

KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ HAKKINDA YÖNETMELİK'İN GETİRDİKLERİ VE DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Doç. Dr. Murat Volkan Dülger*

Kişisel verilerin korunması alanında konunun tüm paydaşları tarafından bir süreden beri merakla beklenen gelişmelerinden biri 28 Ekim 2017 tarihinde gerçekleşti ve Kişisel Verileri Koruma Kurumu tarafından 6698 sayılı Yasaya dayanılarak “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*”, 30224 sayılı ve 28.10.2017 tarihli Resmi Gazete’de yayınlandı. Hemen belirtmeyim ki Yönetmeliğin 14. maddesine göre yürürlüğe giriş tarihi 1 Ocak 2018 olarak belirlendi. Nitekim diğer taslak halindeki yönetmeliklerde de 1 Ocak 2018 yürürlüğe giriş tarihi olarak belirlendi. Dolayısıyla bu tarih KVK hukuku açısından adeta bir başlangıç tarihi olarak belirlenmiş durumda.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 3. maddesinin 1. fıkrasının (b) bendinde “anonim hale getirme” kavramı tanımlanmış ve 7. maddesinde “*kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi*” düzenlenmiştir. 7. maddenin 3. fıkrasında ise kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Ayrıca Yasanın 22. maddesinin 1. fıkrasının (e) bendinde de Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapma görev ve yetkisinde olduğu düzenlenmiştir. İşte bu düzenleme gereğince söz konusu yönetmelik düzenlenmiş ve yayınlanmıştır.

Aşağıda başlıklar halinde yönetmelikle getirilen yeni düzenlemeler ve kavramlar ile açıklanması gereken hususlara teorik ayrıntılara girmeden değineceğim.

Kişisel veri envanteri

Yönetmeliğin dikkatleri üzerine çeken ilk düzenlemesi “Tanımlar” başlıklı 4. maddenin 1. fıkrasının (e) bendinde düzenlenen kişisel veri işleme envanterinin tanımlanmış olmasıdır. Buna göre kişisel veri envanteri; “*Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter*” olarak tanımlanmıştır.

Bu husus, bizim de hem verdiğimiz eğitimlerde hem de gerçekleştirmiş bulunduğumuz uyum projelerinde üzerinde en çok durduğumuz konulardan biri olduğu gibi, uyum projelerinin de ilk safhasını oluşturmaktadır. İşte yönetmeliğin bu maddesiyle kişisel veri

* İstanbul Medipol Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi, Avukat.

envanterinde bulunması gereken asgari şartlar belirlenmiş olmakla birlikte,, bu envanterin mevcut bulunması Yönetmeliğin bütününden çıkan anlam gereğince bir zorunluluk haline getirilmiştir.

Yönetmelik gereğince kişisel veri envanterinde bulunması gereken asgari hususlar şunlardır:

- Kişisel veri işleme amacı,
- Veri kategorisi,
- Aktarılan alıcı grubu,
- Kişisel verinin tutulacağı azami süre,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Veri güvenliğine ilişkin alınan tedbirler.

Bir uyum projesinin ana başlıklarını bu alt başlıklar oluşturmakla birlikte, bunları detaylandıran alt kırılımların olmasının mümkün ve gerekli olduğunu ifade etmeliyim. Böylelikle kişisel verilerin korunmasına uyum sürecinin olmazsa olmaz bileşeni ve ilk adımı olan kişisel veri envanteri oluşturulmasının asgari standartları belirlenmiştir. Bunun bir zorunluluk olduğu ise aşağıda değineceğimiz Yönetmeliğin 5. maddesinden anlaşılmaktadır.

