SİTEPLUS ÖZEL GÜVENLİK HİZMETLERİ A.Ş.

2020

ELEKTRONİK HABERLEŞME VE ELEKTRONİK VERİLERİN DENETLENMESİ HAKKINDA YÖNETMELİK

KVKK_Y5 VERSİYON 1.00

1. AMAÇ VE KAPSAM

1.1. İşbu Yönetmeliğin amacı, Şirket'in elektronik iletişimleri hangi koşullarda ve ne zaman denetleyeceği hususuna ilişkin usul ve esasları belirlemek olup Yönetmelik hükümleri Şirketin elektronik iletişim imkânlarına erişmesine ve/veya kullanmasına izin verilen personel ve üçüncü şahıslar için geçerlidir.

2. ELEKTRONİK HABERLEŞMENİN DENETLENMESİ

2.1. İşbu Yönetmeliğin amaçları bakımından elektronik haberleşme, genel olarak telefon görüşmeleri, faks mesajları, e-postalar, anlık mesajlar, SMS veya diğer kısa mesajlar, tweetler, wiki'ler, bloglar, mesajlaşma platformlarında yayınlanan web içerikleri de dâhil olmak üzere her türlü elektronik mesajdır. Şirketin yürüttüğü işlerin tabiatı gereği personelin veya ziyaretçilerin elektronik iletişimlerinin içeriğinin genel olarak izlenmesi gibi bir sorumluluğu ya da görevi yoktur. Ayrıca, Şirket rutin olarak rastgele örnekleme veya insan müdahalesi yoluyla elektronik haberleşmeler üzerinde genel tarama yapmamaktadır. Bununla birlikte, e-posta trafiğinin otomatik olarak bilgisayar yardımıyla taranması, istenmeyen toplu e-postaları (genellikle "istenmeyen posta-spam" olarak adlandırılır) ve potansiyel olarak zarar verici ileti içeriğini (bilgisayar virüsleri, mali dolandırıcılık girişimleri vb.) engellemek amacıyla sınırlı olarak gerçekleştirilir.

2.2. 5561 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun Erişim sağlayıcının yükümlülükleri başlıklı 6. Maddesi gereği Şirket, kanunda sayılan amaçlarla sınırlı olarak Şirket tarafından alınan ya da gönderilen elektronik haberleşme trafik bilgilerini saklamak, bu bilgilerin doğruluğu, bütünlüğü ve gizliliğini sağlamak için gerekli tedbirleri alacaktır. Bahse konu amaçlara suç teşkil eden ya da izin verilmeyen amaçla için kullanılıp kullanılmadığını kontrol etmek, virüsler, hackleme ve hizmeti engelleme saldırısı (denial of service attack) gibi tehditlere karşı sistemin korunmasına yönelik denetleme ve müdahaleler, bilgi işlem operasyonlarının Şirketin politika ve direktiflerine uygunluğunu temin etmek dâhil ancak bunlarla sınırlı değildir.

2.3. Elektronik haberleşmenin denetlenmesi esas olarak ilgili kişinin rızası alınmak suretiyle yapılacaktır. Bununla birlikte aşağıda sıralanan durumlarda Şirket, meşru amaçlarını gerçekleştirmek için resen denetleme yapma hakkını saklı tutar:

2.3.1. Mali ve ekonomik iş ve işlemlerin güvenliğini sağlamak için ilgili kişiler arasında gerçekleştirilen iletişimin belirli unsurlarını bilmenin gerekli veya arzu edildiği durumlarda işlemlerin ve diğer iletişimlerin kayıtlarının tutulması;

2.3.2. Şirketin idari düzenlemelerine ve şirket içi yönerge ve davranış kurallarının uygulanıp uygulanmadığını kontrol etmek gibi Şirketi ilgilendiren düzenlemeler ve uygulamalara riayet edildiğini teyit etmek için;

2.3.3. Kalite kontrol veya personel eğitimi gibi amaçlar için Şirketin sahip olduğu elektronik bilgi sistemlerini kullanan kişiler tarafından ulaşılması gereken standartları belirlemek veya göstermek amacıyla;

2.3.4. Suç teşkil eden fiillerin önlenmesi veya tespiti için, örneğin yolsuzluk, bilgisayar sistemlerinin kötüye kullanımını veya diğer yasa dışı faaliyetleri tespit etmek için izleme veya kaydetme yapılması.

