**Kimlik Doğrulama Hizmet Sağlayıcısının****, Elektronik Kimlik Doğrulama Sistemi ve Güvenli Kart Erişim Cihazı Çözümleri İle Sosyal Güvenlik Kurumuna Biyometrik Kimlik Doğrulama Sistemi Dahilinde Hizmet Sunumundaki Yükümlülükleri ve Yükümlülükleri Yerine Getirirken Veri Güvenliğinin Sağlanmasıyla Kişisel Verilerin Korunmasına İlişkin Taahhütname**

**FİRMA ADI**:………………

Kimlik doğrulama hizmet sağlayıcısı olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5490 Sayılı Nüfus Hizmetleri Kanunu, 22.09.2020 tarihli ve 31282 Sayılı Resmî Gazetede yayımlanarak yürürlüğe giren T.C. Kimlik Kartı Elektronik Kimlik Doğrulama Yönetmeliği ile 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67. maddesinin amaçları doğrultusunda iş bu taahhütname ve eklerinde yer alan hususları okuduğumuzu, anladığımızı ve bu hususlara uygun davranacağımızı kabul, beyan ve taahhüt ederiz.

Bu taahhütname kapsamında,

**Bakanlık:** T.C. İçişleri Bakanlığı’nı,

**Beyaz Liste:** NVİGM tarafından kimlik doğrulama işlemi yapması onaylanmış Kart Erişim Cihazı listesini,

**EKDS:** Türkiye Cumhuriyeti kimlik kartının elektronik kimlik doğrulama işlemlerinde kullanılabilmesini sağlayan sistemi,

**NVİGM:** Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü,

**KEC:** NVİGM tarafından GEM talebi onaylanmış ve resmî web sayfasında yayımlanmış üreticilere ait Kart Erişim Cihazı,

**KDHS:** NVİGM tarafından Kimlik Doğrulama Hizmet Sağlayıcısı olarak onay almış ve resmî web sayfasından yayımlanmış firma,

**Kurum:** Sosyal Güvenlik Kurumu,

**Yönetmelik:** 22.10.2020 tarih ve 31282 sayılı Resmî Gazete yayımlanarak yürürlüğe giren Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği,

**SHS:** Kurum ile sözleşmeli/protokollü sağlık hizmet sunucusunu,

ifade etmektedir.

