmaktadır
Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır
İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir
Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir
Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır
Kişisel veri güvenliğinin takibi yapılmaktadır
Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır
Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır
Kişisel veri içeren ortamların güvenliği sağlanmaktadır
Kişisel veriler mümkün olduğunca azaltılmaktadır
Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır
Mevcut risk ve tehditler belirlenmiştir
Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır
Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır

7. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Veri Sorumlusu, Kanuna ve sair mevzuat ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri,

İmha Sebepleri
Kişisel Verilerin Korunması Kurulu'nun Kişisel Verinin İmhasına Yönelik Kararı
Saklama Süresinin Sona Ermesi

İlgili Kişi Talebi

sebepleriyle işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

Veri Sorumlusu tarafından kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

7.1 Silme Yöntemleri

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

Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler silinir.

Fiziksel Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Karartma	Fiziksel ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep, kullanılarak görünemez hale getirilmesi şeklinde yapılır.
Bulut ve Yerel Dijital Ortamda/ Yazılımlarda Tutulan Kişisel Veriler İçin Silme Yöntemleri	
Yazılımdan güvenli olarak silme	Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler saklanmasını gerektiren sürenin sona ermesiyle veri tabanı yöneticisi hariç diğer ilgili çalışanların hiçbir şekilde erişemeyeceği şekilde dijital komutla silinir ve tekrar kullanılamaz hale getirilir.
Sunucularda Yer Alan Kişisel Veriler	
Erişim yetkisini kaldırarak silme	Erişim yetkisini kaldırarak silme Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılır ve silme işlemi yapılır.

7.2 Yok Etme Yöntemleri

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

Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler yok edilir.

Fiziksel/Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel yok	Fiziksel yok etme Matbu ortamda tutulan belgeler evrak imha makineleri

etme	ile tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel Dijital Ortamda ve Sunucularda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Fiziksel yok etme	Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.
De-manyetize etme (degauss)	De-manyetize etme (degauss) Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
Üzerine yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
Erişim yetkisini kaldırarak yok etme	Erişim yetkisini kaldırarak yok etme Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılır ve bir daha ulaşılamayacak şekilde yok etme işlemi yapılır.
Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Yazılımdan güvenli olarak silme	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

7.3 Anonimleştirme Yöntemleri

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Aşağıda yer alan tabloda verilen yöntemlerden bir veya birkaçı kullanılarak kişisel veriler anonim hale getirilir.

Fiziksel/Matbu Ortamda Tutulan Kişisel Veriler İçin Anonim Hale Getirme Yöntemleri	
Değişkenleri çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.
Bölgesel gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin

	silinmesi işlemidir.
Genelleştirme	Genelleştirme Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.
Alt ve üst sınır kodlama / Global kodlama	Alt ve üst sınır kodlama / Global kodlama Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir. Aynı kategori içinde kalan değerler birleştirilir.
Mikro birleştirilme	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. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
Veri karma ve bozma	Veri karma ve bozma Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.
Dijital Ortamda/Sunucularda/Bulut Ortamın Tutulan Kişisel Veriler İçin Anonim Hale Getirme Yöntemleri	
Maskeleme (Şifreleme, simge kullanma, bulanıklaştırma, karıştırma, geçersizleştirme)	Maskeleme (Şifreleme, simge kullanma, bulanıklaştırma, karıştırma, geçersizleştirme) Veri maskeleme kişisel verilere yetkisiz kişiler tarafından erişilmesini engellemek amacıyla anlaşılmaz hale getirilmesidir. Bu yöntem kurumda bulunan gizli ve hassas bilgilerin kurum içerisine ve kurum dışarısına sızmasını, kötü niyetli kişilerce ele geçirilmesini engellemek amacıyla kullanılmaktadır. Veri maskelemede veri formatı değiştirilmez sadece değerler değiştirilir ancak bu değişim herhangi bir şekilde tespit edilmeyecek ve geri döndürülmeyecek şekilde yapılmaktadır. Ayrıca kimlerin hangi verilere ulaşabileceği belirlenerek sadece yetkisi olan kişilerin görmesi gereken bilgileri görmesi ve diğer bilgilerin maskelenmesi sağlanır.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Veri Sorumlusu tarafından faaliyetler kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Veri Sorumlusu Kişisel Veri İşleme Envanterinde,
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta,
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında
- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Veri Sorumlusu Kişisel Veri İşleme Envanterinde,
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta,

- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

8.1 Saklama ve İmha Süreleri

Veri Kategorisi	Saklama Süresi
Kimlik	Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - İşleme amacının sona ermesinden itibaren 10 Yıl Diğer - İş akdinin sona ermesinden itibaren 15 Yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 Yıl Diğer - İş ilişkisinin sona ermesinden itibaren 15 Yıl Diğer - İş akdinin sona emesinden itibaren 15 Yıl Diğer - İşleme amacının sona ermesinden itibaren 5 yıl 1 Yıl
Görsel ve İşitsel Kayıtlar	Diğer - İş akdinin sona ermesinden itibaren 15 yıl
Özlük	Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl
Hukuki İşlem	Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl
İletişim	Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - İşleme amacının sona ermesinden itibaren 10 Yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 Yıl Diğer - İş ilişkisinin sona ermesinden itibaren 15 Yıl Diğer - İşleme amacının sona ermesinden

	itibaren 5 yıl 1 Yıl
Fiziksel Mekân Güvenliği	Diğer - İş akdinin sona ermesinden itibaren 15 yıl 1 Ay
Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl
Finans	Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 Yıl
Lokasyon	Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - İş akdinin sona ermesinden itibaren 15 Yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - İş akdinin sona emesinden itibaren 15 Yıl Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl
Müşteri İşlem	Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl
Risk Yönetimi	Diğer - İş akdinin sona ermesinden itibaren 15 yıl Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl
Diğer - Araç Bilgisi	Diğer - İş akdinin sona ermesinden itibaren 15 Yıl Diğer - Hukuki ilişkinin sona ermesinden itibaren 10 yıl Diğer - İş akdinin sona emesinden itibaren 15 Yıl
Sağlık Bilgileri	Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl

	Diğer - İş ilişkisinin sona ermesinden itibaren 15 Yıl
Mesleki Deneyim	Diğer - Faaliyetin sona ermesinden itibaren 10 Yıl Diğer - İş akdinin sona ermesinden itibaren 15 yıl
Diğer - Çalışan Aile Bireyi ve Yakını Bilgisi	Diğer - İş akdinin sona ermesinden itibaren 15 yıl
İşlem Güvenliği	Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl Diğer - İşleme amacının sona ermesinden itibaren 5 yıl
Pazarlama	Diğer - Veri işleme amacının sona ermesinden itibaren 10 yıl

8.2 Veri İmha Süreleri

Veri Sorumlusu, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmhası Politikası uyarınca sorumlu olduğu 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.

İlgili kişi, Kanunun 13'üncü maddesine istinaden Veri Sorumlusu'na başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Veri Sorumlusu talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Veri Sorumlusu'nun talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikası'na uygun olarak yapmış olması gerekir. Veri Sorumlusu, her halde yapılan işlemle hakkında ilgili kişiye bilgi verir.

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Veri Sorumlusu tarafından Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

9. PERİYODİK İMHA SÜRESİ

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Veri Sorumlusu, işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri ilk kez …… tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

Veri Sorumlusu nezdinde kayıtları tutulan kişisel veriler Politika gereği saklama süresinin ve/veya yasal saklama sürelerinin bitmesi nedeniyle periyodik imha süreçlerinin bir parçası olarak imha çalışmasına konu edilmekte ve süreç Kişisel Veri İmha Tutanağı ile belgelenmektedir.

10. POLİTİKANIN YAYINLANMASI VE SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kağıt), basılı veya elektronik QR Kod ve doğrudan elektronik ortamda olmak üzere üç farklı şekilde yayınlanır, Veri Sorumlusu'nun https://www.bmsgeridonusum.com.tr/ internet sayfasında kamuya açıklanır. Basılı kağıt nüshası da Veri Sorumlusu Yönetim Kurulunca veya Kişisel Veri Yöneticisince KVKK dosyasında saklanır.

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

11. UYUM VE DEĞİŞİKLİKLER

Veri Sorumlusu, Mevzuat hükümleri gereği ya da Veri Sorumlusu politikası gereği kişisel verilerin saklanması ve imha politikasında değişiklik yapma hakkına sahiptir.