



VERİ KORUMA ETKİ DEĞERLENDİRMESİ USUL VE ESASLARI HAKKINDA YÖNETMELİK

Doküman No	KVKK_Y3 VERSİYON 1.00
Revizyon Tarihi	-
Yayın Tarihi	09/05/2022
Sayfa	6

1. GİRİŞ ve KAPSAM

1.1.İşbu Veri Koruma Etki Değerlendirmesi (VKED/DPIA) Usul ve Esasları Hakkında Yönetmelik(bundan böyle Yönetmelik olarak anılacaktır) Belediyemizin Bilgi Güvenliği Politikası, Kişisel verilerin Korunması Politikası ve Çerçeve Politikası ile birlikte değerlendirilmelidir.

1.2.İşbu Yönetmelik, bilgi ve iletişim teknolojileri metodolojisi ya da genel ticari kullanım açısından özellikle yeni teknolojiler kullanıldığında ve veri işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, Belediyemiz veri sorumlusu sıfatıyla, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin değerlendirme yapmak durumunda olduğu zaman (GDPR Md. 35) ya da Bilgi Varlıkları Sahiplerinin kontrol ettikleri bilgi varlıklarına ilişkin yıllık gözden geçirme süreçlerinde Veri Koruma Etki Değerlendirmesi yaparken takip edilmesi gereken usul ve esasları düzenlemektedir.

2. VERİ KORUMA ETKİ DEĞERLENDİRMESİ

2.1.Bilgi Varlıkları Sahipleri olarak atanan çalışanların Bilgi Güvenliği Ve Kişisel Veriler Çerçeve Politikasında açıklanan sorumlulukları doğrultusunda kontrolleri altındaki bilgi varlıklarını idare etmekle sorumludurlar.

2.2.Bilgi Varlıkları Sahipleri, en azından yılda bir kez ve özellikle bilgi varlığında, varlığın muhafaza ve işleme metotlarında belirgin değişiklikler olması ya da bilgi varlıkları bünyesinde muhafaza edilen kişisel veriler üzerinde değişiklikler ön gören yasal düzenleme ya da politika değişiklikleri söz konusu olduğunda ise kesinlikle değişiklikler uygulamaya geçilmeden evvel bir etki değerlendirmesi yapmaları gerekmektedir.

2.3.Bilgi Varlıkları Sahipleri kontrol ettikleri varlıkların güvenliklerinin kurumumuzun Bilgi Güvenliği Politikasında zikredilen aşağıdaki koşulları karşıladığından emin olmaları gerekir:

- Tüm kullanıcıların bilgiye erişim sağlamadan önce uygun şekilde yetkilendirilmiş olmalıdır.
- Bilgi varlığının değer ve/veya hassasiyet değeri ile uyumlu olan makul güvenlik düzeyi sağlanmalıdır.
- Kullanıcılar veri güvenliği ihlali ile sonuçlanan ya da sonuçlanması muhtemel her olayı Bilgi İşlem Sorumlusuna bildirmelidir. İlgili kullanıcılar Bilgi İşlem Teknik Destek Ekibini ya da bağlı oldukları Şube Müdürlerini ya da Belediye Başkan Yardımcılarını ihlal hakkında gecikmeden bilgilendirmelidir.

- Kullanıcılar bilgi varlıkları envanterinin yıllık gözden geçirilmesi kapsamında sahip oldukları varlıklara ilişkin Veri Koruma Etki Değerlendirmesi yapmakla mükelleftir.