# KDHS’NİN YÜKÜMLÜLÜKLERİ

1. KDHS olarak sunacağı tüm EKDS hizmetleri ve kullanacağı KEC’ lerden birinci derecede sorumlu olmak.
2. Kurduğu altyapı sistemindeki beyaz listeyi NVİGM’ nin resmi internet sitesinde yayımlanan yöntem ile belirtilen süre içerisinde NVİGM ile paylaşmak. Kurum uygulamasında kullanılacak olan tüm KEC’ leri ayrıca Kuruma bildirmek.
3. Kurumun belirleyeceği periyotlarda, KEC’ lerin kurulu olduğu tesis bazında, doğrulama, doğrulanmama, kaçıncı denemede doğrulama yapıldığı, doğrulama yöntemi vb. bilgilerin yer aldığı raporları üretip Kurumun belirleyeceği yöntemlerle paylaşmak.
4. Verdiği hizmeti, Kurum ve NVİGM ile paylaştığı beyaz liste ile sınırlamak, sertifika geçerlilik süresi biten ve/veya beyaz listeden çıkarılmış olan KEC’ ler üzerinden Kuruma hizmet vermemek, bu cihazları Kurumun belirleyeceği yöntemlerle Kurum ile paylaşmak ve bu işlemlerle ilgili gerekli altyapıyı hazırlamak.
5. EKDS ile ilgili verdiği hizmette kullandığı donanım ve yazılımların EKDS standartlarına uygunluğuna ve bunların güvenliğine ilişkin gerekli tedbirleri almak. EKDS’ de oluşabilecek değişikliklere en kısa sürede uyum sağlamak.
6. EKDS’ ye ilişkin imza oluşturma ve doğrulama verileri ile sertifikasını ve KEC’ lerde kullanılan GEM kartlarını Türkiye Cumhuriyeti sınırları dışına çıkarmamak. Yurt içine ve yurt dışına veri sızıntısını engellemek üzere her türlü tedbiri almak.
7. EKDS’ ye ilişkin kayıtları yalnızca NVİGM tarafından belirlenen ve resmî web sitesinde yayımlanan yöntemlerle ve ilgililerle paylaşılmak üzere, EKDS standartlarına uygun şekilde geri izleme bilgisi olarak 8 (sekiz) yıl süreyle saklamak. Kurum uygulaması kapsamında yapılan kimlik doğrulama işlemleriyle ilgili tüm kayıtları ayrıca Kurumun belirleyeceği yöntemlerle düzenli olarak Kurumla paylaşmak.
8. KDHS bünyesindeki EKDS sunucularına ve çevre birimlerine karşı yetkisiz erişimlerin engellenmesi amacıyla geri izleme ve güvenlik sistemi kurmak.
9. Kimlik doğrulama hizmetini 7/24 esasına göre kesintisiz ve güvenli bir şekilde vermek.
10. Gerekli acil durum eylem planlarını ve iş sürekliliği planlarını hazırlamak.
11. KDHS’ ye verilen hizmet ve yetkilerin başka bir kişi ya da Kuruluşa devredilmesi ancak Yönetmelik hükümleri doğrultusunda gerçekleştirilir.
12. Kimlik kartındaki verilere yetkisiz kişilerce erişimi engelleyecek idari ve teknik tedbirleri almak.
13. Aşağıdaki bilgi ve belgeleri, bu taahhütnamenin eki olarak sunmak.
	1. İletişim Bilgileri: Adı/unvanı ve tüm birimlerine ait iletişim bilgileri (adres, telefon, e-posta adresi, internet adresi),
	2. Ticaret Sicil Gazetesi, vergi levhası, şirketin imza sirküleri, ticaret sicil belgesi ve şirketi temsile yetkili kişi/kişilerin adli sicil kayıtları ve iletişim bilgileri.
	3. KEC Ortak Kriterler (CC) EAL4+ uygunluk sertifikası
	4. KEC TSE uygunluk sertifikası
	5. EKDS Kimlik Doğrulama Sunucusu TSE uygunluk sertifikası
	6. EKDS Politika Sunucusu TSE uygunluk sertifikası
	7. EKDS Rol Sunucusu TSE uygunluk sertifikası
	8. ISO 27001 uyumlu Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgesi (KDHS, KEC yazılım ve EKDS yazılım firmalarına ait)
	9. Kapasite Raporu (KEC donanım, KEC yazılım ve EKDS yazılım üreticisi firmalara ait)
	10. Yerli Malı Belgesi (KEC TSE sertifikasında adı geçen “Cihaz Donanım Üretim Yeri” olan firmaya ait)
	11. Hizmet Yeterlilik Belgesi (KEC yazılımı ve EKDS yazılımı geliştiren firmalara ait)
	12. TS lSO/lEC 15504-7 SPICE Seviye-2 Belgesi veya Eş Değeri (KEC yazılımı ve EKDS yazılımı geliştiren firmalara ait)
	13. Teknoloji Ürün Deneyim Belgesi (KEC yazılımı ve EKDS yazılımı geliştiren firmalara ait)
	14. Kamu Bilişim Yetki Belgesi (KEC yazılımı ve EKDS yazılımı geliştiren firmalara ait)
	15. Yazılım Yetki Belgesi (KEC yazılımı ve EKDS yazılımı geliştiren firmalara ait; 29.06.2022 tarihli ve 31881 sayılı Resmî Gazete’de yayımlanan “Kamu Bilişim Hizmet Alımı Kapsamında Katılımcıların Yetkilendirilmesi Hakkında Yönetmelik” kapsamında)
14. KDHS, KEC ve EKDS ürünlerine ait yukarıdaki tüm sertifika ve belgeleri hizmet süresi boyunca güncel tutmak, gerektiğinde yenilemek ve hizmetlerini daima EKDS Yönetmeliği’ne uygun olarak sunmak.
15. Kurumun isteyeceği, entegrasyon kapsamında belirlenen verileri içeren her türlü istatistiki bilgileri Kurumun belirlediği yöntemlerle Kurum ile paylaşmak.
16. SHS’ ler ve KEC üreticileri ile Kurumca belirlenen şartları taşımak üzere sözleşme ilişkisi kurmak.
17. Yurt çapında 81 il ve ilçelerinde KEC kurulum ve aktivasyon hizmeti sunmak veya alt yüklenici hizmeti satın alınırsa alt yüklenicinin de veri güvenliği ve gizliliği yükümlülüğünden müştereken ve müteselsilen sorumlu olmak.
18. 7x24 çağrı hizmeti sunmak ve/veya bir altyükleniciden hizmet almak. Alt yüklenici hizmeti satın alınırsa hizmetin aksamasından müştereken ve müteselsilen sorumlu olmak.
19. Yurt çapında 81 il ve ilçelerinde yerinde saha destek hizmeti sunmak ve/veya altyüklenici hizmeti almak. Alt yüklenici hizmeti satın alınırsa hizmetin aksamasından müştereken ve müteselsilen sorumlu olmak.
20. Anlaşma süresince KEC onarım ve bakım hizmeti sunmak.
21. KEC yönetimini ve güncellemelerini zamanında sağlamak.
22. KEC’ lerin bağlantı sağladığı IP numarasını doğrulama bildirimi esnasında Kuruma bildirmek.
23. KDHS’ de uygulanan güvenlik ilkeleri, sistemin teknik ve idari işleyişi, iş süreçleri, süreç içindeki görev ve sorumlulukları konusunda personeline gerekli eğitimleri vermek
24. İş bu taahhütname ve ekleri ile hüküm altına alınarak imzalanan ve pilot uygulama sonrasında güncellenecek olan taahhütname hükümlerine uymak.

