13 Temmuz 2014 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği ("Yönetmelik") ile 20 Temmuz 2008 tarihli ve 26942 sayılı Resmi Gazete'de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliği yürürlükten kaldırılmıştır. Yönetmelik ile şebeke ve bilgi güvenliğinin sağlanmasına yönelik olarak yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketlerin, bir başka deyişle, işletmecilerin uyacakları usul ve esaslar oldukça ayrıntılı bir şekilde ve yürürlükten kalkan yönetmelikten farklı bir şekilde düzenlenmektedir. Bununla birlikte, Yönetmelik kişisel verilerin işlenmesi ve gizliliğinin korunmasını kapsamamaktadır. Bilindiği gibi, Kişisel Verilerin Korunması Kanunu henüz tasarı aşamasında olup yasalaşmamıştır.

Yönetmelik ile elektronik haberleşme sektöründe özellikle son yıllarda artış gösteren ve giderek daha büyük tehlike arz eden siber saldırı ve zararlı yazılımların önlenmesi amacıyla işletmelere yeni zorunluluklar getirildiği görülmektedir. Bu çerçevede, şebeke ve bilgi güvenliğinin sağlanmasının yanısıra tüketici haklarının korunması, hizmet kalitesinin yükseltilmesi ve güvenlik ile kullanılabilirlik arasında denge kurulması gibi ilkelerin de gözetildiğini söylemek mümkündür.

Yönetmelik ile düzenlenen önemli hususlar aşağıda dikkatinize sunulmaktadır:

i. İşletmecilerin Yükümlülükleri: Yönetmelik ile işletmeciler arasında tabi oldukları yükümlülükler bakımından bir ayrım yapılmaktadır. Buna göre, tüm işletmeciler Yönetmelik çerçevesinde düzenlenen şebeke ve bilgi güvenliğinin sağlanmasına ilişkin temel yükümlülüklere uymak durumundadır. Ancak, Yönetmelikte sıralanan yetkilendirme tiplerine sahip işletmecilerden yıllık net satışları Bilgi Teknolojileri ve İletişim Kurulu ("Kurul") Kararı ile belirlenen değer ve üzerinde olanlar söz konusu temel yükümlülüklerin yanısıra Yönetmelik hükümleri kapsamında çeşitli ilave tedbirleri almakla da yükümlüdür. Anılan yetkilendirme tipleri şunlardır: a) altyapı işletmeciliği hizmeti; b) çeşitli telekomünikasyon hizmetleri (imtiyaz sözleşmesi); c) GMPCS mobil telefon hizmeti; ç) GSM/IMT-2000/UMTS (imtiyaz

The Regulation on the Network and Data Security in the Electronic Communication Sector ("the Regulation") entered into force through its publication in the Official Gazette on 13 July 2014 and replaced the Regulation on Electronic Communication Security, which was published in the Official Gazette numbered 26942 on 20 July 2008. The Regulation diffentiates itself from the previous regulation in many aspects and provides a far more detailed account of the procedures and principles for network and data security that are to be followed by electronic communication service providers and/or those who provide electronic communication network and operate electronic communication infrastructure, in other words, operators, in accordance with their authorisations. That said, the Regulation does not include personal data processing and protection. As is known, the Law on the Protection of Personal Data remains to be a draft bill until the Turkish Parliament passes it.

It is seen that the Regulation introduced a new set of obligations for the operators in order to prevent cyber attacks and malicious software that seem to have increased in number and the scope of threat that they pose in the electronic communication sector. In this respect, it might be added that in addition to ensuring network and data security principles such as the protection of consumer, improving service quality and maintaining a balance between security and usability have also been taken into account.

