

**YENİ NESİL AKARYAKIT POMPA
ÖDEME KAYDEDİCİ CİHAZLARA AİT
ÖKC TSM TEKNİK KILAVUZU**

Sürüm 2.0

30 ARALIK 2021

YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM TEKNİK KILAVUZU

Amaç

MADDE 1 – (1) Bu Kılavuzun amacı, yeni nesil akaryakıt pompa ödeme kaydedici cihazlara ait ÖKC TSM'lerinin kurulması, işletilmesi, yönetimi ve denetimine ilişkin usul ve esasları ile kapsama dahil olanların bu Kılavuzda belirtilen hususlardaki sorumluluklarını düzenlemektir.

Kapsam

MADDE 2 – (1) Yeni nesil akaryakıt pompa ödeme kaydedici cihaz üreticileri, üye işyeri anlaşması yapan kuruluşlar, dış hizmet sağlayıcıları ve faaliyetlerinde yeni nesil akaryakıt pompa ödeme kaydedici cihaz kullanan işyerleri bu Kılavuz kapsamındadır.

Dayanak

MADDE 3 – (1) Bu Kılavuz, 213 sayılı Vergi Usul Kanununun mükerrer 257'nci maddesinin birinci fıkrasının 1,3 ve 6 numaralı bentleri ile 3100 sayılı Katma Değer Vergisi Mükelleflerinin Ödeme Kaydedici Cihazları Kullanmaları Mecburiyeti Hakkında Kanununun 10'uncu maddesi ve 527 Sıra No.lu Vergi Usul Kanunu Genel Tebliğine dayanılarak düzenlenmiştir.

Tanımlar ve Kısaltmalar

MADDE 4 – (1) Bu Kılavuzda yer alan;

- a) **Bakanlık:** Hazine ve Maliye Bakanlığını,
- b) **Başkanlık:** Gelir İdaresi Başkanlığını,
- c) **BDK:** Bağımsız Denetim Kuruluşunu,
- ç) **BDDK:** Bankacılık Düzenleme ve Denetleme Kurumunu,
- d) **BİM:** Bilgi İşlem Merkezini,
- e) **Cihaz/ ÖKC/ YN Pompa ÖKC:** Bakanlık/Başkanlık BİM ile (EFT-POS ile bütünleşik tasarlanarlarda üye işyeri anlaşması yapan kuruluşlar ile de) doğrudan ya da bağlı oldukları ÖKC TSM aracılığı ile sürekli çevrimiçi çalışabilen, IP tabanlı oluşturduğu fiş ve mali raporları güvenli şekilde iletebilen, akaryakıt pompalarına bağlanacak ve teknik özellikleri 527 Sıra No.lu Vergi Usul Kanunu Genel Tebliği ile bu Teknik Kılavuzda belirtilen yeni nesil akaryakıt pompa ödeme kaydedici cihazı,
- f) **IP:** İnternet Protokolünü,
- g) **ÖKC Üreticisi/Firma:** YN Pompa ÖKC'lerin üretimi/ithali, satışı ve satış sonrası bakım/onarım hizmetlerinin yürütülmesi için Bakanlıktan onay alan ve ÖKC TSM'den sorumlu olan üretici firmayı,
- ğ) **ÖKC TSM (Akaryakıt Pompa Ödeme Kaydedici Cihazlar Terminal Servis Merkezi):**
YN Pompa ÖKC bilgilerinin (üretim, aktivasyon, hurdaya ayırma, devir, bakım vb. işlemlere ait) takip edilmesi, bu cihazların üreteceği fiş veya rapor bilgilerinin Başkanlıkça belirlenen teknik standartlara uygun olarak gizlilik ve güvenliği sağlanarak toplanması, saklanması, işlenmesi, anlık ve/veya periyodik olarak Bakanlık/Başkanlık BİM'e iletilmesi, mükellefler ve ÖKC üreticilerine sunulması ve raporlanması hizmetlerini gerçekleştirmek üzere Başkanlıkça yetkilendirilecek Akaryakıt Pompa Ödeme Kaydedici Cihazlar Terminal Servis Merkezlerini,

- h) **DHS (Dış Hizmet Sağlayıcı):** ÖKC Üreticisine, ÖKC TSM'ine ilişkin hizmet veren kuruluşu,
- i) **EFT-POS:** EMV uyumlu kartlı ödeme sistemleri terminalini,
- i) **Akıllı PinPad Cihazı :** Kart kullanılarak elektronik fon transferi ile ödeme yapmaya yarayan satış terminalini,
- j) **PCI DSS (Payment Card Industry Data Security Standard):** PCI SSC tarafından yayımlanan veri güvenliği standardını,
- k) **PCI SSC (Payment Card Industry Security Standards Council):** Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyini,
- l) **PIN (Personal Identification Number) Güvenliği:** Kart hamilinin kimliğini doğrulama amaçlı kullanılan, sadece kart hamilinin bildiği en az dört rakamdan oluşan değer in güvenliğini belirleyen esasları,
- m) **ISO 20000:** Bilgi Teknolojileri Servis Yönetim Sistemini,
- n) **ISO 22301:** Uluslararası İş Sürekliliği Yönetimini,
- o) **ISO 27001:** Bilgi Güvenliği Yönetim Sistemini,
- ö) **İkincil Merkez:** Kanun ve ilgili mevzuatında, ÖKC TSM için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği anda erişim sağlayan yedek sistemlerin kullanıma hazır olacak şekilde tesis edildiği, herhangi bir kesinti durumunda tüm işlemlere ilişkin faaliyetlerin iş sürekliliği planında ve toplam kullanılabilirlik kurallarına uygun olarak belirlenen kesinti süreleri içerisinde sürdürülür hale getirilmesine ve kuruluşun faaliyetleri sürdürmede kullandığı asıl sistemlerin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş ve yurt içinde, birincil sistemden farklı bir il sınırında ve en az 300 km mesafede yer alan merkezi,
- p) **Korunaklı Sistem:** Bünyesindeki hassas verilere fiziksel ve yazılımsal olarak erişimi kısıtlayan, şifreleme anahtarlarının korunmasını ve yönetimini sağlayan, yetkisiz erişimleri fark eden ve bunlara tepki veren, birimlerinin yetkisiz olarak değiştirilmesi ve çıkarılması ile yeni birim eklenmesi faaliyetlerini algılamaya ve bunlara tepki vermeye yönelik kontroller içeren, çevresel ve operasyonel şartların değiştirilmesi, normal çalışma şartlarının dışına çıkılması veya yazılımsal anormallikler oluşturulması dolayısıyla sağladığı güvenlik seviyesinin azalmayacağına ilişkin makul güvence sunan sistemi ve bu sisteme destek hizmetini gerçekleştirebilecek yönetici ile yeterli sayı ve nitelikte personelin çalıştığı merkezi,
- r) **Denetim İzi:** Operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,
- s) **Güvenli Şifreleme:** Kimlik doğrulama, veri bütünlüğünü sağlama, gizlilik ve mahremiyeti temin etme ve inkâr edememe şartlarını sağlama amaçlarıyla kullanılabilen, literatürde kabul görmüş ve güvenilirliğini yitirmemiş güçlü bir algoritma ile yeterli uzunlukta ve güvenliği kriptografik anahtar yönetimi süreci ile sağlanmış anahtarlar kullanılarak gerçekleştirilen, anahtar kullanılmaksızın şifrelenmemiş verinin elde edilmesi teorik olarak mümkün olsa bile pratikte gerektirdiği zaman ve kaynaklar dikkate alındığında uygulanabilir olmayan şifreleme faaliyetlerini,
- ş) **Kriptolojik Anahtar Yönetim Süreci:** PIN güvenlik kuralları ile anahtarın ve başlangıç vektörleri, sayaçlar gibi ilgili diğer güvenlik parametrelerinin oluşturulması, dağıtımı, saklanması, yüklenmesi ve kullanılması, ömrünü tamamlamasının ardından veya

