MAPP PAZARLAMA VE TANITIM HİZMETLERİ TİCARET ANONİM ŞİRKETİ

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Versiyon 1

Hazırlayan:
MAPP Pazarlama ve Tanıtım Hizmetleri Ticaret Anonim Şirketi
Adres:
Atatürk Mahallesi Namık Kemalbey Cadde No: 17/1 Ataşehir İstanbul
Telefon: +90 216 575 93 60 **WEB:** www.mapp.com.tr

İÇİNDEKİLER

1. GİRİŞ

1.1. Amaç

İşbu Politika, MAPP Pazarlama ve Tanıtım Hizmetleri Ticaret Anonim Şirketi (bundan sonra kısaca **"**MAPP") 'nin işlem süreçleri kapsamında; T.C. Anayasası, 6698 sayılı Kişisel Verilerin Korunması Kanunu (bundan sonra kısaca "Kanun") ve ilgili ikincil mevzuat ile uluslararası düzenlemelere uygun olarak işlenen kişisel verilerin hukuka uygun olarak saklanması ve imha edilmesi açısından benimsenen esas ve usulleri ortaya koymaktadır. Kurumsal olarak benimsenen "şeffaflık" niteliğinin bir gereği olarak kişisel verilerin saklanması ve imhası işbu Kişisel Verilerin Saklanması ve İmhası Politikası (bundan sonra kısaca "Politika") ile açıklanmaktadır.

Kişisel verilerin saklanması ve imhası süreçleri MAPP tarafından, işbu Politikaya uygun olarak gerçekleştirilir.

1.2. Kapsam

İşbu Politika; müşteri, müşteri adayı, çalışan, çalışan adayı, ziyaretçi, katılımcı, iş ve çözüm ortağı hissedarı veya çalışanı gibi veri sahibi ilgili kişilerin MAPP tarafından işlenen tüm kişisel verilerinin saklama ve imhasına ilişkin faaliyetler bütününü kapsamaktadır.

1.3.Tanımlar ve Kısaltmalar

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Birim Arşivi	Kurum ve kuruluşların görev ve faaliyetleri sonucu kendiliğinden teşekkül eden ve bu kuruluşların çeşitli birimlerinde, aktüalitesini kaybetmemiş olarak aktif bir biçimde ve günlük iş akımı içinde kullanılan arşivlik malzemenin belirli bir süre saklandığı arşiv birimleri (taşra, bölge ve yurt dışı kuruluşlarında bulunan arşivler de birim arşivi sayılır).
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.
GVKT (GDPR)	Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
İlgili Kişi/Veri Sahibi	Kişisel verisi işlenen gerçek kişi.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, 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.
Kurum Arşivi	MAPP arşivi.
KVKK	6698 sayılı Kişisel Verileri Koruma Kanunu.

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	İşbu Kişisel Verileri Saklama ve İmha Politikası.
MAPP	MAPP Pazarlama ve Tanıtım Ticaret Anonim Şirketi.
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.
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 (VERBİS)	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
Yönetmelik	28 Ekim 2017 tarihli Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. KAYIT ORTAMLARI

Kişisel veriler, aşağıda Tablo 1'de sayılan elektronik ve elektronik olmayan ortamlarda, hukuka uygun ve güvenli bir şekilde saklanır.

Tablo 1: Kişisel Verilerin Kayıt Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar

• Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) • Yazılımlar (ofis yazılımları, portal, MAPP İK) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Yazıcı, tarayıcı, fotokopi makinesi	• Kâğıt, • Manuel Veri Kayıt Ortamları (Sözleşmeler ve fer'i dokümanları, ziyaretçi kayıt defterleri, gönderici-alıcı formları, anket formları, dilekçeler vb.), • Yazılı, basılı, görsel ortamlar.

