

ÖNSÖZ

Bilişim teknolojilerinin gelişmesi ve yaygınlaşması, bilginin kendisini ve bilgi ile ilişkili her türlü varlığı çok daha değerli bir noktaya getirmiştir. Gelişen teknolojiyle birlikte internetin neredeyse üretilen her ürüne entegre edilmesiyle kişisel ya da kurumsal bilgiler sadece elektronik ortamda değil, taşınabilir teknolojinin izin verdiği her ortamda yer almaya başlamıştır. Böylece yeni yöntemler ya da mecralar kullanılarak, bilginin çok daha fazla kitleye, daha hızlı ve kolay şekilde ulaşması ve aynı hızla paylaşılması mümkün hale gelmiştir.

Bununla birlikte değeri artan bilginin paylaşılması konusunda bazı sakıncaların olduğu da bir gerçektir. Özellikle izinsiz ya da yetkisiz kişilerle paylaşılmasının ciddi sorunlara yol açabileceği düşünülen bilgi varlıkları göz önüne alındığında, konu, kişisel güvenlikten ulusal güvenliğe kadar geniş bir alanı ilgilendirecek hale gelmektedir. Ayrıca bilgi varlıklarının buldukları fiziki ortamın yanı sıra 'siber uzay' adı verilen ortamda da çeşitli tehditlere maruz kaldığı düşünüldüğünde güvenli bilgi paylaşımı hususunda bir düzenleme yapılması gereği ortaya çıkmıştır.

Bilginin paylaşımına ilişkin bu riskler göz önüne alındığında; bilgi varlıklarının tutulduğu ortamlar, içerdiği bilgiler ve bu bilgilerin değeri, kullanım amacı, kapsamı ve bilmesi gereken kişiler dikkate alınarak gizlilik derecelerine göre bir sınıflandırmaya tabi tutulması gereksinim haline gelmiştir.

Söz konusu gereksinimi karşılamaya yönelik temel düzenlemeyi oluşturan bu kriterde, kişisel, ticari, resmi ve milli kapsamdaki bilgi ve bilgi varlıklarının türleri ortaya konulmakta ve bu varlıklara sadece yetkili kişi ve kurumlar tarafından erişilmesinin temin edilmesine yönelik kullanılacak *gizlilik dereceleri* tanımlanmaktadır.

Kriterde çerçevesi ortaya konulan tanımlamalar, bilgiyi üreten tarafından, bilgi varlıklarına tanımlanan gizlilik derecelerinin verilmesi ve etiketlenmesi; hassas bilgi varlıklarının belirlenmesi, bu varlıklara erişen ve kullanan herkesin bu hassasiyet seviyesinden haberdar olması ve buna göre hareket etmesini sağlayacaktır.

Uluslararası düzeyde kullanılagelen gizlilik derecelendirme sistemlerine bakıldığında, Türkiye ve birçok ülke arasında benzer durumlar bulunmaktadır. Bu gizlilik dereceleri ağırlıklı olarak "ÇOK GİZLİ", "GİZLİ", "ÖZEL", "HİZMETE ÖZEL" ve "TASNİF DIŞI" şeklinde bir sınıflandırmaya tabi tutulmaktadır. Yine bazı ülkelerde bu derecelerin dışında kendi özel ibarelerini kullanacak şekilde düzenlemelerin olduğu da görülmektedir.

Ülkemizde Milli Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi ile milli gizlilik derecesi "ÇOK GİZLİ", "GİZLİ", "ÖZEL" "HİZMETE ÖZEL" olmak üzere 4'lü sınıflandırmaya tabi tutularak "ÖZEL" ve üstü gizlilik derecelerine milli güvenlik kapsamında TEMPEST gibi olağanüstü güvenlik tedbirlerinin uygulanacağı belirtilmiştir. Ayrıca yönerge ile "HİZMETE ÖZEL" milli gizlilik derecesi de dahil olmak üzere gizlilik dereceli bilgilerin belgegeçer (faks) ve elektronik posta ile gönderilmesine de imkan verilmemiştir.

"Kişisel Verilerin Korunması Kanunu" gibi yasal hususlar, güncel teknolojiler ve kullanım alanları ile verilere yönelik siber tehditler göz önüne alındığında bu tür bir düzenlemenin uygulamada önemli bir açılım sağlayacağı değerlendirilmektedir. Oluşturulan "TİCARİ GİZLİ", "TİCARİ ÖZEL", "KİŞİYE GİZLİ" ve "KİŞİYE ÖZEL" yeni gizlilik derecelerinin; yasal, resmi, tıbbi, ticari, tüzel ve kişisel alanlardaki bilgi ve bilgi varlıklarının gizliliğinin karmaşa oluşturmadan belirlenmesinde, anlaşılmasında ve bu derecelere yönelik güvenlik tedbirlerinin oluşturulmasında önemli bir kolaylık sağlayacağı da değerlendirilmektedir.