güvenliği zedelendiğinde yeni bir anahtar oluşturularak eski anahtarın imhası veya arşivlenmesinin yazılı ve etkin bir biçimde yönetilmesi sürecini,

- t) **GMP:** YN Pompa ÖKC'ler, ÖKC TSM ve Bakanlık/Başkanlık BİM ile çevre birimleri arasındaki güvenli iletişimi ve fiş, mali raporlar, olay kayıtları vb.'nin mesajlaşma yapısını içeren haberleşme protokol dokümanını,
 - u) **Yetkilendirilmiş ESHS:** YN Pompa ÖKC'lere, ÖKC TSM'lerine ve Başkanlık BİM'e yüklenecek sertifikaların üretimi, dağıtımı ve sonrasında yönetimini ve denetimini gerçekleştirecek kurum (TÜBİTAK Kamu Sertifikasyon Merkezi) ya da Başkanlık tarafından yetkilendirilmiş sertifika otoritesi olan kurumu,
 - ii) **Sertifika:** Yetkilendirilmiş ESHS tarafından üretilen; ÖKC'lere, ÖKC TSM'e ve BİM'e iletilen X509 sertifikalarını,
 - v) **ÖKC Mesajları:** GMP dokümanında belirtilen BİM'e iletilecek olan mesajları,
 - y) **Teknik Kılavuzlar:** Başkanlık tarafından YN Pompa ÖKC'ler ile ilgili yayımlanmış olan teknik kılavuzları,
 - z) **Sızma Testi:** ÖKC TSM'nin güvenlik açıklarını, istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen testi,
- aa) **Simetrik Şifreleme:** Veriyi şifrelemek ve şifreli veriyi açmak için aynı anahtarın kullanıldığı şifreleme yöntemini,
- bb) **Üye İşyeri Anlaşması Yapan Kuruluş:** 5464 Sayılı Banka ve Kredi Kartları Kanunu ile 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkındaki Kanun kapsamında yetki almış kuruluşlarını,
- cc) **BSDHY:** 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,
- ifade eder.

ÖKC TSM'nin Kuruluş Esasları

MADDE 5 – (1) YN Pompa ÖKC Üreticileri, bu Kılavuzun 4-1 maddesinde tanımlanan PCI DSS, ISO 20000, ISO 22301 ve ISO 27001 standartlarını haiz olarak bir ÖKC TSM kurmak veya bu standartları sağlayan bir Dış Hizmet Sağlayıcısının sunduğu ÖKC TSM hizmetinden yararlanmak zorundadır. YN Pompa ÖKC'ye Başkanlık tarafından onay verilebilmesi için YN Pompa ÖKC'nin akredite kuruluşlardan alınmış bu maddede belirtilen sertifikalara haiz bir ÖKC TSM kurması veya dış hizmet sağlayıcısından hizmet alması gerekmektedir.

(2) Kurulan veya dış hizmet sağlayıcıdan faydalanılan ÖKC TSM'nin, bu maddede belirtilen standartları faaliyetleri süresince sağlamaları zorunludur. Söz konusu standartlardan herhangi birinin, ÖKC TSM'nin denetimi sırasında karşılanmadığının tespiti halinde; Başkanlık tarafından yazı ile bildirilecek tamamlama süresi içinde eksikliklerini tamamlamayan ÖKC TSM'nin (Dış Hizmet Sağlayıcıları dahil) izinleri Başkanlık tarafından iptal edilebilecektir.

(3) ÖKC TSM tamamen ÖKC Üreticisi tarafından kurulabileceği gibi ÖKC Üreticisinin yetki ve sorumluluğunda kısmen veya tamamen bir Dış Hizmet Sağlayıcıdan hizmet temin etmek suretiyle de kurulabilir.

(4) ÖKC TSM hizmetlerin kısmen veya tamamen bir dış hizmet sağlayıcısından temin edilmesi halinde; TSM tarafından yerine getirilmesi beklenen faaliyetlerin gerçekleştirilmesinden

müşterek ve müteselsil sorumluluk esasında olmak üzere dış hizmet sağlayıcısı ÖKC Üreticisi ile birlikte sorumludur.

ÖKC TSM Başvuru, Test, Denetim ve Onay Süreçleri

MADDE 6 – (1) ÖKC TSM'nin başvuru, test ve onay denetimi, sadece yetkili ÖKC onayı almış veya başvuruda bulunmuş firmalar için yapılması zorunlu olup ÖKC Üreticisi olmaksızın yapılan ÖKC TSM başvuruları dikkate alınmayacaktır. YN Pompa ÖKC onayı için Başkanlığa yapılacak yazılı müracaat, cihaz ve TSM onay başvurusu olmak üzere iki ayrı teknik dosya ile yapılmalıdır.

ÖKC TSM başvuru dosyasında bu Kılavuzun 5-1 maddesinde bahsi geçen belgelerin ve BDK ile yapılmış olan “Onay Denetimi” sözleşmesinin ibrazı gerekmektedir.