2.3.1. Her bir Bilgi Varlığı Sahibi sahip olduğu bilgi varlığı nezdinde tutulan her türlü materyalin aşağıda listelenen şartları her zaman karşılmasını temin etmek için gerekli makul çabayı sarf etmekle mükelleftir:

- Tutulan veriler hukuka uygun olmalıdır.
- Belediyenin Bilgi Güvenliği Politikasının 11. Bölümünde zikredilen BT Kaynaklarının Kullanım Koşulları ile uyumlu hareket edilmelidir.
- Tutulan veriler yasadışı materyallere bağlantı sağlayan linkler içermemeli ve Belediyemizin Bilgi ve Haberleşme Araçlarının Kullanım Koşulları ile uyumsuz içerik barındırmamalıdır.
- İlgili Başkan Yardımcısı/Şube Müdürü tarafından onaylanmadığı sürece Belediye namına herhangi bir ticari mal, ürün ya da hizmet tanıtımı ya da bunlarla ilgili yorumlara yer verilmemelidir.
- İlgili Başkan Yardımcısı/Şube Müdürü tarafından onaylanmadığı sürece Bilgi Varlığı Sahibinin veya başka herhangi bir kişinin herhangi bir şirketi, ortaklığı, konsorsiyumu veya danışmanlığını veya "özel" faaliyetlerini tanıtmaya veya yorum içerikli bilgi ve/veya veriler barındırılmamalıdır.

2.3.2. Belediyemizin bilgi varlıkları bünyesinde yer alıp herhangi bir kişiye ait olan bilgi ve veriler:

- Belediyeye ait marka, logo, antetli kâğıt vb.ni ihtiva etmemelidir.
- Muhafaza edilen materyaller Bilgi Varlığı Sahibinin Belediyenin BT varlıklarını kullanım noktasındaki yetkilendirme sebebine doğrudan bağlı ya da ilgili olmalıdır.
- İlgili Belediye politika ve yönetmelikleri ve bireysel olarak sahip olunan bilgilerin sunuş biçimi, her ne şekilde atıfta bulunulursa bulunulsun, herhangi bir şekilde Belediye'nin bireysel olarak sahip olunan bilgilerin kendisi veya içerdiği herhangi bir materyal veya görüş için herhangi bir sorumluluk aldığı veya bunları onayladığı şeklinde yorumlanamaz.

Bireysel olarak sahip olunan tüm bilgilerde, bu bilgilerin Belediye tarafından resmi olarak yayınlanmadığını gösteren onaylanmış bir sorumluluk reddi beyanı ekranda görünmelidir.

2.4.Tüm personel, Belediye tarafından tutulan bilgilerin hangi formatta tutulduğuna bakılmaksızın uygun şekilde korunmasını sağlamak için en iyi bilgi güvenliği uygulamalarını takip etmekten sorumludur. Tüm Şube Müdürleri, yönetim sorumluluklarının bir parçası olarak, kendi bölümlerindeki bilgi güvenliği uygulamalarını denetlemekle sorumludur. Bu sürecin bir parçası olarak, Şube Müdürleri, departmanları nezdinde tutulan varlıkları gözden geçirecek ve Belediye'nin Bilgi Varlık Envanterinin tüm yönetilen varlıkların doğru bir şekilde yansıttığını teyit etmek için gerekli tedbir ve kontrolleri sağlamakla mükelleftirler.

2.5.Bilgi Varlıkları Envanteri, bilgi ve haberleşme teknolojileri güvenliği ve BT varlıklarının yönetimi noktasında ilgili departmanların spesifik bilgi varlıklarının hangi özgün BT desteğine ihtiyaç duyacağını belirlenmesi ve bilgi güvenliği kontrollerinin yapılmasına yardımcı olmaktadır. Her ne kadar bilgi varlıkları envanteri Bilgi İşlem Birimi Sorumlusu tarafından idare edilmekte ise de kağıt ortamında tutulan kayıt ve varlıkların güvenliği de göz önünde tutularak gerekli tedbirler alınmalıdır.

2.6.Bilgi varlıkları mantıksal bağlantılar ve toplama yöntemleri kullanılmak suretiyle tanımlanmalıdır. Örneğin, bir sondaj çalışması için toplanan bilgiler, bir dizi dizüstü bilgisayar, bir grup sürücü ve USB bellekler dâhil olmak üzere çeşitli ortamlarda tutulabilir. Bu durumda, her ortamı ve bunların nasıl güvenli tutulduğunu açıklayan bir girdi olarak kaydedilmelidir.