Alıcı grubu

Yönetmeliğin “Tanımlar” başlıklı 4. maddenin 1. fıkrasının (a) bendinde alıcı grubu terimi tanımlanmıştır. Buna göre alıcı grubu; “*Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi*” olarak belirtilmiştir. Bu tanım da Yönetmelikle oluşturulan yeni bir kavramdır. Yönetmelik gereğince kişisel veri envanteri oluşturulurken alıcı grubunun da belirtilmesi gerekir. Dolayısıyla bir değil, birden fazla alıcı grubunun bulunması söz konusu olacaktır. Alıcı grubunun doğru belirlenmesi, envanterin doğru oluşturulmasındaki en önemli adımlardan biridir. Örneğin, alıcı grubunun belli bir devlet kurumu olması ve yasadan kaynaklanan bir istisnanın olması halinde silme, yok etme veya anonimleştirme süresi ve şekli bu yasaya göre belirlenecektir. Söz konusu verilerin de bu alıcı grubuna bağlı olarak envanterde bu şekilde gösterilmesi gerekir.

İlgili kullanıcı

Yönetmelikte “ilgili kullanıcı” kavramı tanımlanmıştır. Buna göre; ilgili kullanıcı “*Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler*” olarak tanımlanmaktadır. İlk olarak belirtilmesi gereken husus ilgili kişi, verisi işlene gerçek kişi iken; ilgili kullanıcının söz konusu kişisel veriyi veri sorumlusu adına işleyen kişi olduğudur.

Bu tanımda bazı hususlara dikkat çekmek gerekir. Öncelikle veri sorumlusu ile ilgili kullanıcı birbirinden farklıdır. Zira ilgili kişi, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan kişi değildir. Yönetmelikte açıkça belirtildiği üzere ilgili kullanıcı, ya veri sorumlusunun organizasyonu içerisinde yer alarak (Örneğin, şirket çalışanı.) kişisel verileri işleyen ya da veri sorumlusundan aldığı yetki ve talimat ile (Örneğin, bu alanda hizmet üreten üçüncü kişiler, danışmanlık şirketleri gibi.) kişisel verileri işleyen kişilerdir.

Ayrıca ilgili kişi, şirketler ya da kurumlarda genellikle dijital her türlü verinin depolanması, aktarılması ve korunmasına ilişkin alt yapı hizmetlerini sunan “bilgi teknolojileri / BT” birimi ya da bu birimin çalışanlarının dışında bulunan kişilerdir. Yönetmeliğin bu tespiti son derece yerinde ve uygulamanın gerçekleriyle örtüşür biçimdedir. Bizim de farkındalık eğitimlerinde ve yürüttüğümüz uyum süreçlerinde gözlemlediğimiz önemli bir husus, BT biriminin kişisel veriler de dahil olmak üzere her türlü veriden sorumlu olduğuna ilişkin yanlış algıdır. Oysa BT birimi Yönetmelikte de gayet güzel bir biçimde ifade edildiği üzere yalnızca verilerin depolanması, korunması, yedeklenmesi, iletilmesi ve işlemeye uygun halde bulundurulmasından sorumludur. Kişisel verileri kaydeden ve işleyenler ise eğer bir şirketten söz ediyorsak; pazarlama, satın alma, insan kaynaklar gibi diğer iş birimleridir. İşte yönetmelikle getirilen bu tanımla “ilgili kullanıcının” bu iş birimleri olduğu açıklığa kavuşturulmuştur.

Kişisel veri saklama ve imha politikası

Yönetmeliğin 5. maddesinde kişisel veri saklama ve imha politikasına ilişkin esaslar düzenlenmiştir. Buna göre veri sorumluları siciline kayıt olmakla yükümlü olan veri sorumluları¹, oluşturdukları kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası oluşturmak zorundadır. Yukarıda da belirttiğim üzere, aslında bu maddeyle veri sorumlularına kişisel veri envanteri oluşturma yükümlülüğü getirilmektedir. Zira yine veri sorumlularına bir yükümlülük olarak getirilen ve bu maddenin konusunu oluşturan kişisel veri saklama ve imha politikası oluşturma yükümlülüğünün yerine getirilebilmesi için öncelikle kişisel veri işleme envanterinin oluşturulması gerekir. Yönetmeliğe göre kişisel veri saklama ve imha politikasının kişisel veri envanterine uyumlu olması gerekir.

