GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

Bilgi Güvenliği Süreçlerinde Denetim Standartları

Giriş ve Gelişmeler

6 Temmuz 2019 tarihinde yayımlanarak yürürlüğe giren Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi ("Genelge") ile kamu kurumları ve kritik altyapı hizmetleri veren işletmeler bakımından bilginin dijitalleşme sürecinde meydana gelebilecek ciddi güvenlik risklerinin azaltılması ve etkisiz kılınması ile özellikle kritik türdeki verilerin güvenliğinin sağlanması amaçlanmıştı.

Genelge'nin ve Genelge'de belirtilen ilgili tedbirlerin uygulama şeklini ortaya koymak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ("DDO") tarafından Bilgi ve İletişim Güvenliği Rehberi ("Güvenlik Rehberi") de hazırlanmış ve güvenlik standarları Güvenlik Rehberi'nde düzenlenmişti. Genelge ve Güvenlik Rehberi'ne ilişkin değerlendirmelerimizi ve uygulanabilecek yaptırımları, "Verilerin Türkiye'de Depolanması Yönünde Gelişmeler" isimli makalemizde bulabilirsiniz.

Genelge, ayrıca Genelge'ye tabi kurum ve kuruluşların, Güvenlik Rehberi'nin uygulanmasına ilişkin denetim mekanizmalarını oluşturmasını ve yılda en az bir defa uygulamayı denetleyemesini, denetim sonuçlan ile yapılan düzeltici ve önleyici faaliyetlerin Güvenlik Rehberi'nde belirtilen usul ve esaslara göre bir rapor halinde DDO'ya bildirilmesini düzenlemekteydi. İlgili denetim faaliyetlerinin DDO tarafından hazırlanacak Bilgi ve İletişim Güvenliği Denetim Rehberi'ne ("Denetim Rehberi") göre yapılması gerektiği vurgulanmakla birlikte Denetim Rehberi, Güvenlik Rehberi ile birlikte yayınlanmamıştı.

DDO tarafından hazırlanan ve denetimin planlanması, denetim prosedürlerinin uygulanması ve denetim sonuçlarının raporlanması hususlarını düzenleyen Denetim Rehberi de 27 Ekim 2021 tarihinde yayınlandı. Ayrıca Denetim Rehberi ile birlikte denetçilerin sertifikasyonunu ve firmaların belgelendirmesini sağlamak amacıyla DDO nezdinde TSE ve TÜBİTAK BİLGEM iş birliğiyle bir belgelendirme programının ("Belgelendirme Programı") da hayata geçirildiği DDO tarafından duyurulmuştur.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

İlgili kurum ve kuruluşların, Güvenlik Rehberi'nde belirtilen çalışmaların planlanması, uygulanması, değişikliklerin yönetilebilmesi, kontrol edilebilmesi ve önlem alma süreçlerinin bir parçası olarak, yılda en az bir kez olmak üzere, bilgi güvenliği süreçlerine ilişkin bir denetim planlaması ve gerçekleştirmesi gerekmektedir. Söz konusu denetimin Denetim Rehberi'nde belirtilen hususlara uygun şekilde gerçekleştirilmesi esastır.

Denetim Rehberi'nin Kapsamındaki Kişiler

Genelge ve Güvenlik Rehberi'nde de düzenlendiği üzere Denetim Rehberi de kamu kurum ve kuruluşları bakımından geçerli olacaktır. Öte yandan, her ne kadar Genelge'nin denetime ilişkin yükümlülüklerini düzenleyen kısmında sadece kurum ve kuruluşlardan bahsediliyor olsa da, Denetim Rehberi'nin kritik altyapı niteliğinde hizmet veren işletmeler bakımından da önemli olduğu açıktır. Denetim Rehberi'nin kritik altyapı niteliğinde hizmet veren işletmeleri de kapsadığını söyleyebiliriz. Yine de Denetim Rehberi'ne ilişkin yayınlanması öngörülen Sıkça Sorulan Sorular dokümantasyonunun bu hususa bir açıklık getirmesini de bekliyoruz.