2.3.5. Elektronik bilgi ve haberleşme sistemlerinin yetkisiz kullanımını önlemek veya tespit etmek için, örneğin, çalışanların Bilgi Güvenliği Politikasında Bölüm 11: "BT Kaynaklarının Kullanım Koşulları (Kabul Edilebilir Kullanım Politikası)" bölümünde zikredilen Şirket düzenlemelerini ihlal etmesini önlemek için;

2.3.6. Virüsleri tespit etmek ve silmek, hackleme veya hizmet reddi saldırıları gibi sisteme yönelik diğer tehditleri kontrol etmek ve durdurmak; ağ içi akışları ve e-posta günlükleri oluşturmak gibi yöntemler vasıtasıyla sistemin etkili bir şekilde çalışmasını temin etmek için;

2.4. Şirketin elektronik haberleşme sistemlerini kullanan kişiler, Şirketin IT hizmetlerinin düzgün çalışmasını sağlamak için zaman zaman Bilgi ve İletişim Teknolojileri Sistem ve Ağ Yöneticilerinin iletimleri izlediğini veya işlem bilgilerini gözlemlediğini bilmelidir. Bu ve benzeri durumlarda, söz konusu personel, istemeden elektronik iletişimin içeriğinden haberdar olabilir. İşbu Yönetmelik veya ilgili mevzuatta aksi belirtilmedikçe, bahse konu görevlilerin Şirket çalışanlarının işlem bilgilerinin içeriğini bilinçli olarak incelemesi veya gördüklerini, duyduklarını veya okuduklarını başka şekillerde kullanmaları yasaktır. Bununla birlikte, Şirket politikaları ve idari düzenlemelerinin veya kanun hükümlerinin ihlal edildiği tespit edilirse, konu hakkında Şirket üst düzey yetkililerine bilgi verilmelidir.

3. ELEKTRONİK VERİLERİN İNCELENMESİ

3.1. Şirketin zaman zaman ağa bağlı olan ya da bağımsız depolama araçlarında muhafaza edilen Şirket kurumsal e-mailleri, yerel, ana ya da grup sürücülerinde bulunan belge ve dosyalar, Şirket sistem veya binasına erişim kayıtlarına ilişkin verileri incelemesi gerekebilir. Bunun yanı sıra Şirket ağına bireysel cihazları ile bağlanan çalışan ve ziyaretçiler Şirketin Bilgi Güvenliği Politikasının Elektronik Haberleşmelerin Denetlenmesi başlıklı 6. Bölümünde belirtilen amaçlarla sınırlı olarak denetlenmesine rıza göstermiş sayılırlar. Bu amaçla yapılan denetimler veri güvenliğinin sağlanması amacı ile sınırlı olup 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda belirtilen esaslara uygun olarak yerine getirilecektir.

3.2. Normal şartlar altında, Şirket e-posta hesapları, ana sürücü veya yerel sürücüler, erişim log kayıtları gibi bireyler tarafından tutulan veya kişilerle ilgili veriler üzerinde herhangi bir inceleme yapılmadan önce kullanıcının rızası alınacaktır. Ancak, aşağıdaki durumlarda kullanıcı izin vermemiş olsa dahi inceleme yapılacaktır:

3.2.1. Kanun tarafından ön görülmüş olması halinde;

3.2.2. Salt dedikodu ya da söylentinin ötesinde güvenilebilir delillerin söz konusu olduğu durumlarda kanun hükümleri veya Şirket politikalarının ihlal edilmiş olabileceğine dair kuvvetli şüphe var ise;

3.2.3. Harekete geçilmediği takdirde ciddi fiziksel zarar, önemli ölçüde mülk kaybı veya hasarı, kanun veya Şirket politika ve idari düzenlemelerinin ihlaline ilişkin önemli kanıtların kaybedilmesi veya Şirket tüzel kişiliği ya da çalışan ve/veya yöneticilerinin belirgin oranda mali yükümlülüklere maruz kalmasının mümkün olduğu zorlayıcı koşullar ve acil durum halleri söz konusu ise;

3.2.4. Harekete geçilmediği takdirde Şirketin idari olarak işleyişi ya da mali sorumluklarını yerine getirme kabiliyetinin ağır zarar görmesi olası ise.