Bu envanterin yapılması ve kişisel veri saklama ve imha politikasının oluşturulması, söz konusu işlemlerin uygulamada yapıldığı anlamına gelmez. Politikalarla uygulamanın paralel olması gerekir. Nitekim bu husus 5. maddenin 2. fıkrasında belirtilmektedir.

¹ Kurum tarafından yayınlanmak üzere Başbakanlığa gönderilen taslak halindeki Veri Sorumluları Hakkında Sicil Yönetmeliği'nin “Kayıt Yükümlülüğünün İstisnaları” başlıklı dördüncü bölümünde yer alan 16. ve 17. maddelerinde kayıt yapmakla yükümlü olmayan veri sorumlularını belirlenmiştir. Buna göre:

İstisna uygulanacak haller

MADDE 16 – (1) Aşağıda belirtilen kişisel veri işleme faaliyetleri bakımından veri sorumlusunun bu faaliyetleri Sicile kayıt etmesi ve bildirmesi yükümlülüğü yoktur.

- a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- ç) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Kurul tarafından belirlenen istisna kriterleri

MADDE 17- (1) Kurul, aşağıdaki kriterleri göz önünde bulundurarak kayıt yükümlülüğüne istisna getirebilir:

- a) Kişisel verinin niteliği,
- b) Kişisel verinin sayısı,
- c) Kişisel verinin işleme amacı,
- ç) Kişisel verinin işlendiği faaliyet alanı,
- d) Kişisel verinin üçüncü kişilere aktarılma durumu,
- e) Kişisel veri işleme faaliyetinin kanunlardan kaynaklanması,
- f) Kişisel verilerin muhafaza edilmesi süresi,
- g) Veri konusu kişi grubu veya veri kategorileri.

(2) Kurul, birinci fıkrada sayılan kriterler çerçevesinde belirlenen istisnaların kapsamını, uygulama esaslarını, hesap yöntemlerini ve usulünü belirlemek amacıyla karar alma yetkisini haizdir. Kurul bu kararlarını uygun yöntemlerle yayımlayarak kamuya duyurur.

Kişisel veri saklama ve imha politikasının hangi hususları kapsayacağı ise Yönetmeliğin 6. maddesinde düzenlenmektedir. Buna göre saklama ve imha politikası asgari olarak;

- Kişisel veri saklama ve imha politikasının hazırlanma politikanın amacına,
- Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
- Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,
- Kişisel verilerin saklanması ve imhasını gerektiren hukuki ve teknik terimlerin tanımlarına,
- Kişisel verilerin saklanması ve imhasını gerektiren hukuki, teknik ve diğer sebeplere ilişkin açıklamaya,
- Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
- Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
- Saklama ve imha sürelerini gösteren tabloya,
- Periyodik imha sürelerine,
- Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe,

ilişkin bilgilere yer vermelidir. Yasaya ve yönetmeliğe uyumun sağlanması ve veri sorumlusunun yasadan kaynaklanan sorumluluğunu yerine getirebilmiş olması için söz konusu politikanın asgari düzeyde belirtilen standartlarda oluşturulması ve bunun uygulamaya geçirilmesi gerekir. Bu da ancak bir KVKK'ya uyum süreciyle olabilecek, dönüşümü gerektiren bir konudur.

Silme, yok etme ve anonimleştirmenin kayıt altına alınması ve bu kayıtların saklanması

Yönetmeliğin 7. maddesinin 3. fıkrası ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemlerin kayıt altına alınacağı ve bu kayıtların en az üç yıl süreyle saklanacağı ifade edilmiştir. Ayrıca başka hukuki yükümlülüklerden kaynaklanan süreler var ise bunların da dikkate alınması gerektiği belirtilmiştir. Buna göre KVK mevzuatına uyum için kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yeterli değildir. Bu işlemlerin kayıt altına alınması (bunun için basılı ya da dijital bir tutanak oluşturulması) ve bu kayıtların en az üç yıl boyunca saklanması gerekir.