Important matters included in the Regulation are summarised for your information as follows:

i. Obligations of the Operators: The Regulation makes a distinction between the operators in terms of the obligations that they are subject to. Accordingly, all operators are obliged to fulfil the basic requirements for network and data security as provided by the Regulation. However, operators who are the bearer of certain authorisation types as listed under the Regulation and whose net annual sales are equal to and over the amount that is determined by a Information and Communication Technologies Board ("Board") Decision are required to fulfil the additional obligations as well as the basic requirements. The said authorisation types are as follows: a) infrastructure operator service; b) various telecommunication services (concession agreement); c) GMPCS mobile telephone service; d) GSM/IMT-2000/UMTS (concession agreement); e) GSM

sözleşmesi); d) hava taşıtlarında GSM 1800 mobil telefon hizmeti; e) internet servis sağlayıcılığı; f) sabit telefon hizmeti; g) sanal mobil şebeke hizmeti; ğ) uydu haberleşme hizmeti; h) uydu ve kablo tv hizmetleri (görev sözleşmesi).

ii. Bilgi Güvenliği Yönetim Sistemi: Tüm işletmecilerin tabi olduğu temel yükümlülüklerin başında yetkilendirmelerine ilişkin tüm hizmetleri ve kritik sistemleri kapsayıcı bir bilgi güvenliği yönetim sistemi ("BGYS") kurulması gelmektedir. BGYS, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, işletmecinin yönetimi tarafından kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü ifade etmektedir. İşletmeci, BGYS'nin kurulması, uygulanması ve sürekliliğinin sağlanması amacıyla bir yönetim mekanizması işletmekle ve ayrıca yönetimi tarafından onaylanmış bir BGYS politikası tanımlamak, dokümante etmek, tüm çalışanlarının ve ilgili tarafların söz konusu politikaya ilişkin farkındalığını sağlamakla da yükümlü tutulmaktadır. BGYS politikasının ihtiva etmesi gereken asgari unsurlar da Yönetmelik tarafından tanımlanmaktadır. Ayrıca işletmecinin BGYS politikasına aykırı ve lisansız yazılım kullanımına izin veremeyeceği de belirtilmektedir.

iii. Risk Değerlendirmesi: Tüm işletmeciler bakımından öngörülen bir başka temel yükümlülük ise, risk değerlendirme ve işlemedir. Yönetmelik hükümleri uyarınca, işletmecinin bilgi güvenliğine ilişkin tehditlerin tanımlanmasını, söz konusu tehditlerin gerçekleşme olasılıklarını ve oluşturabilecekleri olumsuz sonuçları niteleyen ve risklerin sınıflandırmasını içerecek şekilde yılda en az bir defa risk değerlendirmesi yapması gerekmektedir. Değerlendirme sonucunda tüm riskler için Yönetmelik çerçevesinde bir risk işleme kararı alınması ve gerek risk değerlendirme gerekse işlemeye ilişkin metotların dokümante edilmesi ve bunlara göre yapılan işlemlerin kayıt altına alınması da gerekmektedir.

iv. Aboneye Yönelik Tedbirler: Temel yükümlülükler kapsamında getirilen düzenlemelerin bir kısmını aboneye yönelik tedbirler oluşturmaktadır. Buna göre, işletmeci kendisine tahsisli bir IP adresi kullanılarak şebekesine dışarıdan paket

1800 mobile telephone service in aircrafts; f) internet service providers; g) fixed telephone service; h) mobile virtual network service; i) satellite communication service; j) satellite and cable tv services (service contract).

ii. Data Security Management System: Foremost among the basic requirements that all operators are required to fulfil is the establishment of a data security management system ("BGYS") that covers all services and critical systems within the scope of their authorisation. BGYS stands for the totality of activities that are systematic, rule-based, planned, manageable, sustainable, documented and accepted by the management of the operator and which takes the international security standards as their basis in order to maintain the confidentiality, entirety and accessibility of data. In order to establish, implement and maintain the BGYS the operator is required to run a management mechanism and also identify and document a BGYS policy that has been approved by its management and raise awareness of the policy with all of its employees and related parties. The Regulation also provides the minimum requirements of the BGYS policy. Furthermore, it is stated the operator shall not be allowed to permit the use of software that is against its BGYS policy and unlicensed.

iii. Risk Assessment: Another obligation that has been bestowed upon all operators is risk assessment and processing. According the provisions of the Regulation, the operators are required to undertake a risk assessment that describes the risks concerning data security, the possibility of materialisation of such risks and the negative impact that they may create and also includes a categorisation of the risks at least once a year. Upon the completion of risk assessment a risk processing decision for all risks as per the Regulation shall be taken and methods utilitised for both risk assessment and processing shall be documented and all acts undertaken in accordance with them shall be recorded.