(2) ÖKC TSM test işlemlerine başlanabilmesi için, ÖKC Üreticileri ve Dış Hizmet Sağlayıcıları ÖKC TSM hizmetlerine ilişkin gerekli sertifikalara sahip olmalı ve bu sertifikalar Başkanlığa yapılan yazılı başvuru ekinde yer almalıdır. Bu yazılı başvuruya BDK Raporu (Onay Denetimi) ve ÖKC TSM'nin sahip olduğu donanımların marka, model, kapasite ve özellikleri ile yazılımlarının işleyiş süreçlerini anlatan teknik bir rapor da eklenecektir.

(3) ÖKC TSM'nin gerekli şartları haiz olup olmadığının tespiti için, yapılacak onay denetiminin, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş BDK veya TÜBİTAK tarafından yerinde yapılması zorunludur.

Onay denetimi, Başkanlıkça yayımlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu” nda yer alan “ÖKC TSM Onay Denetimi ve Yıllık Denetim Süreçleri Akışı”na uygun olarak yürütülür ve “Bilgi Sistemleri Denetim Adımları” ile “Güvenli Haberleşme Denetim Adımları” olmak üzere iki aşamadan oluşur.

ÖKC TSM'nin Başkanlık tarafından onaylanmasını müteakip yapılacak denetimleri üçer yıllık periyotlarla, “Bilgi Sistemleri Denetim Adımları”na göre yapılır ve “ÖKC TSM Denetim Raporu” düzenlenerek tamamlanır.

“Güvenli Haberleşme Denetim Adımları” onay sürecine münhasıran uygulanır. Ancak, Başkanlık tarafından GMP dokümanında değişiklik yapılması halinde, bu denetimlerin periyodik denetim faaliyetleri kapsamında tekrar edilmesi Başkanlık tarafından istenebilir.

Başkanlık, gerek görmesi halinde yerinde denetimi kendisi de yapabilir.

(4) Başkanlık gerekli belge ve olumlu denetim raporu kontrollerini yaptıktan sonra, ÖKC TSM tarafından BİM test ortamına bağlanılarak uçtan uca test çalışmalarına başlanılır.

(5) TÜBİTAK tarafından gerçekleştirilecek YN Akaryakıt Pompa ÖKC Teknik Kılavuzuna göre yapılan testler sırasında verilerin, GMP dokümanına uygun olarak Başkanlık tarafından verilen bağlantı noktası aracılığıyla ÖKC TSM üzerinden başarılı olarak BİM'e iletilmesi gerekmektedir.

(6) Tüm test süreçlerini başarılı şekilde tamamlayan ÖKC TSM'ye Başkanlık tarafından yazılı olarak “ÖKC TSM Onayı” verilir. ÖKC TSM, söz konusu onay yazısında belirtilen tarih itibari ile BİM'e veri gönderme işlemine başlamak zorundadır.

(7) GMP dokümanına uygun olarak hazırlanan “ÖKC TSM Uçtan Uca Test Senaryoları” Başkanlık tarafından ÖKC Üreticileri ile paylaşılır.

(8) ÖKC TSM, ÖKC Üreticisi için münhasıran kurulmuş donanım, yazılım ve işletimi içermeli ve sunulacak olan sertifikaların bu sistem için alınmış olması gerekmektedir.

(9) YN Pompa ÖKC onayı ancak BDK tarafından düzenlenen onay denetim raporunun TÜBİTAK tarafından kontrolü ve Başkanlığa gönderilmesine müteakip verilecektir.

ÖKC TSM'nin Yönetim Esasları

MADDE 7 – (1) YN Pompa ÖKC'lerin yaşam döngüsünün (Terminal ve Mesaj Yönetim Sistemi) ve ÖKC TSM'nin yönetim, yetki ve sorumluluğu ÖKC üreticilerindedir.

(2) ÖKC Üreticileri ÖKC TSM hizmetlerini DHS'den de temin edebilir. Bu hizmetin DHS'den temin edilmesi ÖKC Üreticisinin, ÖKC TSM hizmetlerine ilişkin sorumluluklarını ortadan kaldırmaz.

(3) YN Pompa ÖKC'ler BİM'e ÖKC TSM üzerinden bağlanacak olup, cihazların doğrudan veya ÖKC TSM'leri haricinde başka bir hat üzerinden BİM'e bağlanması mümkün değildir. ÖKC TSM'leri ile YN Pompa ÖKC'ler ve BİM arasındaki kurulacak olan güvenli altyapı, ağların sorumluluğu ve sahipliği ÖKC Üreticilerinde olacaktır. YN Pompa ÖKC'lerin ÖKC TSM'sine erişmeleri için gereken altyapı, erişim hatlarının sorumluluğu ve sahipliği ise ÖKC kullanan mükelleflere aittir.

(4) ÖKC TSM'leri, YN Pompa ÖKC'leri yönetme, ayakta tutma ve her işlemde cihazdan gelen GMP mesaj bilgilerinin içerisindeki hassas mali verilerin kaynağını kontrol etmekle, doğruluğunu, değişmezliğini ve bütünlüğünü koruyarak göndermekle yükümlüdür. Bu işlem sırasında Başkanlık hassas ÖKC verisinin ve üye işyeri anlaşması yapan kuruluşlara ait hassas verilerin ÖKC TSM tarafından açılmaması ve saklanmaması gerekmektedir. BİM'in cihazları yönetme, ayakta tutma, gelen bilgilerin doğruluğunu değerlendirme veya YN Pompa ÖKC'lerin durumu ile ilgili üreticiye veya ÖKC TSM'lerine geri bildirim yapma görevi bulunmamaktadır. Bu sorumluluk ÖKC Üreticileri ile birlikte ÖKC TSM'lerine aittir.

(5) ÖKC Üreticileri, cihazda oluşturularak ÖKC TSM'leri üzerinden BİM'e gönderilen Başkanlık ÖKC mesajlarının kaynağının doğruluğundan, değişmezliğinden ve bütünlüğünden sorumludur. Başkanlık ÖKC mesajlarının teknik kılavuzlarda ve protokollerde öngörülen zaman ve sıralamaya uygun olarak BİM'e gönderilmesi gerekmekte olup, bozuk, hatalı veya atak içeren mesajların gönderilmesi halinde sorumluluk ÖKC Üreticilerine aittir.

(6) YN Pompa ÖKC'lerin ÖKC TSM'leri üzerinden BİM'e gönderecekleri mesajların doğrudan BİM tarafından kayıt ve analiz edilebilecek mahiyette olması esas olup, bu mesajların üzerinde BİM'in ilave bir çalışma yapmasını gerektirmeyecek yapıda ve ilgili mesajlaşma protokollerine uygun şekilde olması esastır.