Silme, yok etme ve anonimleştirmede yöntem

Kişisel veriler basılı ortamlarda olabileceği gibi dijital ortamlarda da olabilir. Her iki ortam için de yapılacak işlemlere ilişkin yöntemlerin belirlenmesi ve belirlenen yöntemlerin hem kişisel veri saklama ve imha politikasında hem de yöntemlerin belirlendiği politikalarda açıklanması gerekir. Bu yine veri sorumlusuna düşen bir görevdir. Bu durum yönetmeliğin 7. maddesinin 4. fıkrasında düzenlenmiştir. Örneğin üzerinde kişisel verilerin bulunduğu basılı bir belgenin doğrudan çöp kutusuna atılması yok etme için yeterli değildir. Duruma göre belgenin yakılarak ya da uygulamada daha çok görüldüğü üzere kâğıt öğütücünden geçirilerek

yok edilmesi gerekir. Benzer şekilde bir verinin bilgisayar ortamında çöp kutusuna atılması silme anlamına gelmez. Bu, söz konusu verinin indeksten (active directory) silindiği anlamına gelir. Veri aslında diskte olduğu yerde durmaktadır. Gerçek anlamda silmek için verinin hard diskten tamamen kaldırılması gerekir. Bunun için ise ana belleğin formatlanması gerekir. Ancak bu durumda dahi veri kurtarma yazımlarıyla verinin geri dönüştürülmesi mümkündür. O halde verinin yok edilmesinden bahsedebilmek için başka tekniklerin kullanılması gerekir. Örneğin “degauss” yöntemiyle diskin mıknatıs özelliğinin yok edilerek verilerin uçmasının sağlanması gibi. Buradaki son aşama ise veriyi barındıran aygıtın fiziksel olarak yok edilmesi amacıyla öğütülmesidir. İşte veri sorumlusunun, sorumlu olduğu verilerin niteliği ve bu konuda belirlenmiş olan politikalar ve ihtiyaçlar gereğince, hangi tür verileri nasıl bir işleme tabi tutacağı ve bu işlemin sonunda neyin olmasını hedeflediğini, ilgili prosedürlerinde açık bir biçimde belirtmesi gerekir.

Bu bağlamda veri sorumlusunun, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını belirleme hakkı vardır. Kişisel verinin ilgisinin talebi halinde silinmesi, yok edilmesi veya anonimleştirilmesi halinde ise veri sorumlusunun yine yöntemi belirleme hakkı olmakla beraber bunun gerekçesini açıklama zorunluluğu bulunmaktadır.

Kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi

Yönetmeliğin 8. maddesinde kişisel verilerin silinmesi, 9. maddesinde yok edilmesi ve 10. maddesinde anonimleştirilmesi düzenlenmiştir.

Yönetmeliğin 8. maddesinde göre; “(1) *Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür*”.

Yönetmeliğin tanımında yerinde olarak silme işlemi için nasıl bir teknik kullanılacağı belirtilmeden, sonuçta neyin olması gerektiği tanımlanmıştır. İlgili kullanıcı tarafından kişisel verinin hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi, verinin silinmesi işlemidir. Dolayısıyla bu yöntemde kişisel verinin geri dönüştürülmesinin imkansız olması aranmamaktadır. Önemli olan kişisel veri envanterinde verinin kullanıcısı olarak görünenlerin bu veriye bir daha erişememesi ve kullanamamasıdır. Ancak veri kullanıcısı dışındaki üçüncü bir kişinin (örneğin bir suç soruşturmasında görevli adli kolluk memurlarının) bu verileri geri dönüştürerek, verilere erişmesi ve bu verileri kullanması mümkündür.