Milli gizlilik derecesi ile ilgili genel ve özel alanlarda ne tür önlemler alınacağı anılan Yönerge hükümleri gereği belirlenmiştir. Bu kriterde yeni tanımlanan gizlilik dereceleri ile ilgili ise kapsam, ortam, kullanılan teknoloji ile bilgiye nüfuz eden ve edecek taraflar açısından nasıl hareket edilmesi gerektiği bu süreç içinde sonraki aşamalarda değerlendirilecektir ve bu kriterin kapsamı dışındadır. Bu kriterde tüm gizlilik derecelerinin kapsamı ve hassaslığı belirtilmektedir.

Birinci bölümde Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Kriterinin amacı ve kapsamı özetlenmekte, kriterde kullanılan kısaltmalar ve temel kavramların tanımları üçüncü bölümde açıklanmaktadır. Dördüncü bölümde bilgi varlıklarının türlere göre gruplanması bazı örnekleri ile beraber sunulmaktadır. Beşinci bölümde milli gizlilik dereceleri ve yeni tanımlanan gizlilik dereceleri açıklanmaktadır.

Bu kriterin bilgi varlıklarının gizlilik derecelerine göre sınıflandırılmasına önemli bir başlangıç olacağı ve bunun üzerine inşa edilecek bilgi güvenliği yaklaşımlarına temel olacağı düşünülmektedir.

Teknik Çalışma Grubu

Ankara, Mayıs 2016

İçindekiler

| | | |
|----------|---------------------------------------------------------------------------|----------|
| 1 | Giriş | 4 |
| 1.1 | Amaç | 4 |
| 1.2 | Kapsam | 4 |
| 2 | Atıf yapılan standard ve/veya dokümanlar | 4 |
| 3 | Terimler, tarifler ve semboller | 4 |
| 4 | Bilgi Varlıklarının Sınıflandırılması | 5 |
| 5 | Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması | 6 |

Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması

1 Giriş

1.1 Amaç

Kurumlardaki bilgi varlıklarının belirlenmesi, gizlilik derecelerine göre sınıflandırılarak kurumlar arası bilgi paylaşımı esnasında bilginin gizliliğinin güvence altına alınması.

1.2 Kapsam

Bu kriter, kamu kurum/kuruluşları, gerçek ve tüzel kişilere ait olan bilgi varlıklarını kapsar.

2 Atıf yapılan standard ve/veya dokümanlar

Bu kriterde standard ve/veya dokümanlara atıf yapılmaktadır. Bu atıflar metin içerisinde uygun yerlerde belirtilmiş ve aşağıda liste halinde verilmiştir. (*) işaretli olanlar bu kriterin basıldığı tarihte İngilizce metin olarak yayımlanmış olan Türk standardlarıdır.

| No | Türkçe adı | İngilizce adı |
|-----------------------------------------|--------------------------------------------------------------------|---------------------------------------------------|
| 4982 Sayılı Kanun | Bilgi Edinme Hakkı Kanunu | |
| 6698 Sayılı Kanun | Kişisel Verilerin Korunması Kanunu | |
| 5510 Sayılı Kanun | Sosyal Sigortalar Ve Genel Sağlık Sigortası Kanunu | |
| 5502 Sayılı Kanun | Sosyal Güvenlik Kurumu Kanunu | |
| 2937 Sayılı Kanun | Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu | |
| 5411 Sayılı Kanun | Bankacılık Kanunu | |
| MSY 317-2 (C) | Millî Savunma Bakanlığı Savunma Sanayii Güvenliği Yönergesi | |
| 2004/8125 Sayılı Bakanlar Kurulu Kararı | Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik | |
| TS 13298:2015 | Elektronik Belge Ve Arşiv Yönetim Sistemi | Electronic records and archives management system |

3 Terimler, tarifler ve semboller

Belge: Herhangi bir bireysel veya kurumsal fonksiyonun yerine getirilmesi için alınmış ya da fonksiyonun sonucunda üretilmiş, içerik, ilişki ve formatı ile ait olduğu fonksiyon için delil teşkil eden kayıtlı bilgi.

Doküman: Kurumsal faaliyetlerin yerine getirilmesinde üretilen ya da toplanan, henüz belge vasfı kazanmamış her türlü kayıtlı bilgi.

Veri: Bilginin işlenmemiş hali.

Bilgi: Anlamalı hale getirilmiş veri.

Bilgi Varlığı: Gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarının sahip olduğu, işlenebilir, kullanılabilir veya paylaşılabilir değere sahip ve uygun şekilde korunması gereken fiziki veya elektronik her türlü veri.

