# Hazine-i Evrak'ın 170. Kuruluş Yıldönümü
# ve
# XI. Arşivcilik Günü Etkinliği

*'Kolektif Hafızada Kırılganlık: Bilgi Güvenliği'*

**I. OTURUM**

**Oturum Başkanı: Nizamettin OĞUZ**

**Sunum 1:** Yrd. Doç. Dr. Mehmet Fahri FURAT - Prof. Dr. İshak KESKİN: Risk Altındaki Hafıza: Kişisel / Aile Hafızamızı Torunlarımıza Bırakabilecek miyiz?

**Sunum 2:** Yakup YILDIRIM: Bilgi Güvenliğinin Tanım ve Kapsamı

**Sunum 3:** Doğukan Güran: Belge Güvenliği

**Sunum 4:** Abdullah Raşit GÜLHAN: 21. yüzyılda Belge ve Bilgi Güvenliği

**Sunum 5:** Yrd. Doç. Dr. Erkan ÖZHAN: Kurumsal Hafızanın Korunmasında Sistemin Önemi

**II. OTURUM**

**Oturum Başkanı: Dr. Hidayet Yavuz Nuhoğlu**

**Sunum 1:** Prof. Dr. Hamza KANDUR: Elektronik Arşivlerde Sürdürülebilirlik Stratejileri

**Sunum 2:** Prof. Dr. Özgür KÜLCÜ: Elektronik Ortamda Belgelerin Uzun Süre Korunması, Güvenliği ve Erişim Etkinliğinin Artırılmasında Üstveri Elemanlarının Önemi; Sorunlar ve Çözüm Arayışları

**Sunum 3:** Dr. Bahattin YALÇINKAYA: Endüstri 4.0 Bağlamında Siber Güvenlik ve Arşivciliğe Yansımaları

**Sunum 4:** Yrd. Doç. Dr. Türkay HENKOĞLU: Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme

**Sunum 5:** Av. Ceyda AKAYDIN CİMİLLİ: Kişisel Verilerin Korunması İçin Kurumlarda Alınması Gereken Önlemler ve Düzenlemeler

# RİSK ALTINDAKİ HAFIZA: KİŞİSEL HAFIZAMIZI TORUNLARIMIZA BIRAKMAK MÜMKÜN OLABİLECEK Mİ?

**Prof. Dr. İshak Keskin**
ishakkeskin@gmail.com
*İstanbul Üniversitesi Bilgi ve Belge Yönetimi Bölümü*

**Yrd. Doç. Dr. Mehmet Fahri Furat**
m.f.furat@gmail.com
*İstanbul Üniversitesi Bilgi ve Belge Yönetimi Bölümü*

Kişisel dijital mirasımızı ne kadar önemsiyoruz? Her gün bilgi üretim araçlarıyla farklı formlarda belge üretiyoruz. Ancak ürettiğimiz belgelerin geleceğe aktarılması konusunda genel anlamda güçlü bir kaygıya sahip değiliz. Şüphesiz bir kısmımız ürettiği belgelerin güncel değerlerinin farkındadır; ancak onların gelecekteki anlam, önem ve değerine ilişkin çok az düşünüyor veya gelecekte tümüyle yok olabileceğinin farkında değiliz. Geleneksel bilgi kaynakları kolaylıkla çok uzun süreler boyunca korunabilir; üstelik bunu çok fazla zahmet ve maliyet gerekmeksizin yapabilme imkânımız var. Hâlbuki dijital bilgi kaynakları, -geleneksel bilgi kaynaklarının aksine- karmaşık doğaları gereği kırılgandır; onları kullanılabilir halde tutmak ve erişimlerine süreklilik kazandırmak için özel olarak çalışmak gerekir. Bu, aslında sadece taşınabilir dijital kültürel mirasımız adına önemli bir risk değil aynı zamanda bizleri torunlarımıza anlatacak kişisel mirasımızı korumamız gerekliliğini hatırlatan önemli bir uyarıdır. Bu yüzden, zaman kaybetmeksizin ürettiğimiz dijital fotoğraflarımızın, elektronik belgelerimizin, videolarımızın ve diğer dijital formdaki belgelerimizin şahsımıza ait kültürel bir miras olarak gelecek kuşaklara aktarılmasını sağlamak için önemli kararlar almak ve dijital dosyalarımızı aktif biçimde yönetmek zorundayız. Bu bildirinin amacı; kişisel temelde ürettiğimiz yeni teknoloji ürünü materyallerin sonraki kuşaklara aktarılmasında hissetmemiz gereken kaygı, yeni tür bilgi taşıyıcılarının karmaşık yapısının bilginin korunmasında ortaya çıkardığı zorluklar, geleneksel bilgi taşıyıcılarına göre korunmalarının çok daha fazla maliyet ve hassasiyet gerektirdiği, korumak ve hatırlanmamızı sağlayacak bu belgelerin düzenlenerek erişimlerine süreklilik kazandırmak konularında farkındalık oluşturmaktır. Toplumda üretilen kişisel dijital mirasın düzenlenmesi, korunması, erişimlerinin sağlanması konusunda farkındalık oluşturmak da günümüz arşivcilerinin ve arşivlerinin önemli sorumlulukları arasındadır.