3. SAKLAMA

3.1. Saklamayı Gerektiren Hukuki Sebepler

Kanun'un 4. maddesinde işlenen kişisel verinin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi" gerektiği belirtilmiş, 5. ve 6. maddelerinde ise, kişisel verilerin işleme şartları sayılmıştır. Buna göre, MAPP faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

MAPP tarafından işlenen kişisel verilerin saklanmasını gerektiren hukuki sebepler başlıca şöyledir;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 5651 s. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 397 sayılı Vergi Usul Kanunu
- 6098 sayılı Türk Borçlar Kanunu,
- 6100 sayılı Hukuk Muhakemeleri Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,

- 2004 sayılı İcra ve İflas Kanunu,
- 4857 sayılı İş Kanunu,
- 6365 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
- 5070 Elektronik İmza Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- Bu kanunlar uyarınca yürürlükte olan diğer yönetmelik, tebliğ, vb. ikincil düzenlemeler ile MAPP'ın yayınladığı yönerge, prosedür vd. iç düzenlemeler.

3.2. Saklamayı Gerektiren Amaçlar

MAPP'ın işlem süreçleri kapsamında işlenen kişisel verilerin saklamayı gerektiren amaçları aşağıda sayılmaktadır;

- Kanundan doğan yükümlülüklerin yerine getirilmesi,
- MAPP tarafından yürütülen faaliyet ve süreçler ile üstlenilen görevlerin icrası,
- MAPP'ın faaliyet alanı içerisindeki yükümlülükleri ile üstlendiği hizmetler ve sorumlulukların yerine getirilmesi için gerekli aksiyonların alınması,
- Sözleşme süreçlerinin yönetilmesi ve sözleşmelerin ifası,
- İnsan kaynakları süreçlerinin yönetilmesi,
- İletişim sağlanması,
- İş/Çözüm Ortakları ile ilişkilerin ve faaliyetlerin yürütülmesi,
- Mali/Finansal süreçlerin yönetilmesi,
- Doğmuş veya doğabilecek hukuki/cezai/idari uyuşmazlıkların takibi ve ispat külfetinin yerine getirilmesi,
- Anonim şirket statüsünün gerektirdiği zorunlu işlemlerin yapılması,
- Kurumsal politika, plan ve sürdürebilirliğin sağlanması,
- Kurum içi-kurum dışı eğitimlerin planlanması ve gerçekleştirilmesi,
- Toplantı hazırlık ve sonrası süreçlerin yönetilmesi,

- İstihdam edilenlere karşı yükümlülüklerin yerine getirilmesi,
- İstihdam edilenlere kurum içi rehberlik faaliyetlerinin yürütülmesi,
- Kurum içi denetimlerin sağlanması,
- Yapılan iş ve işlemlerin takibi, analiz ve raporlanması,
- İstatistiksel çalışmalar yapılması,
- Müşteri ilişkilerinin yönetilmesi,
- Müşteri memnuniyeti süreçlerinin yönetilmesi,
- MAPP işyerlerinin güvenliğinin sağlanması,
- Ziyaretçi ve toplantı kayıtlarının tutulması,
- Reklam faaliyetlerinin yürütülmesi,
- Öneri, talep ve şikayetlerin sonuçlandırılması (Örneğin; Bilgi Edinme Dilekçesi veya çağrı merkezi vb.).

4. İMHA

4.1. İmhayı Gerektiren Durumlar

Aşağıda belirtilen hallerde kişisel veriler imha edilir:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun MAPP tarafından kabul edilmesi,
- MAPP'ın, 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; Kurula şikâyette bulunması ve bu talebin Kurul 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.

Yukarıda sayılan durumlarında, MAPP tarafından kişisel veriler, ilgili arşiv yönetmeliği ve buna bağlı iç prosedürlere uymak suretiyle, ilgili kişinin Kanun m.13'e uygun talebi üzerine talep tarihinden itibaren en geç 30 (otuz) gün içerisinde silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.2. İmha Teknikleri

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, MAPP tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

4.2.1.Silme

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. MAPP tarafından en çok kullanılan silme teknikleri aşağıdaki Tablo 2'de açıklanmaktadır.

Tablo 2: Kişisel Verilerin Silinmesi Teknikleri

Veri Kayıt Ortamı	**Açıklama**
Sunucu Sistemlerinde Yer Alan Kişisel Veriler	Sunucu sistemlerinde yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Veri Tabanlarında Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer kullanıcılar ve uygulamalar için hiçbir şekilde erişilemez hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler MAPP tarafından re'sen silinir. Re'sen silme işleminde, evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı sistemlerde kişisel veri tutulması Kurum politikası olarak yasaktır.