(7) ÖKC TSM'lerinin, EFT-POS özellikli ÖKC'ler ve EFT-POS cihazları ile entegre çalışan YN Pompa ÖKC'ler de dahil, bankacılık mesajlarının da üzerinden geçecek olması nedeniyle BDDK ve PCI SSC düzenleme ve standartlarının gereklerini karşılaması zorunludur.

(8) Üye işyeri anlaşması yapan kuruluşlara ait olanlar da dahil olmak üzere YN Pompa ÖKC'ler üzerinde çalışan tüm uygulamalar ÖKC TSM üzerinden YN Pompa ÖKC'lere bağlanacaktır. Üye işyeri anlaşması yapan kuruluşun yetkilendireceği kişi veya kurumlar, YN Pompa ÖKC ile birlikte çalışacak bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM'lerine bildireceklerdir. Bu işlemler ÖKC TSM aracılığıyla gerçekleştirilecektir. YN Pompa ÖKC'lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntıları vb.) ÖKC Üreticileri sorumludur.

(9) ÖKC TSM'leri (Dış Hizmet Sağlayıcılar dahil) vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmak zorundadır.

ÖKC TSM'nin Güvenlik Esasları

MADDE 8 – (1) ÖKC TSM'lerinin güvenlik gereksinimleri Başkanlıkça yayımlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu” nda belirtilen kurallar çerçevesinde sağlanacaktır. ÖKC TSM'lerinin sistem güvenliğinde ve sisteminin düzgün işleminde önemli ve dikkat edilmesi gereken temel hususlar bu doküman içerisinde yer almaktadır. Güvenlik gereksinim ana başlıkları aşağıdaki gibidir;

- a) **Kritik Varlıklar:** Sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu ve erişilebilirliğini olumsuz yönde etkileyecek varlıklardır.
- b) **Aktörler:**
 - 1) Yetkili Kullanıcılar (İç personel)
 - 2) Yetkisiz Kullanıcılar (Hacker, Siber Terörist vb.)
 - 3) Teçhizat ve Yazılımlar
 - 4) Çevresel Koşullar
- c) **Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale:** ÖKC TSM'nin sistem güvenliğinin oluşturulması, gerçekleşmesi, bakımının yaptırılması ve sürekli geliştirilmesi için ISO 27001 sertifikasının alınması gerekmektedir. Sistemin iş sürekliliğini ve felaketten kurtarma gereksinimlerinin standardizasyonunu sağlamak için ISO 22301 sertifikasının alınması gerekmektedir.
- ç) **Kullanılan Donanımların Güvenliği:** ÖKC TSM'nin; BİM ve YN Pompa ÖKC ile haberleşmek için kriptografik anahtarlar kullanılması ve bu anahtarların ÖKC TSM'lerinde ISO/IEC 19790, Common Criteria EAL4+ veya FIPS 140-2 level 3 ve üzeri sertifika almış HSM'ler (Hardware Security Module) ile saklanması gerekmektedir.
- d) **Kullanılan Yazılımların Güvenliği:** ÖKC TSM'nin kullandığı yazılımların güvenli olması gerekmektedir.
- e) **Güvenlik Denetimi:** Yılda bir kez Başkanlık ve ÖKC Üreticisi mutabakatıyla belirlenecek tarihlerde BDK tarafından gerçekleştirilecek sızma testleri ile proje genelinde hedeflenen bilgi güvenliği standardına ulaşıp ulaşılmadığı sınıanacak, tespit edilen açıklıkların kapatılmasına yönelik tavsiyeler detaylı bir şekilde bu firmalar tarafından Başkanlığa raporlanacaktır.

ÖKC TSM'nin Risk Yönetim Esasları

MADDE 9 – (1) ÖKC TSM, ÖKC mesajlarına dair işlemlerde kullandığı bilgi sistemlerine ve tüm operasyon süreçlerine ilişkin riskleri tespit etmek, analiz etmek, ölçmek, izlemek, kontrol etmek ve raporlamak üzere kapsamlı bir risk yönetim planı oluşturur.

(2) ÖKC TSM altyapısının bir parçası olan veya herhangi bir noktada ÖKC mesajlarını yöneten donanım, yazılım, uygulama geliştirme, değişim yönetim süreçleri, iletişim altyapıları ve operasyon süreçleri risk yönetim planına dâhil edilir.

(3) ÖKC Üreticisi, ÖKC TSM'nin uyguladığı risk yönetim planı çerçevesinde, faaliyetlerinde kullandığı bilgi teknolojisi varlıklarının risk analizini, Dış Hizmet Sağlayıcılarından kaynaklanabilecek riskleri de dikkate alarak gerçekleştirir. Bu kapsamda varlık envanteri hazırlar, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemleri belirler, yazılı hale getirir.

(4) Bilgi sistemlerine ilişkin risk analizleri, hizmetleri etkileyen önemli güvenlik olayları sonrasında, önemli bir değişiklik öncesinde ve yeni tehditlerin tespiti halinde gözden geçirilir ve yılda en az bir defa olmak üzere güncellenir.

ÖKC TSM'nin İş Sürekliliği Yönetimi

MADDE 10 – (1) ÖKC TSM, YN Pompa ÖKC'ler üzerinden sunduğu hizmetin sürekliliğini ve kesinti halinde faaliyetlerinin sürdürülebilmesini amaçlayan üst yönetim (ÖKC TSM'nin imzaya yetkili yönetimi) tarafından onaylanmış iş sürekliliği yönetim sürecini tesis eder. Bu kapsamda, iş sürekliliği planı ve bu planın bir parçası olan bilgi sistemleri süreklilik planını hazırlar.

(2) ÖKC TSM, iş sürekliliği planlamasına yönelik olarak iş etki analizi yapar ve kurtarma stratejilerini belirler. Bu kapsamda, iç ve dış bağımlılıklar belirlenir ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri ÖKC TSM tarafından değerlendirilir.

(3) İş sürekliliği yönetimi sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyleri dikkate alınarak iş etki analizi çerçevesinde kabul edilebilir kesinti süreleri belirlenir. Bu süreler içinde servislerin tekrar erişime açılabilmesini sağlamak amacıyla, alternatifli kurtarma prosedürleri ile yetki ve sorumlulukları içeren iletişim prosedürleri ÖKC TSM tarafından geliştirilir. Süreç kapsamında; performans takip teknikleri kullanılır, kapasite planlaması yapılır, işlem hacmi tahminleri doğrultusunda stres testleri gerçekleştirilir, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturulur. Ayrıca, servis dışı bırakma atakları göz önünde bulundurulur ve buna karşı gerekli önlemler ÖKC TSM tarafından alınır.