# FİZİKSEL ERİŞİM ve GÜVENLİK TEDBİRLERİ

1. EKDS’ nin çalıştığı veri merkezindeki sunucular ve diğer çevre birimlerinin bulunduğu binalar ve odaların, tüm giriş ve çıkışlarının kontrol edildiği, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri almak.
2. KDHS’ nin kurulduğu yer ve binada güç birimleri, haberleşme birimleri, havalandırıcılar, yangın söndürücüler bulundurmak, yangın, deprem, su baskını ve afetlere karşı gerekli tedbirleri almak.
3. Binaya girişleri güvenlik görevlilerinin kontrolü altında ve gelişmiş erişim kontrol cihazlarıyla sağlamak.
4. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişlerini özel erişim talimatları uyarınca yapmak ve gerekli tedbirleri almak.
5. KDHS işlevlerini sorunsuz bir şekilde yerine getirilmesi için destek birimleri ve gerekli olan güç kaynaklarını bulundurmak ve hizmetin sürekliliği için kullanmak,
6. Kullanılan veri saklama ortamlarını bozulmaya ve yıpranmaya karşı fiziksel ve elektronik olarak korumak.
7. Sistemin sürekliliğini sağlayabilmek amacıyla gerekli görülen bileşenleri güvenli bir şekilde yedeklemek.

# KEC’LER İÇİN YÜKÜMLÜLÜKLER

1. KEC’ lerin TSE standartlarında geçen Tip-2 ve Tip-3 desteğini sağlamasını, ilgili Tip-2 ve Tip-3 sertifikalarına sahip olmasını sağlamak.
2. KEC terminalinin dışardan gelebilecek her türlü yazılımsal müdahale ve ataklara karşı güvenli olmasını sağlamak
3. Başarısız doğrulama işlemlerini de KDHS ile paylaşmak.
4. Doğrulama işlemleri sırasında bilgi paylaşımını Kurumun belirlediği yöntemlerle yapmak.
5. Kurum isterleri gereği KEC üzerinden hastane tesis kodu girilebilmesini sağlamak.
6. KEC’ lerin minimum 8 (sekiz) yıllık GEM kartlar ile ilklendirilmiş olmasını sağlamak.
7. KEC’ lerin ethernet, Wi-Fi ve GSM desteği olmasını sağlamak.
8. KEC’ lerde mobil iletişim için M2M SIM kartların takılı olarak gelmesini ve özel APN üzerinden güvenli olarak çalışır olmasını sağlamak. KDHS firması adına kayıtlı M2M Sim kartları ve APN hizmetlerini kullanmak.
9. KEC’ lerin 2 (iki) yıl üretici garantisi kapsamında olmasını sağlamak.
10. Vatandaşlara T.C. Kimlik Kartları NVİGM tarafından teslim edilirken ön tanımlı olarak kartların içeriğinde bulunan “kişisel mesajın” ve “PIN bilgisinin” değiştirilmesi işlemlerinin KEC tarafından desteklenmesini sağlamak.
11. KEC’ lerde “secure-boot” özelliği bulunmasını sağlamak.
12. KEC’ lerin tamper korumasının (dışarıdan müdahaleye karşı önlem) Ortak Kriterlere (CC) uygun olmasını sağlamak.
13. KEC yazılımlarının güncel sürümler ile işletilmesini sağlamak

