1. **Referans Standart:** BS 10012:2017 Madde 5.2
Mevzuat: KVKK | KEP Yön. Md. 5/g, 16/d, 16/i | Kimlik Doğ. Yön. Md. 7/4

1. AMAÇ

BS 10012:2017 Md. 5.2

Bu politika; ARK Dijital Yazılım A.Ş.'nin Kayıtlı Elektronik Posta Hizmet Sağlayıcısı (KEPHS) sıfatıyla yürüttüğü faaliyetler kapsamında kişisel verilerin işlenmesine ilişkin temel ilkeleri, yönetim çerçevesini ve sorumlulukları belirlemek amacıyla hazırlanmıştır.

Politika; 6698 sayılı Kişisel Verilerin Korunması Kanunu, KEP Yönetmeliği ve BS 10012:2017 standardı gereksinimlerini karşılayan, denetlenebilir ve sürdürülebilir bir kişisel veri yönetim sistemi (KVYS) kurulmasını esas almaktadır.

2. KAPSAM

BS 10012:2017 Md. 4.3

Bu politika; KEP hizmet alıcıları, KEP hesap sahipleri, işlem yetkilileri ve çalışanlar dahil olmak üzere ARK Dijital tarafından herhangi bir ortamda işlenen tüm kişisel verileri kapsar.

- Kapsam dahilindeki başlıca kişisel veri kategorileri şunlardır:
- KEP hesap sahibi kimlik ve iletişim bilgileri;
- işlem yetkilileri kayıtları;
- kimlik doğrulama ve görüntülü doğrulama kayıtları;
- PAdES işlem belgeleri;
- KEP kayıtları;
- imza ve zaman damgası verileri.

Politika; tüm çalışanlar, yöneticiler, alt yükleniciler ve kişisel veriye erişim yetkisi bulunan üçüncü taraflar için bağlayıcıdır.

3. REFERANSLAR

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- Kayıtlı Elektronik Posta Hizmet Sağlayıcıları Hakkında Yönetmelik — Madde 5/g, 16/d, 16/i
- Kayıtlı Elektronik Posta Rehber Hizmet Sağlayıcıları Tebliği
- Kimlik Doğrulama Yönetmeliği — Madde 7/4

- BS 10012:2017 Kişisel Bilgi Yönetim Sistemi
- ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi
- KVKK Veri Güvenliği Rehberi (KVKK Kılavuzu)

4. TANIMLAR

BS 10012:2017 Md. 3

- **Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
- **Özel Nitelikli Kişisel Veri:** Irk, etnik köken, siyasi düşünce, dini inanç, sağlık, biyometrik veriler ve benzeri, işlenmesi özel koruma gerektiren veriler. Görüntülü kimlik doğrulama sürecinde elde edilen veriler bu kapsamda değerlendirilir.
- **Veri Sorumlusu:** Kişisel verilerin işlenme amaç ve yöntemlerini belirleyen kuruluş. Bu politika kapsamında ARK Dijital Yazılım A.Ş.
- **Veri İşleyen:** Veri sorumlusu adına kişisel veri işleyen gerçek veya tüzel kişi.
- **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
- **KVYS (Kişisel Veri Yönetim Sistemi):** BS 10012:2017 çerçevesinde kurulan, kişisel verilerin korunmasına yönelik politika, süreç, kontrol ve kayıtları kapsayan yönetim sistemi.
- **DPIA (Veri Koruma -mahremiyet- Etki Değerlendirmesi):** Kişisel veri işleme faaliyetlerinin bireylerin hakları ve özgürlükleri üzerindeki risklerini değerlendirmeye yönelik süreç.