2.7.Her ilgili departman bünyesinde tuttuğu bilgi varlıklarını beyan ederek envantere kaydedilmelerini sağlamalıdır. Dijital/kayıt depolama amacıyla yerel olarak alınan her bir ek depolama sistemi "Departmanca kullanılan sistem" varlığı olarak kaydedilmelidir. Ek bilgi varlıklarının kaydedilip kaydedilmesi gerektiği hususunda şüpheye düşülmesi halinde Bilgi İşlem Birimi Teknik Destek Ekibi ile irtibata geçilmelidir. Bulut depolama sistemleri ve kâğıt ortamında tutulan dosyalama sistemleri de bilgi varlığı olarak tanımlanarak envantere kaydedilmelidir.

2.8.Mahiyetlerindeki birimlerin bilgi varlıklarını gözden geçirirken Şube Müdürleri aşağıdaki hususları göz önünde bulundurmalıdır:

- Envantere eklenmesi gereken herhangi bir bilgi varlığı mevcut mudur?
- Kullanılmayan ve envantere çıkarılması gereken herhangi bir bilgi varlığı söz konusu mudur?
- Bilgi varlıkları envanterindeki kayıtların güncellenmesini gerektirecek bilgi varlıklarının kullanımı ile ilgili bir değişiklik söz konusu mudur?
- Şube Müdürlüğü tarafından kullanılan bilgi varlıklarının toplanma, işleme biçiminde değişiklik ön gören herhangi bir politika değişikliği ya da yasal düzenleme söz konusu mudur?

2.9.Şube Müdürleri, departmanlarındaki personelin birlikte çalıştığı tüm bilgiler veya bu bilgilerin saklandığı tüm unsurlar hakkında kapsamlı bilgiye sahip olmayacağı kabul

edilmektedir. Departmanların, bilgi varlık kaydını tamamlarken departmanın elinde tuttuğu bilgilerle ilişkili temel riskler ve bu bilgilerin nerede saklandığı hakkında geniş bir şekilde düşünmeleri önerilir. Bölümler, özellikle verilerin hassas olduğu veya Kolej dışına aktarıldığı durumlarda veri aktarımına odaklanmayı faydalı bulabilir. Daha fazla rehberlik için lütfen Bilgi İşlem Birimi Sorumlusu ile iletişime geçiniz.

3. BİLGİ VARLIKLARI ENVANTERİNİN YAPISI

Alan Adı	Açıklamalar
Bilgi Varlığı Sahibi	Bu bilgi varlığında depolanan bilgilerden kim sorumludur ve bu bilgi varlığıyla ilgili yapılacak sorgular için iletişim noktası/irtibat görevlisi kimdir?
Bilgi Varlığı Yöneticisi	Bilgi Varlığı Yöneticisinin üstleneceği rol Bilgi Güvenliği Politikası, Kişisel verilerin Korunması Politikası ve Çerçeve Politikasında tanımlanmış olup bilgi varlığını günlük bazda kullanan en yetkili görevli olarak tanımlanabilir. BELBİS ve EBYS sistemi ile ilgili Bakanlıkça tayin edilen kurallar saklıdır.
Bilgi Varlığının İsmi	Bilgi Varlığına atanan özgül isim
Bilgi Varlığının Tanımı	Bilgi varlığına ilişkin kısa bir tanımlama yapınız. Mümkün ise varlık bünyesinde tutulacak olan bilgilere ilişkin kısa bir bilgilendirme notu yazınız.
Varlığın Güncel Durumu	Yalnızca Bilgi Varlıkları envanterinde-Geçici, Onaylanmış ya da aktif değil vb.
Sınıflandırma	<ul style="list-style-type: none">• Bilgi varlığı özel nitelikli veri ihtiva etmekte midir? Bu verilerle alakalı riskler nelerdir? Risklerin elimine edilmesi veya azaltılması için alınan tedbirler nelerdir? Özel nitelikli veriler olarak değerlendirilecek olan veriler aşağıdaki gibidir:<ul style="list-style-type: none">○ Ticari açıdan hassas veri olarak değerlendirilen Belediye idaresine ilişkin veriler ya da araştırma verileri.○ 6698 sayılı kanunun 6. Maddesinde belirtilen “Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”.○ Bireysel finans verileri○ Belediyenin yaptırdığı araştırma/sondaj çalışmalarına ilişkin veriler.○ Yukarıda yer almamakla birlikte ifşa edildiği