# AĞ GÜVENLİĞİ DENETİMLERİ

1. Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği denetimlerini yapmak veya yaptırmak.
2. Sistemin dışa açık ağ bağlantısında güvenlik duvarı kullanmak.
3. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi sunucuları kurmak.
4. İnternet üzerinden giden tüm trafik şifreli olacaktır.
5. TSE onaylı Sızma Testi Firmalarından biri ile tüm sistem 6 ayda bir test edilip, sonuçları Kuruma sunulacaktır.

# UYGUNLUK DENETİMLERİ

1. KDHS, mevzuat gereği NVİGM tarafından incelenir/denetlenir.
2. KDHS’ nin denetim kapsamı NVİGM tarafından belirlenir.
3. Kurum, ilgili birimleri vasıtasıyla KDHS’ nin faaliyetlerinin yukarıdaki taahhütler uyarınca yürütüldüğünü temin etmek üzere yerinde denetimler gerçekleştirebilir; faaliyete ilgili işbu taahhütname uyarınca ek bilgi ve belge isteyebilir.
	1. KEC ilklendirme odası (GEM kartların takıldığı ve ilk cihaz yazılımlarının yüklendiği) Kurum denetimine açık tutulur.
	2. KDHS servislerinin (EKDS yazılımları dahil) çalıştığı ve yönetildiği ortam Kurum denetimine açık tutulur.
4. KDHS, ISO/IEC 27001 bilgi güvenliği yönetim standardına uygun olarak hizmet verir ve standart gereği düzenli olarak iç ve dış denetimlere tabi tutulur.
5. KDHS, EKDS kapsamında kullanılmak üzere TSE’den almış olduğu uygunluk sertifikalarının ve Ortak Kriterler sertifikasının son geçerlilik tarihlerini takip etmek ve mevcut belgelerin geçerliliği bitmeden ilgili belgeleri yenileyerek Kuruma bildirmekle yükümlüdür. Kurum uygunluk belgelerini inceleyebilir ve denetleyebilir.

Elektronik kimlik doğrulama sistemi ve güvenli kart erişim cihazı çözümleri ile Kuruma biyometrik kimlik doğrulama sistemi dahilinde hizmet sunacağımızı, bu hizmeti sunarken;

Yukarıda beş ana başlıkta altında ve alt maddelerinde belirtilen tüm yükümlülükleri eksiksiz yerine getireceğimizi, bu konularda mevcut 6698 sayılı Kişisel Verilerin Korunması Kanunu ile diğer alakalı tüm mer’i mevzuat kapsamında iş ve işlemleri yürüteceğimizi, iş bu taahhütname ve eklerinde bulunan hükümlerine veya yasal mevzuata uymadığımız takdirde her türlü cezai ve hukuki sorumluluğun tarafımıza ait olduğunu, biyometrik EKDS doğrulaması nedeniyle firmamızın kusurundan kaynaklanan Sosyal Güvenlik Kurumu zararlarını derhal ve defaten karşılayacağımızı, Kurumun bu taahhütname ile belirlenen kimlik doğrulama sisteminden her zaman tek taraflı ve neden belirtmeksizin vazgeçebileceğini bu sebeple Kurumun bir sorumluluğu bulunmadığını, SHS lerin bu sebeple veya EKDS, KDHS kullanımı dolayısıyla uğrayacağı bir zarar olursa bu zararların da tarafımızca karşılanacağını Kurumun bu konuda bir sorumluluğunun bulunmadığını ayrıca kabul ve taahhüt ederiz.

**EK:** Diğer Hususlar