# BİLGİ GÜVENLİĞİNİN TANIM VE KAPSAMI

**Yakup Yıldırım**
*yakupyildirim2002@yahoo.com*
*Osmanlı Arşivi Bilgi-İşlem Koordinatörü*

**Tanım :** Bilgi güvenliği, bilginin istenen zamanda istenen kişiye istenilen şekilde iletilmesi ve bu işlem için gerekli tüm faaliyetlerdir. Bilgi güvenliği kavramı genel bir ifadedir. Özelde; personel/kullanıcı güvenliği, yazılı veya elektronik belgelerin güvenliği, varlık güvenliği, veritabanı güvenliği, web servislerinin güvenliği, kablolu/kablosuz ağ güvenliği, veri güvenliği sisteminin kendi güvenliği vb. alt alanlar ayrı ayrı kendi prosedürlerini belirlerler. Alt alanların güvenlik politikası genel veri güvenliği politikasıyla çelişemez.
**Kapsam :** Bilgi güvenliği sadece BT servisini ilgilendiren bir faaliyet değildir. Kurumun tüm paydaşlarını ilgilendirir. Kurumlar veri güvenliği politikasının kapsamını kendisi belirler. Kapsam, tüm kurum olabileceği gibi bazı grup veriler veya bazı birimler öncellenebilir.
**Prosedürler :** Kurumlar bilgi güvenliği sisteminin oluşturulması için, öncelikle bir "bilgi güvenliği komisyonu" kurar. Komisyonca belirlenene politika ve prosedürler idare tarafından onaylanmış olmalıdır.
**Kontrol / Denetim:** Güvenlik politikalarının prosedürlere uygun yürüyüp yürümediği en az altı ayda bir kontrol edilir, denetlenir. Eksik kalan yönlere ilişkin denetim raporları düzenlenir.

*Bilgi güvenliğinin üç temel hedefi vardır.*
**Gizlilik (Confidentiality) :** Bilgi güvenliği üç unsuru hedefler: bilginin yetkisiz kişilerin erişimine kapalı olması, yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.
**Bütünlük (Integrity) :** Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunması, kazara veya kasıtlı olarak bozulmamasıdır.
**Kullanılabilirlik (Availability) :** Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır.

# BELGE GÜVENLİĞİ

**Doğukan Güran**
*dogukan.guran@ingbank.com.tr*
*İngBank Kıdemli Yazılım Mühendisi*

Her belgenin, ya internete açık ya da şirket içi digital ortamlarda kaydedilmesi sonucunda bu bilgilere erişim çok önem arz etmektedir. Kim? Ne zaman? Nasıl? Neden? Nerede? gibi soruların her birine anlamlı cevaplar verilmediği sürece belgelerin güvende olmadıkları kanısına varılabilir. Peki en ideal şekilde bilgiler nasıl saklanmalıdır. Nasıl sorgulanmalıdır?

# 21İNCİ YÜZYILDA BELGE VE BİLGİ GÜVENLİĞİ

**Abdullah Raşit Gülhan**
*argulhan@gmail.com*
*SinerjiTürk Vakfı, Verasoft*

Hemen herşeyin "online&connected" (çevrim içi ve bağlantılı) olduğu günümüzde geçmişi bugünlere, bugünleri geleceğe taşıyan belgelerin güvenli saklanması, içeriğinin değişmediğinden emin olunması sadece kamu arşivciliği açısından değil, kamu ile birlikte her sektör için de aynı şekilde önem arz etmektedir.

Bu konuşmada; Belge yönetimi konusu ile bilişimsiz hayatın düşünülemediği günümüzde bilgi güvenliğine de ‘Belge güvenliği’ açısından yaklaşılarak bir değerlendirme yapılmaya çalışılacaktır.