(4) ÖKC TSM tarafından, süreç kapsamında yurt içinde bir İkincil Merkez tesis edilir. Veri ve sistem yedekleri kurulan bu İkincil Merkezde kullanıma hazır bulundurulur.

(5) ÖKC TSM, bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra iş sürekliliği planını gözden geçirir ve günceller. Mevcut planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa bir günlük operasyonlarının tamamını İkincil Merkez üzerinden gerçekleştirecek şekilde testler yapar, test sonuçlarını ve hizmet sürekliliğini etkileyen olayları üst yönetime raporlar.

(6) ÖKC TSM, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en aza indirmek üzere acil ve beklenmedik durum planı oluşturarak gerekli önlemleri alır. Faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci ile beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis eder. Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulma, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçlerini ele alır. Bilgi sistemlerine ilişkin beklenmedik olayların sonradan incelenmesine imkân tanıyacak, yetkili merciler tarafından talep edildiğinde kullanılabilir nitelikte kayıt ve bilgileri toplayan bir mekanizma oluşturur.

(7) ÖKC TSM, YN Pompa ÖKC'ler üzerinden sunduğu hizmetler için üye işyeri anlaşması yapan kuruluşa sözleşmede taahhüt ettiği düzeyde servis sürekliliği sağlar ve raporlar.

(8) ÖKC TSM, ÖKC TSM bilgi sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde, mimari tasarımın ve testlerin yapıldığına dair güvence sunar. Bu kapsamda sunulacak güvence ve raporlamalar asgari olarak "Uptime Institute Tier 2" standartlarını sağlamalı/yerine getirmelidir. Kesinti süreleri yıllık plansız toplam 18 saati ve planlı bir defada 1,5 saati aşmayacak şekilde yılda 4 defadan (toplam 6 saatten) fazla olamaz. Planlı kesintilerin ÖKC TSM'sinden hizmet almakta olan üye işyeri anlaşması yapan kuruluşlara 15 gün önceden gerekçeleri ile birlikte bildirilmesi zorunlu olup planlı kesintilerin günün yoğun olmayan saatlerinde gerçekleştirilmesi gerekmektedir. ÖKC TSM aylık olarak kullanılabilirlik raporunu hazırlayarak Başkanlığa ve ÖKC TSM hizmeti almakta olan üye işyeri anlaşması yapan kuruluşlara sunacaktır. Aylık olarak hazırlanan bu raporlar denetimlerde sunulmak üzere hazır bulundurulacaktır.

Değişiklik Yönetimi

MADDE 11 – (1) ÖKC TSM, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve ÖKC mesajlarını yöneten donanım ve yazılımlara ilişkin her türlü bakım, güncelleme ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak yazılı ve etkin bir değişiklik yönetimi süreci işletir.

(2) ÖKC TSM, ÖKC mesajını yöneten yazılımlar için, yazılım geliştirilen ortamların ve geliştirilen yazılımların canlı ortama aktarılmadan önce test edileceği ortamların canlı ortamlardan ayrılmasını ve bu ortamların herhangi birinde değişiklik yapma yetkisine sahip personelin diğerlerinde değişiklik yapma yetkisinin bulunmamasını sağlamalıdır. Test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleştirilemez nitelikte olmasını da temin edecektir.

(3) ÖKC TSM, ÖKC mesajını yöneten sistemlere ilişkin değişikliklerde etki analizi yapılması, değişikliğin yetkili kişi veya kişilerce onaylanması ve değişikliği geri çekme prosedürünün oluşturulmasını sağlar.

ÖKC Mesajlarının Yönetimi

MADDE 12 – (1) YN Pompa ÖKC'ler, ÖKC TSM ve BİM arasındaki haberleşme ve mesaj yapıları GMP dokümanında açıklandığı şekilde yapılmalıdır.

Denetim İzlerinin Oluşturulması

MADDE 13 – (1) ÖKC TSM'leri, Yeni Nesil Akaryakıt Pompa ÖKC mesajlarının yönetildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, işlem altyapısını kullanan yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması tesis eder.

(2) Denetim izleri, kullanıcılara sorumluluk atayan, yeterli detay içeren ve şüpheli bir olayı izleme imkânı sunan nitelikte tutulur.

(3) Denetim izleri, asgari olarak aşağıdaki bilgileri içerir:

- a) İşlemi gerçekleştiren uygulama,
- b) İşlemi gerçekleştiren ve varsa onaylayan kişiler,
- c) İşlemin açıklaması,

- ç) Yapılan işlemin zaman bilgisi,
- d) İşlemin olumlu veya olumsuz sonucu,
- e) Etkilenen veri ve sistemlerin bilgisi.

(4) Denetim izleri, asgari 5 yıl süreyle denetime hazır bulundurulacak şekilde ÖKC TSM tarafından saklanır.

(5) Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır.

(6) Denetim izleri, yetkisiz değiştirilmeye karşı ayrıcalıklı yetkiye sahip kullanıcıların kendi faaliyetlerine ilişkin denetim izlerine müdahale edemeyeceği şekilde ÖKC TSM'leri tarafından korunur.

(7) Denetim izi mekanizmalarının geçici veya sürekli olarak durdurulmasını önlemeye ve durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(8) Denetim izlerinin yeterli güvenlik seviyesi bulunan ortamlarda saklanması, yedeklerinin alınması ve olası bir mücbir sebep ya da olağanüstü hal sonrasında erişilebilir olması gerekmektedir.

(9) Bilgi sistemleri faaliyetleri kapsamında dış hizmet alınıyor olması durumunda ÖKC Üreticisi ve DHS tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve kendisinin bu denetim izlerine erişebilirliğini temin eder.

(10) ÖKC Üreticisi, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin süreçlerini oluşturur.

(11) YN Pompa ÖKC'lere, ÖKC TSM'sinde denetim izi oluşturulmadan bir yazılım veya parametre yükleme işlemi yapılamaz.

Dış Hizmet Alımı

MADDE 14 – (1) Dış hizmet alan ÖKC Üreticisi, bu Kılavuzun 5-1 maddesi kapsamında almak zorunda olduğu ISO 20000, 22301, 27001 ve PCI DSS belgelerine DHS'nin uyumluluk onay durumunu izler ve aldığı hizmetin herhangi bir kapsam kısıtlamasına gitmeksizin mezkûr standartlar ile uyumlu olduğunun yılda bir defa belgelendirildiğinden emin olur.