Denetim Rehberi de her ne kadar Genelge ve Güvenlik Rehberi'nde olduğu gibi kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelere yönelik olsa da özellikle bu kişilere getirilen yükümlülüklerin etkisi, bu kurum ve işletmelere hizmet veren özel hukuk tüzel kişilerini de ilgilendirmektedir. Dolayısıyla, Denetim Rehberi'nin de kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin tedarikçileri ve iş ortakları açısından da dolaylı olarak uygulanabileceğini belirtebiliriz.

Denetim Rehberi'nin Getirdiği Düzenlemeler

Denetim Rehberi, amacın ve yapının düzenlendiği giriş bölümü hariç olmak üzere 3 esas bölümden oluşmaktadır:

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

a. Denetim Çalışmalarına Hazırlık

Güvenlik Rehberi, 27 Temmuz 2020 itibarıyla çeşitli aşamalardan oluşan 24 aylık bir uyum süresi düzenlemekteydi. Bu kapsamda, Denetim Rehberi'nin kapsamında bulunan kişilerin ilk yıllık denetimleri için hazırlık faaliyetlerine en geç 27 Temmuz 2022 tarihinde başlaması gerekmektedir.

Denetim Rehberi, denetim faaliyetlerinin öncelikle kurumların iç denetçiler tarafından gerçekleştirilmesini esas almakla birlikte özellikle kritik altyapı hizmeti veren işletmeler bakımından ise bu işletmelerin düzenleyici ve denetleyici kurumların ilgili mevzuatlarının da denetim faaliyetleri için dikkate alınması gerektiği belirtilmiştir.

Ayrıca kritik altyapı hizmeti veren işletmeler ile iç denetim birimi bulunmayan kurum ve kuruluşların, dışarıdan denetim hizmeti alma yoluyla denetim faaliyetlerini gerçekleştirmeleri halinde kurumların ve denetçilerin tüm yükümlülükleri detaylı olarak Denetim Rehberi'nde açıklanmıştır.

Dışarıdan hizmet alınarak gerçekleştirilecek denetim faaliyetlerinde denetim hizmet alım sözleşmelerinde uyulması gereken yükümlülükler de özel olarak düzenlenmektedir. Bu çerçevede özellikle aşağıdaki hususlar, denetim firmasının belirlenmesi sürecinde denetim kapsamındaki kişiler açısından dikkate alınmalıdır:

- Denetim hizmetinin alınacağı firma Belgelendirme Programı kapsamında yetkilendirilmiş olmalıdır;
- Denetim hizmeti sunacak firma, son 2 yıl içerisinde denetime konu kurumlara Güvenlik Rehberi'ne uyumla ilgili danışmalık hizmeti vermemiş olmalıdır;
- Bir firmadan en çok 3 yıl art arda denetim hizmeti alınabilir;
- Denetim firması ile imzalanacak sözleşme Denetim Rehberi'nde düzenlenen hususları açıkça düzenlemelidir;
- Denetim firması ve personeli gizlilik yükümlülüğüne tabi olacaktır, bu kapsamda denetim firması ile denetim kapsamında yer alan süreç, altyapı ve uygulamalara yönelik elektronik ve fiziksel ortamda yapılan

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

tüm çalışmalar hakkında tam ve doğru bilgi paylaşılmalıdır (bu husus aynı zamanda denetime hazır olmak için ilgili bilgilerin sistematik olarak düzenlenmesini gerektirmektedir) ve gerekli personel kaynağı da denetime destek olmak adına kurum nezdinde sağlanmalıdır;

- Denetimler fiziki olarak çalışma merkezlerinde de gerçekleştirilebilecektir.

b. Denetim Metodolojisi

Denetim Rehberi, denetimin temel hedefinin Güvenlik Rehberi'nin uygulanma sürecinin etkinliği ve varlık gruplarına uygulanan tedbirlerin etkinliğinin ölçülmesi olduğunu vurgulamaktadır. Denetime ilişkin sorumlulukların ilgili kurumlarda kimlere ait olacağı hususu da Denetim Rehberi'nde düzenlenmektedir.