# KURUMSAL HAFIZANIN KORUNMASINDA SİSTEMİN ÖNEMİ

**Yrd.Doç.Dr. Erkan ÖZHAN**
*erkanozhan@gmail.com*
*Namık Kemal Üniversitesi, Mühendislik Fakültesi*

Bu çalışmada kurumsal hafızanın korunmasında sistemin önemi anlatılmaya çalışılmıştır. Günümüzde özellikle elektronik ortamda tutulan kurumsal bilgilerin miktarı devasa boyutlara ulaşmıştır. Kurumlar, bilgi ve belge yönetiminde kullanılan donanım ve yazılım temelli sistemleri sıklıkla kullanmakta hatta bunlar kurumların hayati parçası haline gelmektedir. Bilgi kurumlar için önemli bir servettir. Kurum içerisinde geçmişten gelen bilgi havuzu -ki kurumsal hafıza olarak ta isimlendirilir, belirli bir sistematiği ve esnekliği olan koruma sistemleri tarafından yönetilmelidir. Uygun olmayan koruma, depolama sistemleri, bilginin normal kullanılmasını zorlaştırabileceği gibi, yetkisiz erişimlere, kullanımlara, bilginin bozulmasına vb. neden olabilir. Bu çalışmanın birinci bölümünde kurumsal hafızayı oluşturan ana unsurlar, ikinci bölümde dijital koruma sistemlerinin önemi ve bu sistemlerin çalışma prensipleri, üçüncü bölümde koruma sistemini tehdit eden unsurlar ve son bölümde ise çözüm önerileri yer almıştır.

# ELEKTRONİK ARŞİVLERDE SÜRDÜRÜLEBİLİRLİK STRATEJİLERİ

**Prof. Dr. Hamza Kandur**
kandur@marmara.edu.tr
*Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü*

Elektronik belgelerin hukuki açıdan fiziksel belgeler ile eşdeğer sayılmasının üzerinden 10 yıldan fazla zaman geçti. Elektronik imza kanununun 23 Temmuz 2004 tarihinde yürürlüğe girmesi ile kurumların ürettikleri belgeleri elektronik ortamda imzalama, kullanma ve arşivlemesinin önü açılmış oldu. Yine ilk olarak 2007 yılında yürürlüğe giren TS13298 standardının 2008/16 sayılı Başbakanlık genelgesi ile tüm kamu kurumlarında zorunlu hale getirilmesi ile kamu kurumlarının belge yönetimi alanındaki uygulamaları başka bir boyut kazanmış oldu.

On yılı aşkın bir süredir elektronik ortamda işlem yapan ve bu işlemin belgesini elektronik ortamda üreten kurumlar, bu belgeleri kurum arşivlerine veya Devlet Arşivlerine transfer etmek durumuna gelmiştir. Elektronik belgelerin arşiv formatına dönüştürülmesi, uzun süreli saklanması, transferi ve erişimini sağlamak yeni bir meydan okuma olarak kamu kurumlarının önündedir. Kurumların üretmiş oldukları elektronik belgelerin sürdürülebilir ortamlarda araştırmacılarla buluşmasını sağlayacak stratejiler geliştirmek durumundadır. Bu bağlamda kurumların teknolojik, yönetimsel ve süreç tabanlı dönüşümleri gerçekleştirme ihtiyacı vardır. Bu çalışma bu ihtiyaçları analiz etme ve sürdürülebilir elektronik arşivler için bir yönetim modeli sunmayı amaçlamaktadır.

# ELEKTRONİK ORTAMDA BELGELERİN UZUN SÜRE KORUNMASI, GÜVENLİĞİ VE ERİŞİM ETKİNLİĞİNİN ARTIRILMASINDA ÜSTVERİELEMANLARININ ÖNEMİ; SORUNLAR VE ÇÖZÜM ARAYIŞLARI

