Hergüner Bilgen Özeke
Avukatlık Ortaklığı Attorney Partnership

Bilgi Sistemlerinin Yönetimi ve Denetimine İlişkin İki Yeni SPK Tebliği Yürürlüğe Girdi

Sermaye Piyasası Kurulu'nun ("**Kurul**") Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) ("**Yönetim Tebliği**") ve Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2) ("**Denetim Tebliği**") 5 Ocak 2018 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Yönetim Tebliği, kapsamındaki kuruluşların[1] bilgi sistemleri kuruluş ve işletilişine ilişkin hususları düzenlerken, Denetim Tebliği ise bu sistemlerin üçüncü kişi ve kuruluşlar tarafından bağımsız denetimine ilişkin hususları düzenlemektedir. Denetim Tebliği, Yönetim Tebliği kapsamındaki her kuruluş için bağımsız denetim yükümlülüğü öngörmemiş olup, halka açık ortaklıkları denetim zorunluluğunun dışında tutulmuştur.

1. Hangi kuruluşlara yükümlülük getiriliyor?

Yönetim Tebliği uyarınca, halka açık ortaklıklar ve emeklilik yatırım fonlarına ek olarak Borsa İstanbul A.Ş. ve portföy saklayıcısı kuruluşları da içerecek şekilde tüm sermaye piyasası kurumları ve diğer birtakım kurum, kuruluş ve ortaklıklar[2] bilgi sistemleri yönetimine ilişkin yükümlülüklerin kapsamına dâhil edilmiştir.

Tebliğler kapsamında sayılan banka ve sigorta şirketleri[3] ile finansal kiralama, faktöring ve finansman şirketlerinin[4] bilgi sistemlerinin hali hazırda kendi mevzuatları uyarınca bilgi sistemlerine ilişkin özel düzenlemeler tabi oldukları dikkate alınarak, bu kurumların kendi mevzuatlarındaki yükümlülüklere uyumunun Yönetim Tebliği'nde öngörülen yükümlülüklerin yerine getirilmesi hükmünde olduğu belirtilmiştir.

2. Tebliğ ne tür yükümlülükler öngörüyor?

Yönetim Tebliği uyarınca kapsam dâhilindeki kurum, kuruluş ve ortaklıkların ana yükümlülükleri genel hatlarıyla aşağıdaki şekilde özetlenebilir:

- Bilgi sistemlerine ilişkin olarak ana iki kategoride politika ve süreç geliştirmek; (i) bilgi sistemleri yönetimi ve (ii) bilgi sistemleri risk ölçüm ve takibi;
- Bilgi sistemlerinin yönetimine yönelik finansman ve insan kaynağı tesis etmek;
- Bilgi sistemleri neticesinde müşteri bilgilerini de içerecek şekilde elde edilen datanın gizliliğini sağlamak; ve
- Finansal ya da operasyonel işlemlerin takip edilmelerini sağlayan bir denetim izi kayıt mekanizmasının tesis edilmesi ve bu mekanizmadan elde edilen kayıtların asgari beş yıl boyunca saklanması.

3. Sistemlerin oluşturulması ve işletilmesinde kimler sorumlu?

Yönetim Tebliği uyarınca, bilgi güvenliği politikasının uygulanması, sistemlerin işletilişinden sorumlu ***üst yönetim*** tarafından gözetilirken, bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesine ilişkin genel sorumluluk ise ***yönetim kurulu***nundadır.

Yönetim Tebliği, üst yönetimi, bilgi sistemlerine ilişkin diğer ikincil yükümlülüklere ek olarak (i) bilgi sistemlerinin kullanımına ilişkin **projelerin** onayı, (ii) bilgi sistemlerine ilişkin süreçlerin yürütülmesinden sorumlu olacak yeterlilikte teknik bilgi ve tecrübeye sahip **bilgi sistemleri güvenliği sorumlusu** tespit edilmesi ve (iii) bilgi sistemleri konusunda öngörülen süreçlerin devamlılığını sağlamak amacıyla **iş sürekliliği planı** hazırlanması hususunda yükümlü kılınmıştır.

4. Yaptırımlar

Yönetim Tebliği ile getirilen yükümlülüklere aykırılık hallerine özgü bir idari ya da cezai yaptırım öngörülmemiştir, bu nedenle Sermaye Piyasası Kanun'undaki genel yaptırım hükümlerinin uygulanması söz konusu olacaktır.

Two New Communiqués of the CMB on the Management and Audit of Information Systems Have Entered into Force

The Capital Markets Board ("**the Board**") issued the Communiqué on the Management of Information Systems (VII-128.9) ("**Management Communiqué**") and the Communiqué on the Independent Auditing of Information Systems (III-62.2) ("**Audit Communiqué**"), which both entered into force following their publication in the Official Gazette on 5 January 2018.