Bunun yönetimini belirlemek veri sorumlusunun görevidir; nitekim buna ilişkin her türlü teknik ve idari tedbiri almanın veri sorumlusunun yükümlülüğünde olduğu maddenin 2. fıkrasında belirtilmiştir.

Yönetmeliğin 9. maddesinde göre; “(1) *Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür*”.

Teknik belirtilmeksizin tanımlama yok etme işlemi için de kullanılmıştır. Yok etme, silmeden farklı olarak, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez geri getirilemez ve tekrar kullanılamaz hale getirilmesidir. O halde kişisel verilerin yok edilmesi

işlemi için, verilere adli bilişim ve veri kurtarma yazılımlarıyla dahi erişilmez bir yöntemin uygulanması gerekir. Bunun için yukarıda belirtmiş olduğum degauss vb. yöntemlerin ya da donanımların uygulanması mümkündür. Bu işlem sonucunda yalnızca verinin kullanıcısı değil, hiç kimse veriye ulaşamamalıdır. Bunun yöntemini belirlemek yine veri sorumlusuna aittir.

Yönetmeliğin 10. maddesine göre; “(1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. (2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. (3) Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür”.

Kişisel verinin tanımı Yasada kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Dolayısıyla bilginin bir gerçek kişiyi belirlemesi veya belirlenebilir olmasını sağlaması ihtimalinin ortadan kaldırılması halinde anonimleştirme söz konusu olacaktır. İşte Yönetmeliğin 10. maddesinde Yasaya bağlı kalınarak bu esastan hareketle anonimleştirme düzenlenmiştir. Anonimleştirme öyle bir yöntemle yapılmalıdır ki kişisel veriler başka verilerle eşleştirilse, aralarında bir bağ kurulsa dahi hiçbir surette ait olduğu gerçek kişiyi belirlenebilir hale getirmemelidir. Bu bağlamda kişisel verinin maskelenmesi yetmemektedir. Zira maskeleyemede, başka verilerle eşleştirme halinde verinin sahibine ulaşılması mümkündür. Benzer şekilde anonimleştirme öyle yapılmalıdır ki, bunu yapan dahi sonradan geri dönüp veri sahibini belirleyememelidir. Anonimleştirme işleminin sonucunda sosyal mühendislik, adli bilişim uygulamaları vb. gibi yöntem ve teknikler kullanılarak verilerin gerçek kişilerle eşleştirilme olanağının olmaması gerekir. Bu işlem için de kullanılacak yöntem ve idari tedbirlerin seçilmesi görevi veri sorumlusuna bırakılmıştır.

İfade etmeliyim ki, kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesi için; veri sorumlularının, hem bu alanda uzman hukukçulardan hem de bilişim güvenliği uzmanlarından destek almaları gerekir. Zira hem hukuki hem de bilişim güvenliği alanındaki ihtiyaç ve riskler ancak bu kişilerin desteği ile tam olarak belirlenip, giderilebilir. Özellikle kişisel verilerin korunması alanının ülkemiz açısından oldukça yeni olması bu gerekliliği bir zorunluluk haline getirmektedir.

Resen silme, yok etme ve anonim hale getirmeye ilişkin süreler

Bu başlık altında karşımıza çıkan ilk kavram “periyodik imha işlemi”dir. Veri sorumlusunun verileri kaydetmeye ve işlemeye başlamasından itibaren, bu süreçlere paralel olarak yasada veya veri işleme politikasında belirtilen nedenlerle kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesini gerektirecek hususlar sürekli gerçekleşecektir. Ancak bir yandan verilerin kaydedilmesi, işlenmesi, aktarılması vs. gibi işlemler yapılırken bir yanda da sürekli olarak verilerin silinmesi, yok edilmesi veya anonimleştirilmesinin yapılması ciddi bir zaman ve emek gerektirecektir. İşte bu durumu dikkate alan Kurum bunun periyodik bir sürece bağlanmasını öngörmüş ve veri sorumlularından bunu istemiştir.