**Prof.Dr. Özgür KÜLCÜ**
ozgurkulcu@gmail.com
*Hacettepe Üniversitesi, Bilgi ve Belge Yönetimi Bölümü*

Elektronik ortamda uzun süre korunmasında öncelik gerektiren kültür kaynakları genel olarak arşivler, kütüphaneler, müzelerde, araştırma merkezlerinde yer alan tarihi belgeler, yazmalar, kitaplar, efemeral dokümanlar, görsel ve işitsel malzemeler, geçmişe ait bilgi veren algı yaratan elektronik ortamda her türlü içerikten oluşmaktadır. Geniş bir çerçevede tanımlananın ve bilgi içerikli kültürel mirasın bir parçası olarak değerlendirilebilecek elektronik kaynakların ortak noktası; gelecek kararları, hareketleri ve algıları yönlendirebilecek geçmişe ait birinci el bilgi içermesidir. Bu çerçevede bireysel ve toplumsal yaşamın doğal akışı içerisinde oluşan içerik, idari ve araştırma değeri göz önüne alınarak saklanmakta ve sistematik olarak yönetilmektedir. Bilgi içerikli kültürel miras geleneksel olarak basılı formlarda üretilirken, özellikle 1990'lı yıllarla birlikte giderek daha fazla oranda elektronik ortamda oluşturulmaya ya da basılı ortamdan elektronik ortama aktarılmaya başlanmıştır. 2000'li yıllarla birlikte bilgi içeriğinin yönetimi ve entegrasyonu üzerine gelişmeler de eklendiğinde kültürel mirasın yönetiminde yeni meydan okumaların son derece güçlenmiştir. Bu çerçevede çalışmada geleneksel olarak arşivler, kütüphaneler, müzeler ve araştırma merkezlerinde birbirlerinden farklı ortamlarda, farklı tekniklerle hizmete sunulan kültürel mirasın, teknolojik olanaklar ve yeni yaklaşımlarla nasıl bir arada ele alınmaya başlandığı değerlendirilmektedir. Bahsi geçen farklı kaynaklardan gelen elektronik içeriğin entegrasyonu çalışmaları kapsamındastandartlaşmış ve eşgüdümlü çalışmalara uygun üstverialanlarının geliştirilmesi son derece önemlidir. Dijital kültürel miras kapsamındaki içeriğe erişim, içeriğin korunması vegüvenliğinde temel rol içeriği tüm yönleriyle tanımlayanüstveri elemanlarıdır. Bu çerçevede çalışmada dünyada ve ülkemizde kültür kaynaklarının elektronik ortamda tanımlanmasına dönük üstveri elemanlarının kullanım koşullar karşılaştırmalı olarak incelenmekte, sorunlar tartışılmaktadır, çözüm önerileri sunulmaktadır.

# ENDÜSTRİ 4.0 BAĞLAMINDA SİBER GÜVENLİK VE ARŞİVCİLİĞE YANSIMALARI

**Arş. Gör. Dr. Bahattin YALÇINKAYA**
bahakaya@gmail.com
*Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü*

Günümüz endüstrisinde Rönesans benzeri bir devrim yaşandığı konusunda uzmanlar hem fikirler. Kurum ve kuruluşlar bu dönüşümde yeni bir dünya geleceği ile endüstri 4.0'la alakalı yatırımlarını ve teknoloji güncellemelerini yapmaya devam ediyorlar. Özellikle ön plana çıkan konuların başından kıymetli bilgi olarak adlandırılabilecek kurumsal hafızanın geleceğe yönelik olarak kullanımı söz konusu yatıyor. Ancak tüm dünyada şirketlerin ve kurumların % 40'ında kurumsal bilginin sızdırıldığı konusu bilinmektedir. Özellikle veri işleme ile ilgili teknolojinin gelişimi bloklar halinde duran ve işlenmediği zaman bir anlam ifade etmeyen verilerin bir değer olarak korunması gerektiğini ortaya koymaya başladı. Veri güvenliği, güvenirliği, kişisel veriler, kurumsal hafıza, arşivler gibi kavramların bu bağlamda yeniden alınması gerekliliği kaçınılmaz bir hal almaya başladı.

Bu çalışmada endüstri 4.0'ın getirdikleri ile siber güvenlik kavramının arşivler açısından nasıl bir etki yapacağı konusu ele alınacaktır. Kişisel verilerin ve kurumsal verilerin manipülasyona uğraması, elektronik arşivlere yapılacak siber saldırıların ülkelerin güvenliğini nasıl tehdit ettiği konusu üzerinde durulacaktır. Kötü niyetli insanlar tarafından arşivlerde bulunan nitelikli bilgilerin (finansal, sağlık vb.) nasıl ticari amaçlar için kullanılacağı konusu gözler önüne serilecektir. Endüstri 4.0'la birlikte gerçekleşen devrimin arşivciler açısından özellikle elektronik ortamda hangi tedbirleri almaları gerektiği konusu tartışılacaktır.