iv. Measures for Subscribers: Measures for subscribers also constitute a part of the regulations introduced within the scope of basic requirements. Accordingly, the operator is required to take the necessary measures for prevention of packages being sent to its

gönderilmesini ve abonelerinin kendisine atanmamış bir IP adresi kullanarak paket göndermelerini engellemeye yönelik gerekli önlemleri almakla yükümlüdür. Ayrıca, işletmecinin abonelerini bilinçlendirmek ve gerekli önlemlerin alınmasını sağlamak amacıyla zararlı yazılımlar ve muhtemel siber tehditler gibi tehlikeler bakımından da onları bilgilendirmesi gerekmektedir.

v. Kullanıcılara İlişkin Parola Yönetimi: Yönetmelik, işletmecinin kritik sistemlerde kullanılan kullanıcı parolaları ile ilgili olarak uygulayacağı hususları sıralamakla birlikte güvenlik gereksinimlerinin karşılanması şartıyla kullanıcı parolaları yerine biyometrik doğrulama, akıllı kart gibi sistemlerin de kullanılabileceğini düzenlemektedir.

vi. Siber Saldırılara Yönelik Tedbirler: Şebeke ve bilgi güvenliğinin sağlanmasına ilişkin ilave yükümlülüklerin başında siber saldırılara yönelik tedbirler gelmektedir. Yönetmelik uyarınca işletmeciler, bünyelerinde Siber Olaylara Müdahale Ekibi ("SOME") kurmakla ve ulusal siber güvenliğin sağlanmasına ilişkin Ulusal Siber Olaylara Müdahale Merkezi'nin ("USOM") ve Bilgi Teknolojileri ve İletişim Kurumu bünyesinde kurulan sektörel SOME'nin koordinesinde ve belirlediği esaslar çerçevesinde gerekli tedbirleri almakla yükümlüdür. Bu çerçevede, işletmecilerin çeşitli mekanizmalar kurması ve talep edilmesi halinde siber saldırılara karşı koruma hizmeti sunması gerekmektedir. Ayrıca, USOM tarafından bildirilen siber saldırı kaynağının kendi abonesi olması durumunda ilgili abonenin bilgilendirilmesini, başka bir işletmecinin abonesi olması durumunda ise gerekli önlemlerin alınması için ilgili işletmecinin bilgilendirilmesini sağlamaları öngörülmektedir.

Yukarıdaki hususlarda daha ayrıntılı bilgi talep etmeniz durumunda, ofisimizle irtibata geçebileceğinizi ve tarafınıza yardımcı olmaktan mutluluk duyacağımızı belirtmek isteriz.

network from outside through an IP address that has been assigned to it and packages being sent by the subscribers through an IP address that has not been assigned to it. Also, the operator is required to inform its subscribers on dangers such as malicious software and potential cyber threats in order to raise awareness and ensure that necessary measures are taken.

v. Password Management for Subscribers: In addition to defining the matters that will be undertaken by the operator for the user passwords, which are used in critical systems, the Regulation also provides that systems such as biometric verification, smart cards may be used instead of user passwords provided that security requirements have been met.

vi. Measures for Cyber Threats: Measures for cyber threats are one of the primary additional liabilities introduced to ensure network and data security. As per the Regulation, the operators are required to establish a Cyber Incidents Intervention Team ("SOME") within their organisation and take the necessary measures within the scope of the principles as defined by and with the coordination of the Centre for Intervention to National Cyber Incidents ("USOM") and the sectoral SOME, which is set up under the framework of the Information Technology and Communication Authority. Within this framework, the operators are required to set up various mechanisms and provide protection service against cyber threats if and when requested. The operators are also required to ensure that the subscriber is informed in case the source of the cyber threat that has been notified by USOM is their own subscriber or, if it is a subscriber of another operator, the said operator is informed.

We would like to inform you that you may contact our office and we shall be glad to provide assistance, in case you require further information in relation to the matters above.

Ebulula Mardin Caddesi Maya Meridyen Is Merkezi Kat: 5 Akatlar Besiktas 34335 Istanbul Turkey
T +90 212 351 54 55 **F** +90 212 352 70 80 info@akinlawoffice.com www.**akinlawoffice**.com