Buna göre periyodik imhanın gerçekleştirileceği zaman aralığının kişisel veri saklama ve imha politikasında belirlenmesi gerekir. Bu süre altı aydan fazla olamaz. Silme, imha etme veya anonimleştirme işleminin, yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde gerçekleştirilmesi gerekir. Örneğin, bir şirketin bu süreleri 1 Ocak ve 1 Haziran olarak belirlemesi halinde, 1 Ocak'tan 30 Mayıs'a kadar olan süreçte ortaya çıkan imha yükümlülüğüne ilişkin her bir işlem 1 Haziran'da gerçekleşecek ve bu kayıt altına alınacaktır.

Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu için ise (ki bunlar sicile kayıt olma yükümlülüğünün istisnasını oluşturan gruptur) bu süre imha yükümlülüğün doğduğu andan itibaren üç aydır. Dolayısıyla bu tür veri sorumluların kendilerine üç aylık periyotlar belirlemeleri gerekir.

Talebe bağlı silme ve yok etmeye ilişkin süreler

Resen silme, yok etme ve anonimleştirmenin yanı sıra, Yönetmeliğin 12. maddesinde ilgilinin talep etmesi halinde silme ve yok etme süreleri de düzenlenmiştir. Buna göre kişisel verileri işleme şartlarının tamamının ortadan kalkması halinde, veri sorumlusu talebe konu kişisel verileri silecek, yok edecek veya anonimleştirecektir. Bu talep en geç otuz gün içinde yerine getirilecek ve ilgili kişiye bilgi verilecektir. Yönetmelikte bu konuda bir ayırım yapılmadığı için talebin yerine getirilmesi ve bildirilmesi işlemi için toplamda otuz gün verildiğini düşünmekteyim.

Kişisel verilerin üçüncü kişilere aktarılması halinde ise, veri sorumlusu bu talebi üçüncü kişilere aktarır ve vaki talebin üçüncü kişi tarafından yerine getirilmesini sağlar. Başka bir süre belirtilmediği için veri üçüncü kişide bulursa da otuz günlük süre geçerlidir.

Kişisel verileri işleme şartlarının tamamının ortadan kalkmaması halinde ise, bu talep reddedilebilir ve bu durum gerekçesiyle birlikte ilgili kişiye bildirilir. Bildirim yazılı ve elektronik ortamda yapılabilir. Buna göre elektronik postayla yapılan bildirimin yeterli sayılması gerekir. Bu bildirimin de otuz gün içinde yapılması gerekir.

Tereddütlerin giderilmesi

Ülkemiz açısından yeni olan kişisel verilerin korunması alanının ve bu alana özgü çıkartılan mevzuatın yorumlanmasında ve uygulanmasında çeşitli tereddütlerin ve belirsizlik hallerinin ortaya çıkması son derece doğaldır. İşte bu tür tereddütlerin doğması halinde bunların giderilmesi yetkisinin de Kurul'da olduğu belirtilmiştir. Dolayısıyla Kurul hem vereceği kararlarla hem de gerektiğinde bu konuya özgü alacağı ilke kararlar ya da tebliğlerle uygulamaya da yol gösterici olacaktır.

Yönetmeliğin bu maddesiyle bu yetki Kurul'da tutulmak istenmişse de buna göre bu yalnızca bir niyetin ifadesidir. Zira şu an olduğu gibi, kişisel verilerin korunmasına ilişkin mevzuat ve uygulama, öğretide yorumlanıp eleştirilebileceği gibi, hem mevzuatın hem de Kurul'un vereceği kararların yargının denetime tabi olacağı kaçınılmaz bir gerçektir. Dolayısıyla özellikle yargı mercilerinin vereceği kararlar da bu alanda yol gösterici olacaktır. Bildiğim kadarıyla hali hazırda Kişisel Verilerin Korunması Kanunu hakkındaki bir iptal davası Anayasa Mahkemesi'nin önünde karara bağlanmayı beklemektedir. Mahkemenin bu konuda vereceği red ya da iptal kararı konunun açıklanması bakımından son derece önemlidir.