The Management Communiqué regulates the establishment and running of all information systems of all organizations falling within its scope[1], and the Audit Communiqué regulates the inspection of these systems by third parties. The Audit Communiqué does not envisage an independent audit obligation for all institutions falling within the scope of the Management Communiqué, and publicly listed partnerships fall outside the scope of mandatory audits.

1. Which organizations are subject to these obligations?

All capital markets institutions including Borsa İstanbul A.Ş. and its portfolio depository entities; all publicly listed partnerships; all private pension funds; and certain other[2] institutions, organizations, and partnerships fall under the scope of the Management Communiqué.

The information systems of banking and insurance companies[3] mentioned in the Communiqués, as well as those of financial leasing, factoring, and financing companies[4] are already subject to their own similar sectoral regulations, therefore there is a provision stating that the satisfaction of these obligations constitutes satisfaction of the obligations stipulated under the Management Communiqué as well.

2. What obligations are set forth under the communiqué?

The primary obligations for institutions, organizations, and partnerships that fall within the scope of the Management Communiqué can be summarized follows:

- Developing policies and processes in two main categories: (i) information systems management, and (ii) information system risk analysis and follow-up;
- Allocating finances and human resources for information systems management;
- Ensuring the privacy of all data pertaining to information systems, including customer information; and
- Implementing an audit trail mechanism designed to track financial or operational processes and maintaining the records obtained from this mechanism for a minimum of five years.

3. Who is responsible for the establishment and operation of these systems?

The Management Communiqué states that the implementation of data security policies must be monitored by ***senior management*** who is responsible for operations, and that the ***Board of Directors*** has overall responsibility for carrying out effective and sufficient oversight of information systems.

The Management Communiqué states that, in addition to their certain secondary obligations regarding information systems, senior management must (i) obtain ***project consent*** for the use of information systems, (ii) appoint a ***person responsible for the security of information systems*** who has adequate technical knowledge and experience to be responsible for the implementation of processes pertaining to information systems, and (iii) formulate a ***continuity of business plan*** in order to ensure the continuity of the processes for information systems outlined under the Communiqué.

4. Sanctions

The existing general sanctions listed under the Capital Markets Code No. 6362 will likely remain applicable since the Management

[1] Yönetim Tebliği ve Denetim Tebliği'nde yer alan ve burada özetlenen düzenlemelerin bir kısmından, dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları gibi birtakım kurum, kuruluş ve ortaklıklar muaf tutulmuştur.

[2] Tebliğlere tabi kurumlar: Halka açık ortaklıklar, emeklilik yatırım fonları, Borsa İstanbul A.Ş., Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri, İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., Portföy saklayıcısı kuruluşlar, Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş., Sermaye piyasası kurumları, Türkiye Sermaye Piyasaları Birliği ve Türkiye Değerleme Uzmanları Birliği.

[3] 6362 Sayılı Sermaye Piyasası Kanunu'nun 136. maddesi uyarınca.

[4] 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu uyarınca.

Communiqué does not specify particular administrative or criminal penalties that would be applicable for violation of the obligations to manage the information systems.

---

[1] Institutions which fall within the scope of the Communiqués: Publicly listed partnerships, pension investment funds, Borsa İstanbul A.Ş Stock Markets and market operators and other organized markets, İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., Portfolio depository organizations, Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş., capital markets organizations, the Turkish Capital Markets Association and the Turkish Appraisers Association.

[2] Organizations, institutions and partnerships which fall into the scope of the Management and Audit Communiqués such as narrowly authorized intermediary institutions, asset leasing companies, mortgage financing institutions, the Turkish Capital Markets Association, the Turkish Appraisers Association, independent audit, grading and valuation organizations, publicly listed partnerships, asset financing funds, collective investment entities, private pension funds and housing finance funds have been held partly exempt from the provisions summarized here.

[3] Pursuant to Article 136 of the Capital Markets Code numbered 6362.

[4] Pursuant to the Financial Leasing, Factoring and Financing Companies Code numbered 6361.

Daha fazla bilgi ve sorularınız için:

Kayra Üçer: (kucer@herguner.av.tr)
Emel Tulun: (etulun@herguner.av.tr)

Büyükdere Caddesi 199, Levent 34394 ISTANBUL
Telefon: (90) 212 310 18 00 Fax: (90) 212 310 18 99

http://www.herguner.av.tr

For further information please contact:

Kayra Üçer: (kucer@herguner.av.tr)
Emel Tulun: (etulun@herguner.av.tr)

Büyükdere Caddesi 199, Levent 34394 ISTANBUL
Telephone: (90) 212 310 18 00 Fax: (90) 212 310 18 99

http://www.herguner.av.tr