Denetim 3 temel aşamada gerçekleşmelidir:

1. Denetimin Planlanması

- Denetim ekibinin belirlenmesi: Ekip en az iki denetçiden oluşmalıdır. Denetçilerin çeşitli ihtimallere göre taşıması gereken vasıflar, benimsemesi gereken etik ilkeler ve seçimleri sırasında dikkat edilmesi gereken hususlar Denetim Rehberi'nde detaylı bir şekilde açıklanmıştır.
- Kurumun anlaşılması: Denetim ekibinin kurumun yapısını anlamaya yönelik gerçekleştirdiği bilgi toplama faaliyetleri düzenlenmiştir. Denetim ekibi bu kapsamda kurumun organizasyon yapısını, iş süreçlerini, önceki döneme ait denetim raporlarını, kurumun bilişim faaliyetlerinde üçüncü taraflardan aldığı hizmetlerin kapsamını, kurumun mevzuattan kaynaklanan yükümlülüklerini, varlık gruplarını incelemelidir.
- Denetim kapsamının belirlenmesi (denetim kapsamındaki varlık gruplarının tespit edilmesi): Denetim ekibi bu belirlemeyi yaparken risk odaklı bir yaklaşım benimsemeli, önemlilik kriterini göz önünde bulundurmalıdır. Denetim ekibi, denetim sonucu

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

ortaya çıkacak durumların kurumun bilgi ve iletişim güvenliğine yansıyacak olası sonuçları ile ilgili bir risk denetimi yapar.

- Denetim stratejisi ve denetim programının hazırlanması: Denetim ekibi, etkinlik değerlendirmelerini nasıl gerçekleştireceğini ele alan denetim stratejisini belirlemelidir. Devamında denetimin ana hedefleri olan Güvenlik Rehberi'nin uygulama sürecinin ve varlık gruplarına uygulanan tedbirlerin etkinliğini değerlendirmek amacıyla gerçekleştirilecek çalışmaların belirli bir program dâhilinde yürütülmesi için denetim programı oluşturulmalıdır.

2. Denetim Prosedürlerinin Uygulanması

-
- Denetim yöntemleri: Hangi denetim yöntemlerinin uygulanacağı belirlenmelidir. Mülakat, gözden geçirme, güvenlik denetimi, sızma testi ve kaynak kod analizinden oluşan denetim yöntemleri uygulanabilecektir. Belirlenecek denetim yöntemi, ilgili güvenlik tedbirinin uygulanma biçimine ve güvenlik tedbirinin uygulandığı varlığa uygun şekilde seçilmelidir.
- Denetim kanıtlarının toplanması: Denetim kanıtı denetim süresinde elde edilen tüm bilgi ve belgelerdir. Denetçi, denetim kanıtı toplarken önceki dönem denetim raporu ve bulgularından faydalanabilir. Denetim kanıtında güvenilirlik, uygunluk, yeterlilik ve tekrar edilebilirlik unsurlarının bulunması gerekmektedir. Denetçi topladığı denetim kanıtlarını ilgili olduğu çalışma formuna referans olarak göstermelidir.
- Güvenlik Rehberi'nin uygulama sürecinin ve Güvenlik Rehberi kapsamında uygulanan tedbirlerin etkinliğinin değerlendirilmesi: Denetçi, genel olarak Güvenlik Rehberi'nin uygulama sürecinin ve varlık gruplarına uygulanan tedbirlerin etkinliğini değerlendirir. Bu değerlendirmeyi yapılması için kullanılacak bazı denetim soruları da denetçinin etkinlik değerlendirme çalışmalarına yardımcı olmak için Denetim Rehberi'nin eklerinde genel bir çerçeve ve örnek olarak ilgililerin dikkatine sunulmuştur. Denetçi tedbirlerin etkin olup olmadığına karar verirken çalışmalarını, ilgili kurumun uyumu

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

açısından verimli ve nitelikli bir bilgi sağlama potansiyeli olan belirli bir örneklem üzerinden gerçekleştirecektir.