(2) ÖKC Üreticileri, DHS'nin bu Kılavuzda belirlenen koşullar ile uyumlu olduğuna ve sistem altyapısının güvenlik seviyesini düşürmediğine DHS nezdinde gerçekleştirdiği denetimlerle veya başka taraflarca gerçekleştirilen yerinde denetimler sonucunda oluşturulan onay belgelerinden faydalanarak emin olur ve buna ilişkin belgelendirme dokümanlarını kendisinde muhafaza eder ve talep edilmesi halinde Başkanlığa sunar.

(3) ÖKC TSM'lerinin Birincil ve İkincil Merkezleri (DHS'den temin edilenler dahil) yurt içinde olmak zorundadır. ÖKC TSM'lerine ilişkin İkincil Merkezlerinin; Birincil Merkezden farklı bir il sınırları içinde ve aralarında en az 300 km mesafe bulunacak şekilde kurulmuş olması zorunludur.

(4) ÖKC Üreticileri, kendi kuracakları ÖKC TSM'sine ait Birincil Merkezin donanım altyapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil Merkezin tüm işletim ve operasyon süreçlerini ÖKC Üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personel nitelik ve niceliği ile ilgili "ÖKC TSM Personel Gereksinimleri" başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir

kısının ÖKC Üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC TSM'si DHS'nin verdiği bu hizmetler bakımından da test, değerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC Üreticileri kendi kuracakları ÖKC TSM'lerine ait İkincil Merkezin; sadece donanım altyapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, İkincil Merkeze ait donanım altyapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC Üreticisinin kendi personeli tarafından yürütülmesi zorunludur.

DHS, ÖKC TSM'lerine ait İkincil Merkezin; sadece donanım altyapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, İkincil Merkeze ait donanım altyapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ilgili DHS/ ÖKC Üreticisinin kendi personeli tarafından yürütülmesi zorunludur.

ÖKC TSM'nin Denetim Esasları

MADDE 15 – (1) Onay Denetimi; ÖKC TSM'si olmak için Başkanlığa başvuruda bulunan ÖKC Üreticilerinin kurmuş oldukları sistemin Başkanlık tarafından talep edilen gerekli şartları haiz olup olmadığının tespiti için gerçekleştirilen denetim sürecidir. ÖKC TSM'lerinde gerçekleştirilecek Onay Denetim faaliyetleri esas itibariyle “Bilgi Sistemleri Denetimi” ve “Güvenli Haberleşme Denetimi” olarak isimlendirilen iki kısımdan oluşmaktadır.

(2) Periyodik Denetim; ÖKC TSM'nin Başkanlık tarafından onayını takip eden her 3 yılda en az 1 defa olmak kaydı ile gerçekleştirilecek olan denetim sürecidir. ÖKC TSM'lerinde gerçekleştirilecek denetim faaliyetleri, ÖKC TSM onay denetiminde de yer alan “Bilgi Sistemleri Denetimi” sürecini kapsamaktadır.

(3) Bilgi Sistemleri Denetimi; ÖKC TSM'lerinin bu Kılavuzda belirtilen kurallara uyum durumunun tespit edilmesi amacıyla verileri yöneten kişiler, süreçler, yazılımlar, donanımlar ile bu kapsamda tesis edilen iş süreçleri ve iç kontrollerin Başkanlık tarafından belirlenen BDK (ÖKC TSM ve ÖKC Üreticisi ile doğrudan veya dolaylı yönetim, temsil görevi bulunmayan) tarafından değerlendirilmesi sonucunda, söz konusu iç kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir. Bilgi sistemleri denetiminin uygulama ve raporlama esasları “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu”nda detaylı olarak düzenlenmiştir.

(4) Güvenli Haberleşme Denetimi; ÖKC TSM'lerinin bu Kılavuzda belirtilen hükümlere uyum durumunun tespit edilmesi amacıyla, ÖKC TSM'lerinin YN Pompa ÖKC ve BİM ile olan mesajlaşma yönetiminin; Başkanlıkça yayımlanan/paylaşılan ve ÖKC TSM'lerine doğrudan veya dolaylı olarak etki eden mesajlaşma protokolü ve dokümanlarında yer alan esaslara (GMP'ler, Başkanlıkça yapılan diğer yazılı bildirimler vb.) uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir. Bilgi sistemleri denetiminin uygulama ve raporlama esasları “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu”nda detaylı olarak düzenlenmiştir.

(5) Başkanlık, gerekli gördüğü hallerde Bilgi Sistemleri Denetiminin kapsamını ve sıklığını değiştirebilir.

(6) Denetimler sonucunda düzenlenen raporda tespit edilen sorun ve eksiklikler ÖKC TSM'leri tarafından ivedilikle giderilir.

(7) ÖKC TSM'si, herhangi bir kapsam kısıtlamasına gidilmeden ve işlem sayısından bağımsız olarak, PCI DSS ile uyumlu olduğunu, asgari yılda bir defa, standartları PCI SSC tarafından tanımlanmış olan yerinde denetimler ile ispatlar.

(8) ÖKC TSM'si, gerçekleştirilen denetimler sonucunda oluşturulan Denetim Mektubunu ve PCI DSS onay belgelerini, hizmet verdiği bütün üye işyeri anlaşması yapan kuruluşlar ile paylaşmak zorundadır.

(9) ÖKC TSM'sinde gerçekleştirilecek denetim faaliyetlerine ilişkin usul ve esaslar Başkanlıkça yayımlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu” nda belirlenmiştir.

ÖKC Üreticileri ve Üye İşyeri Anlaşması Yapan Kuruluşlara İlişkin Esaslar

MADDE 16 – (1) ÖKC Üreticileri, YN Pompa ÖKC'ler üzerinde veya YN Pompa ÖKC'lerle birlikte çalışacak cihazlarda (EFT-POS, PinPad), üye işyeri anlaşması yapan kuruluşlara ait uygulamaların (Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlar Teknik Kılavuzunda belirtilen şekilde) uyumlu olarak çalıştırılmasını sağlamak zorundadır.

(2) Üye işyeri anlaşması yapan kuruluşun YN Pompa ÖKC'nin yaşam döngüsü kapsamındaki yazılım geliştirme, program yükleme, güncelleme, parametre yükleme, kartlı işlemlerin yönetimi, güvenli anahtar yönetimi, terminal güvenlik kontrolleri, işlemlerin yönlendirilmesi, çalıştırılması ve sonuçlarının sözleşmelere ve sözleşmelerde belirtilen kriterlere (SLA- Service Level Agreement) uygun şekilde iletilmesi vb. faaliyetlerinin yetki ve sorumluluğu ÖKC Üreticilerindedir.