5. SORUMLULUKLAR

BS 10012:2017 Md. 5.1, 5.3

- **Üst Yönetim;** bu politikayı onaylama, gerekli kaynakları tahsis etme, KVYS'nin etkinliğini yönetim gözden geçirmesi aracılığıyla izleme ve kişisel veri yönetimini kurumsal stratejinin bir parçası olarak sahiplenme sorumluluğunu taşır.
- **Veri Koruma Sorumlusu (DPO) / Kişisel Veri Yönetim Temsilcisi;** KVYS'nin kurulmasını, uygulanmasını ve sürekliliğini koordine eder. Veri ihlali bildirimlerini yönetir, DPIA süreçlerini yürütür, mevzuat değişikliklerini izler ve çalışanların farkındalığını destekler.
- **Birim Yöneticileri;** kendi süreçlerinde kişisel veri işleme faaliyetlerinin bu politikaya uygunluğunu sağlar, veri envanterinin güncelliğini korur ve ekiplerinin eğitimini destekler.
- **Çalışanlar;** bu politika ve ilgili prosedürlere uymakla yükümlüdür. Gözlemledikleri ihlal veya riskleri derhal raporlar.

- **Alt Yükleniciler ve Veri İşleyenler;** imzaladıkları Veri İşleme Sözleşmesi (DPA) kapsamında bu politikanın ilgili hükümlerine uymakla sorumludur.

6. POLİTİKA

6.1 Temel İlkeler

BS 10012:2017 Md. 4.4, 8.2

ARK Dijital, kişisel verileri aşağıdaki ilkeler doğrultusunda işler:

- Hukuka ve dürüstlük kurallarına uygunluk.
- Doğruluk ve güncellik.
- Belirli, açık ve meşru amaçlar için işleme.
- Amaçla bağlantılı, sınırlı ve ölçülü veri işleme.
- Saklama sürelerinin mevzuata uygun belirlenmesi.
- Veri güvenliğinin teknik ve idari tedbirlerle sağlanması.

6.2 Hukuki Dayanak ve Amaç Sınırlaması

BS 10012:2017 Md. 8.2.1, 8.2.2

Kişisel veriler yalnızca aşağıdaki hukuki dayanaklardan birine dayalı olarak işlenir: kanunlarda açıkça öngörülmüş olması; veri sahibinin açık rızası; bir sözleşmenin kurulması veya ifasına doğrudan ilgi bulunması; veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi; meşru menfaat.

KEP hizmetinin zorunlu kıldığı kimlik doğrulama, rehber kaydı, delil üretimi ve saklama işlemleri Yönetmelik'ten doğan hukuki yükümlülük kapsamında değerlendirilir.

6.3 Tasarım olarak mahremiyet ve Temel mahremiyet

BS 10012:2017 Md. 6.1, 8.1

ARK Dijital, kişisel veri korumayı sistem ve hizmet tasarımının başlangıcından itibaren gözetir. Yeni sistem, hizmet veya süreç tasarımında mahremiyet gereksinimleri işlevsel gereksinimlerle eş zamanlı değerlendirilir. Varsayılan ayarlar, kişisel veri işlemeyi gerekli asgari düzeyde tutacak biçimde yapılandırılır.

6.4 Veri Yaşam Döngüsü Yönetimi

- Kişisel veri toplama aşamasında yalnızca işleme amacının gerektirdiği veriler toplanır. Aydınlatma yükümlülüğü ve gerektiğinde açık rıza alınması toplama öncesinde yerine getirilir.

- Saklama aşamasında veriler veri envanterinde tanımlanan saklama süreleri boyunca güvenli şekilde saklanır. KEP delilleri ve ilgili işlem belgeleri Yönetmelik gereği en az 20 yıl saklanır.
- İmha aşamasında saklama süresi dolan veriler, Kişisel Veri Saklama ve İmha Politikasında belirlenen yöntemlerle imha edilir ve imha kaydı tutulur.

6.5 Açık Rıza Yönetimi

Açık rıza; anlaşılır bir dil ile, belirli bir konu için, özgür iradeyle ve önceden alınır. Rıza kayıtları elektronik ortamda saklanır ve gerektiğinde ibraz edilebilir. Veri sahibi rızasını geri alabilir; bu durumda işleme durdurulur ve kayıt güncellenir. Görüntülü kimlik doğrulama sürecinde elde edilen biyometrik nitelikli veriler için açık rıza zorunludur.