- Bulguların tespiti, değerlendirilmesi ve izlenmesi: Denetçi, denetim sonucunda denetlenen ilgili kurumun bilgi güvenliğinde meydana gelebilecek risklerin değerlendirilmesi sonucu bir bulguya ulaşacaktır. Denetçi bulgularını Güvenlik Rehberi'nde yer alan bulgu kritiklik seviyesi tablosunda yer alan bulgunun sebep olabileceği güvenlik riskinin meydana gelme olasılığı ve etkilerini düzenleyen açıklamalardan faydalanarak, eksiklikleri ve bu eksikliklerin yaratabileceği riskleri de değerlendirerek, kritiklik düzeylerine göre bir sınıflandırmaya tabi tutacaktır. Tespit edilen bulgular, öncelikle bulguların isabetli olup olmadığını değerlendirmek amacıyla denetim kapsamındaki birim sorumluları ve/veya yöneticileri arasında yapılacak bir toplantıda değerlendirilecektir.Tespit edilen bulguların değerlendirilmesinden sonra bu bulguların izlenmesi aşamasına geçilecektir. Bu aşamada, özellikle kritiklik derecesi yüksekten düşüğe doğru olacak şekilde bulguları ortadan kaldırmak ya da kritiklik derecesini düşürmek için düzeltici ve önleyici faaliyetlerin belirlenmesi, planlanması ve bu faaliyetleri gerçekleştirecek ekiplerin oluşturulması gerekecektir.

3. Denetim Sonuçlarının Raporlanması (Denetim Raporunun Hazırlanması)

- Denetimi gerçekleştiren ekibin görüş oluşturması için gerekli olan bilgi, belge ve evrak tam ise ve denetimin sağlıklı şekilde yapıldığı düşünülüyorsa, ilgili ekipçe denetim raporu hazırlanır. Denetim raporu gizli bilgi niteliğinde olacaktır.

c. Denetim Sonuçlarının DDO'ya Gönderilmesi

Genelge'de de düzenlendiği üzere denetim raporları, DDO'ya da gönderilecektir. DDO, raporların paylaşılması için bir sistem oluşturacak ve denetim raporlarının denetim tarihinden itibaren 2 ay içerisinde yüklenmesi gerekmektedir.

GÜN + PARTNERS
AVUKATLIK BÜROSU

Kore Şehitleri Cad. 17
Zincirlikuyu 34394
İstanbul, Turkey

T: +90 (212) 354 00 00
F: +90 (212) 274 20 95
E: gun@gun.av.tr

www.gun.av.tr

Denetim çalışmaları herhangi bir nedenle yapılamadıysa bu durumun 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kapsamındaki kamu kurum ve kuruluşları için ilgili kanun kapsamında belirlenen üst yöneticiler tarafından ve Denetim Rehberi'nin kapsamındaki diğer kişiler için ise bilgi işlem biriminden sorumlu olan en üst yönetici tarafından DDO'ya gerekçeli bir biçimde açıklanması gerekmektedir. DDO bu mekanizma içerisinde denetim sonuçlarını incelemekte ve mevzuat kapsamında bir gözetleyici rol üstlenmektedir.

Beklenen Gelişmeler ve Sonuç

Denetime ilişkin olarak hazırlık çalışmalarının en kısa süre içerisinde başlanması gerekecektir. Güvenlik Rehberi'nin uyum süreci 27 Temmuz 2022'de sona ereceği için ilk denetim raporunun da bu tarihten sonra hazırlanması uygun olacaktır ve en geç 2022 yılı içerisinde hazırlanması gerekecektir. DDO'nun Denetim Rehberi'ne ilişkin muğlak hususlara ilişkin yakın zamanda bir 'Sıkça Sorulan Sorular' belgesi de yayınlaması bekleniyor.

Sürecin kurumlar ve kritik altyapı hizmeti veren işletmeler bakımından yakınen takip edilmesi gerekmektedir. Kurumlar ve kritik altyapı hizmeti veren işletmeler bakımından bu düzenlemelere uygun hareket edilmemesinin yaptırımları söz konusu olabilir. Öte yandan, Genelge ile Güvenlilk Rehberi ve Denetim Rehberi'nin özel hukuk kişileri üzerindeki bağlayıcılığının uygulama ve doktrinde hala tartışmalı olduğunu özel olarak vurgulamak isteriz.

Her durumda, Denetim Rehberi'nin Güvenlik Rehberi ile birlikte kural olarak bu mevzuatın kapsamında olmasalar dahi bilgi yönetim sistemi işleten diğer tüm veri sorumluları açısından da referans alınabileceğini düşünüyoruz. Veri güvenliği açısından pek çok bilgi yönetim sistemi sertifikasyon süreci ile uyumlu olan bu düzenlemelerin veri güvenliği açısından yakın bir tarihte Kişisel Verileri Koruma Kurumu bakımından da asgari bir standart olarak kabul edilmesi mümkün.

Atacan Yılmaz'a katkılarından dolayı teşekkür ederiz