4.2.2.Yok Etme

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. MAPP tarafından en çok kullanılan yok etme teknikleri aşağıdaki Tablo 3'de açıklanmaktadır.

Tablo 3: Kişisel Verilerin Yok Edilmesi Teknikleri

Veri Kayıt Ortamı	**Açıklama**
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, MAPP tarafından re'sen imha edilmektedir. Re'sen imhada, kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Disk Sistemlerinde, Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

4.2.3.Anonim Hale Getirme

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

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

MAPP tarafından, kişisel veriler hakkında; değişkenleri çıkartma, kayıtları çıkartma, alt ve üst sınır kodlama, bölgesel gizleme, örnekleme, mikro birleştirme, K anonimlik, L çeşitlilik, T çeşitlilik gibi teknikler kullanılmaktadır.

Veri kayıt ortamlarının her biri için Silme, Yok Etme ve Anonimleştirme politikalarının ayrı ayrı belirlenmesi gerekmektedir.

5. SAKLAMA VE İMHA SÜRELERİ

MAPP'ın kişisel veri işlenen süreçlerinin tek tek hukuki risk analizleri yapılmış olup, kanun ve ikincil mevzuata uygun olarak, kişisel veri kategorisi bazında saklama süre ve amaç tablosu hazırlanmıştır. Ekte bir örneği yer alan tabloda belirtilen saklama süreleri sona erdiğinde kişisel verilerin, MAPP tarafından imha edilmesi öngörülmektedir **(EK- Kişisel Veri Saklama Amaç ve Süreleri Tablosu)**.

6. PERİYODİK İMHA SÜRESİ

Yönetmelik'in 11. maddesi gereğince MAPP, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, MAPP'da, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

7. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK SAKLANMASINI VE İMHA EDİLMESİNİ SAĞLAMAK ÜZERE ALINAN TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin hukuka uygun olarak; işlenmesini, saklamasını ve imha edilmesini sağlamak üzere; gerek KVKK ve ikincil mevzuat hükümleri gerekse Kurul kararları ve rehberleri uyarınca alınması gereken teknik ve idari tedbirler alınarak kişisel verilerin hukuka uygun şekilde korunması sağlanmaktadır.

7.1. Teknik Tedbirler

- Sızma (Penetrasyon) testleri ile MAPP'ın bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim ve kullanıcıların yetkilendirilmesi (erişim ve yetki matrisi) ile kişisel verilerin işlenmesi sınırlandırılmaktadır.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirler alınmaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- MAPP internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak şifrelenmektedir.

7.2. İdari Tedbirler

MAPP tarafından işlenen kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Tüm çalışanlara, kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu, ikincil mevzuat, Kurul kararları ve diğer düzenlemelere uygun bir şekilde işlenmesinin sağlanması amacıyla periyodik olarak eğitimler verilmektedir.
- MAPP tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Kişisel veri işlemeye başlamadan önce MAPP tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir
- Alıcı gruplarıyla akdedilen sözleşmelere gizlilik ve kişisel verilerin korunmasına ilişkin maddeler eklenerek alıcı gruplarının kişisel verilerin korunmasına riayet etmeleri sağlanmaktadır.

- İlgili kişinin kişisel verilerini imhaya yönelik talebinin uygun bulunması durumunda Yönetmelik m. 12/b gereği, alıcı gruplarına aktarılan kişisel verilerin alıcı grupları tarafından da imha edilmesinin temin edilmesine yönelik prosedür oluşturulmuştur.
- MAPP içinde kişisel verilerin korunması ve uyum süreçlerini yönetmek üzere üst ve alt komiteler oluşturulmuştur.
- Arşiv sorumluları tarafından arşivlere yetkisiz girişlerin engellenmesi ve kişisel verilerin saklandığı fiziksel ortamların güvenliğinin sağlanması için gerekli çalışmalar yapılmaktadır.
- Veri güvenliği hususunda risk analizleri gerçekleştirilmektedir.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmelerin takip edilmesi ve gerekli aksiyonların alınması hususunda hukuki ve teknik danışmanlık hizmetleri alınmaktadır.
- Kişisel verilerin personelin çalışma ortamı içerisinde de korunmasına ilişkin uygulama talimatlarına yer verilmekte ve uyulmadığı takdirde yaptırıma bağlanmaktadır (Örneğin; personel bilgisayarlarının şifreli olması ve bilgisayar kilitlenmeden çalışma ortamının terk edilmemesi, banko gişe masa gibi yerlerde bulunan kişisel verilerin başkaları tarafından görülmesini, duyulmasını engellemeye yönelik tedbirler vb.).
- MAPP internet sitesinde "Gizlilik" sekmesi içerisinde kişisel verilerin korunmasına ilişkin olarak; genel aydınlatma metni, bilgilendirme formu ve veri sorumlusu olarak MAPP'a başvuru formu gibi dokümanlara yer verilmiştir.