(3) YN Pompa ÖKC'ler üzerinde veya YN Pompa ÖKC'ler ile birlikte çalışacak cihazlar (EFT-POS, PinPad) yoluyla üye işyeri anlaşması yapan kuruluşun uygulamalarının çalıştırılmasına ilişkin sahada yapılması gereken tüm servis ve saha operasyonlarının yetki ve sorumluluğu ÖKC Üreticilerindedir.

(4) ÖKC Üreticileri, üye işyeri anlaşması yapan kuruluşa vereceği hizmetler kapsamında Başkanlık tarafından belirlenen standartlara uymak ve ilgili sertifikalara sahip olmak zorundadır.

(5) Üye işyeri anlaşması yapan kuruluş, hizmet aldığı ÖKC TSM'nin PCI DSS ile uyumlu olduğuna ve işlem altyapısının güvenlik seviyesini düşürmediğine ilişkin, gerçekleştirdiği denetimlerden veya geçerliliğini yitirmemiş denetim raporu, sertifika gibi belgelerden faydalanarak makul güvence oluşturur.

(6) Üye işyeri anlaşması yapan kuruluşlar, sahtecilik ve dolandırıcılık faaliyetlerinin önlenmesine yönelik olarak, anlaşması bulunan üye işyerleri ve YN Pompa ÖKC'ler için takip mekanizmaları tesis eder. Takip ettiği alanlarda olağan dışı değişiklik meydana gelen üye işyerleri ile YN Pompa ÖKC'ler için, gerekli incelemeleri gerçekleştirerek uygun aksiyonları alır, ÖKC Üreticisine ve ÖKC TSM'sine bu konuda gereken bilgilendirmeleri yapar.

(7) ÖKC TSM'leri, Başkanlık ve yasalarca yetkili kılınmış diğer kurumlardan gelen talimatlar doğrultusunda YN Pompa ÖKC'lerin fonksiyonlarının tümünü veya belli bir kısmını durdurabilir veya değiştirebilir.

(8) ÖKC Üreticileri ve bunlara ait ÖKC TSM'leri Başkanlıktan gelen talimatlar doğrultusunda veya ÖKC Üreticilerinin oluşturduğu sahtekarlık senaryolarına göre otomatik izleme mekanizmalarını ve raporlamalara uygun şekilde sahtekarlık önleme ve izleme sistemini kurmakla yükümlüdür.

(9) EFT-POS özellikli YN Pompa ÖKC'ler ve haricen EFT-POS ile entegre çalışan YN Pompa ÖKC'lerde terminal yönetim ve üye işyeri anlaşması yapan kuruluşlar ile iletişim YN Pompa ÖKC ve ÖKC TSM üzerinden şifreli olarak GMP'lerde veya Başkanlıkça yazılı olarak belirtilen kurallara göre gerçekleştirilecektir.

(10) EFT-POS cihazlarının YN Pompa ÖKC'ye haricen bağlı olması halinde aşağıdaki esaslara uyulması gerekmektedir.

- a) EFT-POS cihazı ile YN Pompa ÖKC arasındaki iletişim ÖKC-Harici Donanım ve Yazılım Haberleşme Protokolü (GMP-3) kurallarına ve Başkanlıkça izin verilen diğer esaslara göre gerçekleştirilecektir.
- b) EFT-POS cihazı, ÖKC TSM üzerinden yapılan yönlendirme ile üye işyeri anlaşması yapan kuruluş bilgi sistemleri ile haberleşecektir.
- c) ÖKC TSM, EFT-POS cihazı verilerini şifreli olarak üye işyeri anlaşması yapan kuruluşlara, sözleşmelerinde belirtilen kriterlere (SLA- Service Level Agreement) ve PCI-DSS kurallarına uygun şekilde iletecektir.
- ç) Finansal işlemler YN Pompa ÖKC'den başlayacak ve EFT-POS cihazı GMP-3 kurallarına veya Başkanlıkça izin verilen kurallara göre tetiklendikten sonra provizyon işlemlerini gerçekleştirmek amacıyla ÖKC TSM üzerinden şifreli olarak haberleşecektir. Bu suretle provizyon alındıktan sonra ödeme işlem bilgisi EFT-POS cihazından YN Pompa ÖKC'ye aktarılacaktır.

(11) Üye işyeri anlaşması yapan kuruluşlara ait Başkanlık tarafından hassas veri olarak kabul edilen verilerin ÖKC TSM tarafından her halükarda açılmaması ve saklanmaması gerekmektedir (Başkanlık tarafından ÖKC Üreticilerine yapılacak yazılı bildirim ile ÖKC TSM'sinde açılmasına izin verilen finansal veri dışında kalan mali rapor verileri hariç).

(12) ÖKC TSM'lerinin, müşteriler (kart hamilleri) ile ilişkilendirilebilecek hiçbir veriye ve Başkanlık tarafından hassas veri olarak tanımlanan verilere erişebilme kabiliyeti bulunamaz. Bu Kılavuzda yer verilen sorumlulukları esnasında söz konusu veriye erişmesinin gerekmesi halinde, erişilebilen verinin anonim olması ve herhangi bir müşteri ile ilişkili olmaması sağlanır.

Üye İşyeri Adına Verilecek Olan Katma Değerli Hizmetler

MADDE 17 – (1) Faaliyetlerinde YN Pompa ÖKC kullanan mükellefler (üye işyeri) adına ve bir sözleşmeye bağlı olmak koşulu ile ÖKC TSM ve ÖKC Üreticisi üye işyerine yönelik katma değerli özel uygulamalar geliştirebilir, ÖKC üzerindeki bu uygulamalara ait verileri YN Pompa ÖKC veya ÖKC TSM üzerinde sözleşmede belirtilen kurallar çerçevesinde işleyebilir, iletebilir, saklayabilir ve raporlayabilir.

(2) Tüm katma değerli uygulamalar teknik kılavuzlara, GMP dokümanlarına ve Başkanlıkça yazı ile izin verilen durumlara uygun olarak geliştirilir ve iletir.

(3) Üye işyeri ile ÖKC Üreticisi ve ÖKC TSM (DHS dahil) arasında yapılacak olan sözleşmelerde; işlenecek, saklanacak ve raporlanacak olan verilerin içeriği, saklama süresi, gizlilik kuralları ile ilgili yetki ve kapsamın açıkça belirtilmesi zorunludur.