	takdirde ilgili kişilerin zarar görmesine ya da itibarının zedelenmesine neden olabilecek kişisel veriler de bu kategoride değerlendirilmelidir.
Varlığın Depolanacağı Ortam Türü	Elektronik, manuel ya da her ikisi
Kanuni Dayanak	İlgili verinin işlenmesi ve/veya depolanması için kullanılan yasal dayanak nedir? 6698 Sayılı Kanun gereği kişisel verilerin hukuka uygun olarak işlenebilmesi için veri sorumluları tarafından kullanılabilen meşru veri işleme sebepleri göz önüne alınmalıdır.
İş Akışı Açısından Taşıdığı Önem	Bilgi varlığının Belediyenin iş akışı açısından taşıdığı hayati önem düzeyi ve varlığın kaybı ya da gizliliklerinin ihlal edilmesi durumunda ortaya çıkacak olumsuzluk seviyesi
Bilgi Varlığının Konumu	Bilgi varlığı fiziksel olarak nerede muhafaza edilmektedir? Örneğin yerel bilgisayarlarda, merkezi sistemde, portal nezdinde ya da sunucu haricinde bulunan bir noktada
Bilgi Varlığını Ekleyen Taraf	İlgili kaydın Bilgi Varlıkları Envanterine girişini yapan kimdir?
Ön Görülen Depolama Süresi	Bilgi varlığı hangi süreyle envanterde tutulacaktır? Bilginin Belediye operasyonları açısından gerekli olmadığını tespit etmek ve güvenli bir şekilde imha edilmesi için ön görülen süreç nedir? Verilerin hangi süreden sonra imha edilmesi gerektiği hususunda Belediyemizin Veri Saklama ve İmha Politikasını inceleyiniz.
En Eski Girdi	Güncel tarih-saklama süresi aralığı içinde olmaması gereken en eski kaydın tarihi
En Son Kayıt Girdisi	Artık güncellenmesi yapılmayan bilgi varlıkları için son kaydın yapıldığı tarihi

Bilgi Varlığı Sahibi olarak atanan görevlilerin ayrıca aşağıda sıralanan hususları göz önünde bulundurması gerekmektedir:

- Sorumlu Birim: hangi birim bahse konu bilgi varlığından sorumludur? (Genellikle “varlık sahibinin” görevli olduğu birim)
- Bilgi varlığına erişim sağlayacak olan birim ve/veya görevliler? İlgili bilgi varlığına erişim sağlaması ön görülen kişi gruplarını belirtiniz. Örneğin belirli bir ekipte görevli çalışanlar ya da tüm Belediye çalışanları. Ayrıca Belediye çalışanı olmamakla birlikte ilgili bilgi varlığına erişim sağlaması ön görülen üçüncü taraflar da açık bir şekilde belirtilmelidir.
- Bilgi varlığının güvenliği nasıl sağlanacaktır? Bilgi varlığının güvenliğini sağlamak için alınan tedbirleri özetleyiniz. Örneğin şifre ile koruma. Özel nitelikli kişisel veri ihtiva eden kâğıt ortamında tutulan kayıtlar kilitli bir dosyalama sisteminde muhafaza

edilmekte midir? Kilitler ne şekilde muhafaza edilmektedir? Uyarı: kesinlikle kullanılan şifre ya da kilitlerin tutulduğu konumu belirtmeyiniz!

- Yedekleme, Mukavemet ve Afet Kurtarma düzenlemeleri: Verilerin kaybı ya da veri/sistem(ler) güvenliğinin ihlali ile afet, deprem vb. hallerde verilerin kurtarılması ve/veya işlevsellik ve erişilebilirliklerinin korunması için alınan tedbirler nelerdir?