Gizlilik Derecesi: Bilmesi gereken kişiler dışındakilere açıklanmasının veya verilmesinin millî güvenlik veya kişisel güvenlik açısından sakıncalı görülen bilgi varlığının, ülke menfaatine, gerçek ve tüzel kişiler

ile kamu kurum/kuruluşlarına zarar vermesini önlemek amacıyla önem derecesine göre sınıflandırılması ve adlandırılması.

Kişisel bilgi (veri): Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

İz kaydı (log kaydı): Düşük seviyede (makine diline yakın), sistem ve ağ uygulamalarının çalışma zamanında ürettiği kayıtlar.

İşlem kaydı: Yüksek seviyede (insan diline yakın), kullanıcı ve iş uygulamalarının yaptığı işlere ait ürettiği kayıtlar.

Bilmesi Gereken Kişi: Gizlilik dereceli bir bilgiyi, görev ve yetkisi gereği erişme, işleme, öğrenme, kullanma veya paylaşma sorumluluğu olan kişi.

BDDK: Bankacılık Düzenleme ve Denetleme Kurumu

CD: Compact Disc ("Yoğun Disk" - TDK)

DVD: Digital Video Disc ("Sayısal Görüntü Diski" - TDK)

KEP: Kayıtlı Elektronik Posta

MİT: Milli İstihbarat Teşkilatı

MSB: Milli Savunma Bakanlığı

NATO: North Atlantic Treaty Organization ("Kuzey Atlantik Antlaşması Örgütü")

SGK: Sosyal Güvenlik Kurumu

4 Bilgi Varlıklarının Sınıflandırılması

Bilgi varlıkları, bilginin niteliğine, tutulduğu ortama, saklanmasına, sunulmasına, işlenmesine ya da aktarılmasına ilişkin hususlar göz önünde bulundurularak **6 başlık altında** sınıflandırılır:

1. Fiziksel/Elektronik Bilgi Varlıkları

- Sunucu ve bilgisayarlar (tablet, dizüstü bilgisayar, masaüstü bilgisayar, akıllı telefon, giyilebilir bilgisayar vb.)
- Depolama ortamları (manyetik, optik, sabit disk, harici disk, disket, CD, DVD vb.)
- Haberleşme cihazları (telsiz, telefon, faks (belgegeçer), cep telefonu, sayısal mesaj iletim cihazları vb.)
- Girdi/çıkıtlı cihazları (yazıcı, tarayıcı, çizici, kameralar vb.)
- Basılı veya elektronik doküman/belge (yazışmalar, mektup, e-posta, KEP, tasarım belgeleri, planlar, sözleşmeler, raporlar, ihale dosyaları, kroki, fikri mülkiyet haklarına dair belgeler vb.)
- Sosyal medya paylaşımları

2. Yazılım Bilgi Varlıkları

- Veri tabanları, veri dosyaları
- İz ve işlem kayıtları
- Yazılımlar (sistem, uygulama, geliştirme, kurumsal vb.)
- Yazılım kaynak kodları ve yazılım yan ürünleri (tasarım, algoritma vb.)

3. İnsan

4. Soyut değerler (İtibar, imaj vb.)

5. Hizmetler

- Re'sen sunulan hizmetler (kurumların görev alanına giren ve herhangi bir başvuru gerektirmeyen hizmetler)
- Başvuru ile sunulan hizmetler (talep üzerine karşılanan hizmetler)

6. Projeler

- Kamu ve özel sektör projeleri

5 Bilgi Varlıklarının Gizlilik Derecelerinin Sınıflandırılması

Bilgi varlıkları gizlilik derecelerine göre 8 başlık altında sınıflandırılır:

ÇOK GİZLİ: İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza **hayati derecede** zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından **olağanüstü** sonuçlar doğurabilecek bilgi için kullanılır.

GİZLİ: İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza **büyük zarar** verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgi için kullanılır.

ÖZEL: İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgi için kullanılır.

HİZMETE ÖZEL: İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgi için kullanılır.

TİCARİ GİZLİ: İzinsiz açıklanması durumunda, haksız rekabete yol açabilecek veya aynı konuda hizmet veren diğer firmalara avantaj sağlayabilecek olan bilgi için kullanılır.

TİCARİ ÖZEL: İçerdiği bilgi itibarıyla TİCARİ GİZLİ derecesiyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi istenmeyen bilgi için kullanılır.

KİŞİYE GİZLİ: Kişisel Verilerin Korunması Kanunu çerçevesinde özel nitelikli kişisel veri kapsamına giren bilgi için kullanılır.

KİŞİYE ÖZEL: İçerdiği bilgi itibarıyla KİŞİYE GİZLİ derecesiyle korunması gerekmeyen, ancak ait olduğu kişi ve bilmesi gerekenler dışındaki kişiler tarafından bilinmesi istenmeyen bilgi için kullanılır.

TASNİF DIŞI: Gizlilik derecesi olmayan ve özel olarak korunması gerekmeyen bilgi için kullanılır.