(4) Bu sözleşmelerin elektronik ortamdaki bir örneğinin, sözleşmenin imzalandığı tarihten itibaren 15 gün içinde BİM'e elektronik ortamda aktarılması gerekmekte olup buna ilişkin sorumluluk ÖKC üreticilerindedir.

Mevcut Teknik Kılavuz ve GMP Dokümanlarının Uyumlandırılması

MADDE 18 – (1) Bu Kılavuzda belirlenen kurallar çerçevesinde ihtiyaç duyulması halinde mevcut teknik kılavuzlar ve GMP dokümanları Başkanlık tarafından güncellenecek ve gizlilik esasları da göz önünde bulundurularak Başkanlık internet sitesinde yayımlanacaktır.

ÖKC TSM'leri İçin Uygulanacak Diğer Esaslar

MADDE 19 – (1) ÖKC TSM'leri için “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait TSM Başvuru, Test, Denetim ve Onay Teknik Kılavuzu”nda tanımlanan kritik varlıklar; Fiş Mesajları ve Plaka Bazlı Günlük Satış Raporu ile sınırlandırılmıştır. YN Pompa ÖKC'lerden Düzenlenecek Fiş Ve Rapor Formatları Teknik Kılavuzu’nda belirtilen diğer raporların da kritik varlık sınıfına eklenmesi Başkanlık tarafından talep edilebilir.

(2) Kritik varlıklar GMP dokümanında belirtildiği şekilde BİM’e iletilecektir.

(3) ÖKC Üreticileri veya ÖKC TSM'leri YN Pompa ÖKC'lerin, durum bilgilerini, olay kayıtlarını ve fiş, Plaka Bazlı Günlük Satış Raporu vb. mali bilgilerini, BİM’e ulaştırma amacı dışında başka hiç bir amaçla kullanamaz ve/veya üçüncü kişilere kullanılamaz, paylaşım açamazlar. Bu mahremiyet hükümlerine aykırı davrandığı tespit olunan ÖKC Üreticileri ile ÖKC TSM'lerinin Bakanlığımız ve/veya Başkanlığımız tarafından verilen onay ve izinleri belli bir süreyle durdurulabilir ya da iptal edilebilir.

(4) ÖKC Üreticileri ile ÖKC TSM'leri (DHS'ler dahil); ÖKC ile ilgili TSM aracılığıyla yerine getirecekleri kendilerine ait sorumluluklarını ve Başkanlığa karşı her türlü bildirim yükümlülüklerini (cihaz bilgileri ve cihazların üreteceği rapor bilgilerini) müşterek ve müteselsil sorumluluk altında gerekli her türlü teknik (donanımsal, yazılımsal vb.) önlemleri alarak sağlayacaklarını birlikte yazılı olarak Başkanlığa taahhüt etmeleri durumunda ve bankacılık ve kartlı ödeme işlem kurallarına aykırı olmamak şartıyla, TSM altyapısını birlikte kullanabilirler.

Geçiş Hükümleri ile Sorumluluklar

MADDE 20 – (1) ÖKC TSM onay başvurusu Başkanlık tarafından kabul edilen ÖKC Üreticilerinin, ÖKC TSM onay denetimlerini Başkanlık tarafından belirtilen süre içerisinde yaptırımları zorunludur.

(2) BDK tarafından düzenlenen “Periyodik Denetimi” raporunun bu kılavuzda belirlenen süre içerisinde ibraz edilmemesi durumunda YN Pompa ÖKC'lerin mühürleme ve satış işlemleri Başkanlık tarafından durdurulur ve/veya ÖKC Üreticisi izinleri iptal edilir. İzni iptal edilen üreticiler tarafından satılmış ve mükelleflerce kullanılmakta olan YN Pompa ÖKC'lerin mali hafızalarında kayıtlı bilgiler ÖKC yetkili servislerince raporlanır ve bu raporlar mükellef tarafından ilgili vergi dairesine verilerek cihaz hurdaya ayrılma işlemine tabi tutulur. Hurdaya ayrılan cihazın rayiç veya emsal bedelinin mükellefe geri ödenmesinden ilgili ÖKC Üreticisi sorumludur. Bu yükümlülüklerin ÖKC Üretici onaylarının iptal edildiğinin Başkanlık tarafından duyurulduğu tarihten itibaren en geç 60 gün içerisinde yerine getirilmesi gerekmektedir.

(3) YN Pompa ÖKC'lerin sahada bulunduğu süre içerisinde belirlenen kurallar dâhilinde tüm saha ve bakım hizmetlerinin sorumlusu ÖKC Üreticisidir.

(4) Üye işyeri anlaşması yapan kuruluşun uygulamalarının YN Pompa ÖKC üzerinde çalışması için sahada yapılması gereken tüm kurulum, servis ve operasyonların sorumlusu ÖKC Üreticisidir.

(5) Güvenilir Sertifika Otoritesi ile anlaşma yapılması, sertifika temini, sertifikaların yüklenmesi, bunun için uygun yapıların kurulması ve işletilmesi sorumluluğu ÖKC Üreticisine aittir.

(6) YN Pompa ÖKC'ye bağlı olarak çalışacak olan bütün çevre birimlerinin ve yazılımların GMP'lerde belirlenen kurallara uygun olarak çalışmasına yönelik saha ve servis hizmetlerinin verilmesinin sorumluluğu ÖKC Üreticisine aittir.

(7) YN Pompa ÖKC'ler sadece kendi ÖKC TSM'leri ile haberleşecektir. Bu kuralın hayata geçirilmesi ve korunması yetki ve sorumluluğu ÖKC Üreticisine aittir.

(8) ÖKC TSM'nin BİM ile haberleşmesinin yönetilmesi sorumluluğu ÖKC TSM'leri ile birlikte ÖKC Üreticisine aittir.

(9) ÖKC TSM'nin üye işyeri anlaşması yapan kuruluş ile haberleşmesinin sorumluluğu ÖKC TSM'leri ile birlikte ÖKC Üreticisine aittir.

(10) YN Pompa ÖKC'ye bağlı olarak çalışacak olan barkod, EFT-POS, PinPad, otomasyon veya harici diğer tüm sistemlerin uyumlaştırma, entegrasyon işlemlerinin GMP'lerde belirtilen kurallara göre sağlanması yetki ve sorumluluğu ÖKC Üreticisine aittir.

Yürürlük

MADDE 21 – (1) Bu Kılavuz www.ynokc.gib.gov.tr internet adresinde yayımlandığı tarihte yürürlüğe girer.

Yürütme

MADDE 22 – (1) Bu Kılavuz hükümlerini Gelir İdaresi Başkanlığı yürütür.