Sonuç yerine ana başlıklar

Yönetmeliğin incelenmesi sonucu ulaştığım ve dikkate alınması gerektiğini düşündüğüm ana başlıklar şunlardır:

- “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik”, 30224 sayılı ve 28.10.2017 Resmi Gazete’de yayınlandı.
- Yönetmeliğin 14. maddesine göre yürürlüğe giriş tarihi 1 Ocak 2018 olarak belirlendi.
- Yönetmeliğin dikkatleri üzerine çeken ilk düzenlemesi “Tanımlar” başlıklı 4. maddenin 1. fıkrasının (e) bendinde düzenlenen kişisel veri işleme envanterinin tanımlanmış olması.
- Yönetmeliğin bu maddesiyle kişisel veri envanterinde bulunması gereken asgari şartlar belirlendiği gibi, bu envanterin bulunması Yönetmeliğin bütününden çıkan anlam gereğince bir zorunluluk haline getirilmiş.
- Yönetmelik gereğince kişisel veri envanterinde bulunması gereken asgari hususlar şunlardır: Kişisel veri işleme amacı, veri kategorisi, aktarılan alıcı grubu, kişisel verinin tutulacağı azami süre, yabancı ülkelere aktarımı öngörülen kişisel veriler, veri güvenliğine ilişkin alınan tedbirler.
- Yönetmeliğin “Tanımlar” başlıklı 4. maddenin 1. fıkrasının (a) bendinde alıcı grubu tanımlanmıştır.
- Alıcı grubunun doğru belirlenmesi, envanterin doğru oluşturulmasındaki en önemli adımlardan biridir.
- Yönetmelikte “ilgili kullanıcı” kavramı tanımlanmıştır. İlgili kullanıcı, ya veri sorumlusunun organizasyonu içerisinde yer alarak (Örneğin, şirket çalışanı.) kişisel verileri işleyen ya da veri sorumlusundan aldığı yetki ve talimat ile (Örneğin, bu alanda hizmet üreten üçüncü kişiler, danışmanlık şirketleri gibi.) kişisel verileri işleyen kişilerdir.
- İlgili kişi, şirketler ya da kurumlarda genellikle dijital her türlü verinin depolanması, aktarılması ve korunmasına ilişkin alt yapı hizmetlerini sunan “bilgi teknolojileri / BT” birimi ya da bu birimin çalışanlarının dışında bulunan kişilerdir.
- Veri sorumluları siciline kayıt olmakla yükümlü olan veri sorumluları, oluşturdukları kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası oluşturmak zorundadır.
- Kişisel veri envanterinin yapılması ve kişisel veri saklama ve imha politikasının oluşturulması, söz konusu işlemlerin uygulamada yapıldığı anlamına gelmez. Politikalarla uygulamanın paralel olması gerekir. Nitekim bu husus 5. maddenin 2. fıkrasında belirtilmektedir.
- Kişisel veri saklama ve imha politikasının hangi hususları kapsayacağı ise Yönetmeliğin 6. maddesinde düzenlenmektedir.
- Yasaya ve Yönetmeliğe uyumun sağlanması ve veri sorumlusunun yasadan kaynaklanan sorumluluğunu yerine getirebilmiş olması için söz konusu politikanın asgari düzeyde belirtilen standartlarda oluşturulması ve bunun uygulamaya geçirilmesi gerekir. Bu da ancak bir KVKK’ya uyum süreciyle olabilecek, dönüşümü gerektiren bir konudur.