6.6 Veri Sahibi Hakları

ARK Dijital; veri sahiplerinin bilgi alma, düzeltme, silme, işlemenin kısıtlanması, itiraz ve taşınabilirlik haklarını güvence altına alır. Başvurular belirlenen kanal üzerinden alınır ve yasal süreler içinde (kural olarak 30 gün) yanıtlanır. Yanıtlanamayan başvurular gerekçesiyle birlikte bildirilir. Başvuru ve yanıt kayıtları veri sahibi hakları sicilinde tutulur.

6.7 Veri Koruma Etki Değerlendirmesi (DPIA)

Yüksek risk içeren veri işleme faaliyetleri öncesinde DPIA yürütülür. DPIA zorunlu tutulan başlıca durumlar şunlardır:

- görüntülü kimlik doğrulama ve biyometrik veri işleme;
- büyük ölçekli özel nitelikli veri işleme,
- otomatik karar alma ve profilleme;
- yeni teknoloji kullanımı.

Mahremiyet etki değerlendirme sonuçları dokümante edilir, kalıntı riskler kabul edilir veya kontrol tedbirleri uygulanır.

6.8 Veri Güvenliği

Kişisel veriler; erişim kontrolü, şifreleme, günlük kaydı ve izleme, fiziksel güvenlik ve yedekleme mekanizmaları aracılığıyla korunur. Teknik ve idari güvenlik tedbirleri ISO/IEC 27001:2022 gereksinimleri ve KVKK Veri Güvenliği Rehberi çerçevesinde uygulanır.

6.9 Kişisel Veri İhlali Yönetimi

Tespit edilen veya şüphelenilen her veri ihlali derhal Veri Koruma Sorumlusu'na bildirilir. İhlal değerlendirmesi yapılır; bireylerin haklarını etkileyen ihlaller 72 saat içinde KVKK'ya bildirilir. Veri sahipleri gereken durumlarda bilgilendirilir. İhlal kayıtları ve alınan önlemler dokümante edilir.

6.10 Alt Yüklenici ve Üçüncü Taraf Yönetimi

Kişisel veri işleyen tüm alt yükleniciler ve üçüncü taraflarla Veri İşleme Sözleşmesi (DPA) imzalanır. Alt yüklenicilerin veri koruma yeterlilikleri sözleşme öncesinde değerlendirilir ve periyodik olarak gözden geçirilir. Yurt dışına veri aktarımı KVKK'nın öngördüğü güvencelere dayandırılır.

6.11 Farkındalık ve Eğitim

Kişisel veriye erişimi olan tüm personel göreve başlama ve periyodik dönemlerde KVKK ve KVYS farkındalık eğitimi alır. Eğitim katılım kayıtları saklanır.

6.12 Politikanın Gözden Geçirilmesi

Bu politika en az yılda bir kez, mevzuat değişikliklerinde, önemli güvenlik olaylarında veya organizasyonel değişikliklerde gözden geçirilir.

7. KAYITLAR

Veri envanteri ve işleme kayıt tablosu. Açık rıza kayıtları. Veri sahibi başvuru ve yanıt sicili. Mahremiyet Etki Değerlendirme raporları. Veri ihlali kayıt defteri. DPA sözleşmeleri. Eğitim katılım kayıtları. Veri imha tutanakları.

8. İLGİLİ DOKÜMANLAR

- Kişisel Veri Saklama ve İmha Politikası
- Kişisel Veri Envanteri İşleme Yönetimi Prosedürü
- Veri Sahibi Hakları Prosedürü
- Kişisel Veri İhlal Müdahale Prosedürü (ARKD-PR-17)
- KEP Alt Yüklenici Veri İşleme Sözleşmesi (DPA)
- KVKK Aydınlatma Metni