**Anahtar Kelimeler:** Endüstri 4.0, gizlilik, siber güvenlik, kişisel veriler, kurumsal hafıza

# KİŞİSEL VERİLERİNİZ NE KADAR GÜVENDE? BİLGİ GÜVENLİĞİ KAPSAMINDA BİR DEĞERLENDİRME

**Yrd.Doç.Dr. Türkay Henkoğlu**
*turkay.henkoglu@adu.edu.tr*
*Adnan Menderes Üniversitesi, Yönetim Bilişim Sistemleri Bölümü*

Elektronik ortamda bulunan bilgi varlıklarındaki çeşitliliğin artışına bağlı olarak veri depolama ortamlarına yönelik güvenlik endişelerinin artması ve elektronik ortamda daha etkin bilgi yönetimini için kullanılan bilişim teknolojilerinin hedef haline gelmesi, günümüzde bilgi güvenliğinin sağlanması konusuna daha geniş bir çerçevede ve sistematik olarak bakmayı zorunlu hale getirmektedir. Özellikle kişisel verilerin korunması konusu hukuksal yönleriyle değerlendirildiğinde, bilginin gizliliğinin korunmasından farklı olarak daha etkin ve kapsamlı koruma önlemlerinin alınmasını gerektirmektedir. Bu konuda yapılan araştırmalar, hukuksal düzenlemelerin dikkate alınmadığı Türkiye'de bilgi güvenliğinin sağlanmasına yönelik önlemlerin, kişisel hak ve özgürlüğün korunmasına ilişkin risklerin artmasına neden olduğunu göstermektedir.

Bilgi saklama/depolama ve arşiv işlemlerinin "ayıklama" yerine bilginin elektronik ortamda doğuşu ile başlaması, klasik bilgi güvenliği anlayışındaki değişimi ve farklı disiplinlerin de bu konuya neden dâhil olması gerektiğini açıklamaktadır. Bilginin işlendiği/üretildiği andan imha edilmesine kadar olan süreçte yer alan tüm aktörlerin, bilgi güvenliğinin sağlanması konusunda sorumlulukları bulunmaktadır. Çalışmada, kişisel verilerin korunması çerçevesinde bilgi güvenliğinin sağlanmasına yönelik olarak uygulamada yapılan yanlışlar ve bu konudaki sorumluluklara değinilerek, teknik ve hukuksal açıdan ne gibi risklerle karşı karşıya olunduğuna dikkat çekilmesi amaçlanmaktadır. Uygulamadaki risklerin değerlendirilmesi ve daha geniş çerçevede sorumlulukların belirlenmesi ile birlikte, bilginin gizliliğinin ve kişisel hakların birlikte korunması mümkün olabilecektir.

# KİŞİSEL VERİLERİN KORUNMASI HAKKINDA KANUN KURUMLARA HANGİ YÜKÜMLÜLÜKLERİ GETİRİYOR?

**Av. Ceyda AKAYDIN CİMİLLİ**
*ceyda@ceydaakaydin.av.tr*

Kişisel verilerin korunması hakkında kanun tarihinde yürürlüğe girdi. Kabul tarihine kadar pek çok taslak hazırlandı, çeşitli kurum ve kuruluşlardan çok farklı talep ve yorumlar aldı. Yasanın çıkma nedeni temel olarak Avrupa Birliği uyum çalışmaları ve özellikle yargı kurumlarının veri taleplerinin ülkemizde uygun düzenlemelerin bulunmaması nedeniyle veri paylaşmaması nedeniyle yaşanan zorluklar. Yasanın kabul edilmesinin önündeki en büyük engel ise en büyüğünden en küçüğüne kadar tüm kurumların bu düzenleme ile gelecek ek yükümlülükler ve bunların getireceği maliyetler nedeniyle direnişi ve tabii ki konunun pazarlama amaçlı veri toplanması ve paylaşımı açısından pek çok kurumun hemen hemen tüm dijital pazarlama faaliyetlerinin temel kaynağı olan verinin gözden geçirilmesi ve hatta imhası gerekliliğinin şirketlerin tepkisine neden olması.

Her ne kadar ilgili yönetmelik henüz çıkmamış olduğundan uygulamada pek çok konu halen belirsiz olsa da, yasanın yürürlüğe girmesi ile tüm kurumlarda süreçleri yasaya uygun hale getirmek için hummalı bir çalışma başladı. Bu yazıda öncelikle yasanın getirdiği temel değişiklikleri, sonrasında da özellikle insan kaynakları ve müşteri ve tedarikçi ilişkileri süreçlerinde yapılması gereken temel düzenlemeleri inceleyeceğiz.