- Yönetmeliğin 7. maddesinin 3. fıkrası ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemlerin kayıt altına alınacağı ve bu kayıtların en az üç yıl süreyle saklanacağı ifade edilmiştir.
- Veri sorumlusunun, sorumlu olduğu verilerin niteliği ve bu konuda belirlenmiş olan politikalar ve ihtiyaçlar gereğince, hangi tür verileri nasıl bir işleme tabi tutacağı ve bu işlemin sonunda neyin olmasını hedeflediğini, ilgili prosedürlerinde açık bir biçimde belirtmesi gerekir.
- Veri sorumlusunun Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını belirleme hakkı vardır.
- Kişisel verinin ilgisinin talebi halinde silinmesi, yok edilmesi veya anonimleştirilmesi halinde ise veri sorumlusunun yine yöntemi belirleme hakkı olmakla beraber bunun gerekçesini açıklama zorunluluğu bulunmaktadır..
- Yönetmeliğin 8. maddesinde kişisel verilerin silinmesi, 9. maddesinde yok edilmesi ve 10. maddesinde anonimleştirilmesi düzenlenmiştir.
- Yönetmeliğin tanımında yerinde olarak silme işlemi için nasıl bir teknik kullanılacağı belirtilmeden, sonuçta neyin olması gerektiği tanımlanmıştır.
- İlgili kullanıcı tarafından kişisel verinin hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi, verinin silinmesi işlemidir.
- Bu yöntemde kişisel verinin geri dönüştürülmesinin imkansız olması aranmamaktadır. Önemli olan kişisel veri envanterinde verinin kullanıcısı olarak görünenlerin bu veriye bir daha erişememesi ve kullanamamasıdır.
- Teknik belirtilmeksizin tanımlama yok etme işlemi için de kullanılmıştır.
- Yok etme, silmeden farklı olarak, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesidir.
- Anonimleştirme öyle bir yöntemle yapılmalıdır ki kişisel veriler başka verilerle eşleştirilse, aralarında bir bağ kurulsada hiçbir surette ait olduğu gerçek kişiyi belirlenebilir hale getirmemelidir. Bu bağlamda kişisel verinin maskelenmesi yetmemektedir.
- Periyodik imhanın gerçekleştirileceği zaman aralığının kişisel veri saklama ve imha politikasında belirlenmesi gerekir. Bu süre altı aydan fazla olamaz.
- Silme, imha etme veya anonimleştirme işleminin, yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde gerçekleştirilmesi gerekir.
- Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu için ise (ki bunlar sicile kayıt olma yükümlülüğünün istisnasını oluşturan gruptur) bu süre imha yükümlülüğün doğduğu andan itibaren üç aydır.
- Dolayısıyla bu tür veri sorumlularının kendilerine üçer aylık periyotlar belirlemeleri gerekir.
- Kişisel verileri işleme şartlarının tamamının ortadan kalkması halinde, veri sorumlusu talebe konu kişisel verileri silecek, yok edecek veya anonimleştirecektir.
- Bu talep en geç otuz gün içinde yerine getirilecek ve ilgili kişiye bilgi verilecektir.
- Kişisel verilerin üçüncü kişilere aktarılması halinde ise, veri sorumlusu bu talebi üçüncü kişilere aktarır ve vaki talebin üçüncü kişi tarafından yerine getirilmesini sağlar.

- Başka bir süre belirtilmediği için veri üçüncü kişide bulunsa da otuz günlük süre geçerlidir.
- Kişisel verileri işleme şartlarının tamamının ortadan kalkmaması halinde ise, bu talep reddedilebilir ve bu durum gerekçesiyle birlikte ilgili kişiye bildirilir.
- Bildirim yazılı ve elektronik ortamda yapılabilir. Bana göre elektronik postayla yapılan bildirimin yeterli sayılması gerekir. Bu bildirimin de otuz gün içinde yapılması gerekir.