3.3. İlgili kullanıcı, Şirket bina ve tesislerinden başka bir noktada bulunuyor ve kullanıcı tarafından tutulan veya kişilerle ilgili verilerin incelenmesi ticari nedenlerle gerekliyse, öncelikle ilgili kullanıcının onayı alınmalıdır. Kullanıcı ile iletişime geçilemiyorsa, İlgili Daire Başkanı ve Genel Müdür, kullanıcının Şirket işlerinin görülmesi için tahsis edilen bilgisayar veya başka cihazlarında denetim yapılması için yazılı olarak izin verebilir. Bu halde rızanın alınması için alınan tedbirler ve denetim yapılmasını gerektiren gerekçeler bir tutanakla kayıt altına alınacaktır.

3.4. Yukarıda 3.2. bölümde belirtildiği şekilde bir kullanıcı tarafından tutulan veya kişilerle ilgili veriler üzerinde inceleme yapılmasının ilgilinin rızası alınmaksızın yapılmasının zaruri olması halinde aşağıdaki kurallar geçerli olacaktır:

3.4.1. Acil Durumlar: Acil durumun gerektirdiği asgari içerik incelenebilir ve durumun giderilmesi için gerekli asgari tedbirler izin alınmaksızın derhal yapılabilir, ancak acil durum ortadan kalktıktan sonra uygun izin gecikmeden aranmalı ve paragraf 3.3 uyarınca durum kayıt altına alınmalıdır;

3.4.2. Diğer tüm durumlarda İlgili Daire Başkanı ve Genel Müdürün yazılı izni olmadan hareket edilmeyecektir.

3.4.3. Şifrelenen Veriler: Sistem içerisinde yapılacak denetlemede şifrelenmiş verilerin bulunması halinde ilgili şifre kaldırma anahtarı talep üzerine ibraz edilmelidir.

3.4.4. Artık Şirketimiz tarafından istihdam edilmeyen çalışanlar tarafından oluşturulan veya bunlarla ilgili verilerin zilyetliği yasal imha sürelerine ilişkin hükümler saklı kalmak kaydıyla Şirket'e aittir. Bu tür bilgilerin incelenebilmesi için ilişiği kesilmiş olan çalışanın iznini almak gerekli değildir. Bilgileri görüntülemek için yukarıda 3.3. maddede belirtilen usul izlenerek izin alınacaktır.

3.5. İzin verildikten sonra Şirket sistemlerinde bulunan veriler aşağıda belirtildiği şekilde ele alınacaktır:

3.5.1. Şirket ile alakalı materyaller olağan iş pratiklerine göre değerlendirilecek olup gerekli görüldüğü takdirde muhafaza edilecek ya da silineceklerdir.

3.5.2. Kişileri ilgilendiren veriler meşru bir sebep olmadıkça incelenmeyecektir.

3.5.3. Şirket çalışanları ilişikleri kesilmeden önce elektronik belge ve elektronik postalarında yer alan kişisel verilerini silmekten sorumludur.

3.6. Özel Hayatın Gizliliği: İşbu Yönetmelik kapsamında gerçekleştirilen her türlü denetim, özel yaşamın gizliliği hakkı dikkate alınarak yürütülecektir. Kişilerin özel hayatını ilgilendiren materyaller, denetimin amaçları için gereken minimum incelemeye tabi olacaktır. Karşılaşılan ve aramanın amacı ile ilgili olmayan herhangi bir gizli bilgi hiçbir tarafa ifşa edilmeyecek ve gizli kalacaktır. Bununla birlikte, yasa dışı olan veya Şirket politikalarına aykırı olduğu anlaşılan bir materyalin denetimler esnasında bulunması halinde, konu hakkında derhal Genel Müdür bilgilendirilerek talimatları doğrultusunda hareket edilecektir.

Belge Versiyon Tarihçesi

Versiyon/Durum	Yayınlama Tarihi	Açıklamalar
1.0/Onaylandı	…./…./…….	Onaylandı