7.3. Özel Nitelikli Kişisel Verilerle İlgili Tedbirler

MAPP, özel nitelikli kişisel verilerin niteliği itibariyle ilgili kişi açısından özel bir önem taşımakta olduğu ve kritik bir değere sahip olduğu bilinciyle hareket ederek, özel nitelikli verilerin saklanmasında, alıcı gruplarına aktarılmasında ve imhasında, yukarıda sayılan teknik ve idari tedbirlere ek olarak birtakım tedbirler alarak, söz konusu verilere özel bir koruma atfetmektedir. Böylelikle, Kurul'un 31.01.2018 tarihli ve 2018/10 sayılı kararına uygun olarak koruma sağlanmaktadır.

Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

Özel nitelikli kişisel verilere ilişkin olarak alınan ek teknik ve idari aşağıda sayılmaktadır;

- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
- Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, MAPP tarafından kendisine tahsis edilen envanterin iade alınması,
- Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

- Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Verilere bir yazılım aracılığı ile erişilmesi halinde, bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Verilere uzaktan erişim halinde en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle aktarılması,
- Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında IPSec VPN kurularak veya kriptolu yöntemlerle veri aktarımının gerçekleştirilmesi.

7.4. Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi

MAPP nezdine alınan tedbirlerin uygulanmasına yönelik olarak, şikâyet üzerine veya re'sen denetim ve incelemeler gerçekleştirilmekte olup, tespit edilen eksiklikler derhal giderilmektedir. Öte yandan MAPP Yönetim Kurulu kararı ile kurulmuş olan Kişisel Verilerin Korunması Üst ve Alt Komiteleri aracılığıyla hem alınan tedbirlerin denetimi hem de daireler arası iş birliği sağlanarak kişisel verilerin işlenmesi ve korunması süreçlerinde meydana gelebilecek risk ve ihlaller gerçekleşmeden engellenmektedir. Bununla birlikte alınan teknik ve idari tedbirlere riayet edilmemesi halinde ilgili personel hakkında disiplin prosedürleri işletilmektedir.

Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.

Güvenlik politika ve prosedürlerine uymayan çalışanlara uygulanacak disiplin prosedürü hazırlanmıştır.

MAPP içinde periyodik ve rastgele denetimler yapılmaktadır.

8. SORUMLULUK ve GÖREV DAĞILIMI

MAPP'ın tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm

ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 4'te verilmiştir.

Tablo 4: Sorumluluk ve Görev Dağılımı

UNVAN	**BİRİM**	**GÖREV**
Bilişim Uzmanı	Bilişim Birimi	Veri güvenliği hususunda teknik tedbirlerin alınmasını ve denetim yapılmasını sağlamaktadır.
İrtibat Kişisi	Hukuk Müşavirliği	Kişisel verilerin korunması açısından MAPP'ın İrtibat Kişisi olarak Kurul ile MAPP arasındaki iletişimin sağlanmasından sorumludur.
MAPP'ın tüm personeli	Tüm Birimler	Birimlerin görev kapsamına giren faaliyet konularında işbu Politikaya uygunluğun sağlanmasından sorumludur.

9. UYGULAMA VE YÜRÜRLÜK

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da MAPP'da saklanır.

İşbu Politikada düzenlenen hususlar, KVKK ve ikincil mevzuata tabi olup, Politika ile mevzuat hükümleri arasında çelişki olması halinde, mevzuat hükümleri uygulanacaktır.

İşbu Politika, MAPP'ın internet sitesinde yayımlanarak yürürlüğe girer.

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