## Kanunun gerekçesi ve temel ilkeleri

Bir yasanın uygulamasına ilişkin olarak boşluklar olması halinde yani yoruma ihtiyaç olması durumunda yasa koyucunun bu yasayı çıkartmaktaki amacını ve yasanın genel ilkelerini incelemek gerekir.

Öncelikle Türkiye 28 Ocak 1981 tarihinde imzalanan "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" yi imzalamıştır. Bu sözleşme taraf ülkelere yerel mevzuatlarında kişisel verilerin korunmasına ilişkin düzenlemeler getirme yükümlülüğü getirmektedir. Ayrıca AB üyeliği için uyum çalışmaları kapsamında da bu mevzuat değişikliği zorunlu hale gelmiştir. Ayrıca son yıllarda siyaset alanında çok yer alan dinlemeler ve izinsiz kayıtlar da yasanın çıkarılmasında önemli rol oynamıştır. Gerek ilgili meclis tutanakları incelenerek, gerekse kanunun gerekçesi incelendiğinde bu husus açıkça görülecektir. 2016 yılında Türk Ceza Kanunu 'nda kişisel verilerin korunmasına ilişkin cezai düzenlemeler getirilmiş ve son olarak da 26/04/2016 tarihinde anılan yasa yürürlüğe girmiştir. Yasanın gecikmesindeki temel neden de özellikle doğrudan pazarlama ve tüketiciye yönelik ticari faaliyetler yapan kuruluşların direnci olmuştur.

Yasanın kişisel verilerin işlenmesi için getirdiği temel ilkeler:

a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan
süre kadar muhafaza edilmedir.

**Kişisel verinin tanımı ve türleri**

Yasa kişisel veriyi "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlamıştır. Bu tanımlama yasadan önce kişisel verinin ne olduğu, hangi bilgilerin kişisel veri sayılacağı yönünde yapılan tartışmaları da sonlandırmıştır. Bu düzenleme öncesinde kişisel veri sadece Türk Ceza Kanunu'nda Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler kişisel veri olarak tanımlanmış ve bu verilerin hukuka aykırı olarak kaydedilmesinin yaptırımı 6 aydan 3 yıla kadar hapis cezası olarak tanımlanmıştı. Ancak, burada tanımlananlar dışındaki veriler, örneğin kişinin adresi, dış görünüşü, iletişim bilgileri, medeni hali gibi veriler bu madde kapsamına girmediğinden bu verilerin korunmasına ilişkin bir düzenleme yoktu.

6563 sayılı elektronik ticaretin düzenlenmesi hakkında kanun kişisel verilerin korunmasından hizmet sağlayıcıyı sorumlu tutmuş ve kişisel verilerin ilgili kişilerin onayı olmaksızın paylaşılamayacağını düzenlemişse de, kişisel veriyi tanımlamamıştır. Bunun yanında sosyal güvenlik mevzuatı, Noterlik Kanunu, Türk Ticaret Kanunu, Sermaye Piyasaları Mevzuatı, Elektronik Haberleşme Kanunu gibi çeşitli mevzuat kişisel verilerin korunması ile ilgili tedbirlerin alınmasını düzenlemişse de, kişisel veri tanımı bu mevzuatta da yapılmamıştır. Bu nedenle yasanın çıkışından önce nelerin kişisel veri sayılması gerektiği konusunda çeşitli tartışmalar yaşanmış, yasanın yürürlüğe girmesi ile bu tartışmalar büyük ölçüde sona ermiştir.

Yasa kişisel veriyi "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımladıktan sonra "özel nitelikte kişisel veri" tanımı yapmıştır. Özel nitelikte kişisel veri ise yasada kişinin rkı, 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 özel nitelikli kişisel veridir.

**Kişisel Verilerin Korunması Hakkında Kanun kurumlara hangi yükümlülükleri getiriyor**

**Veri sorumlusu belirleme ve bildirme yükümlülüğü**

Yeni çıkan kanun öncelikle kişisel veri işleyen kurumlara bir kişisel veri koruma yetkilisi belirlenmesi ve bu yetkilinin kurula bildirilmesi yükümlülüğünü getiriyor. Bireysel müşterisi olamayan kurumlar için bile çalışanlarının verisini işledikleri düşünülünce tüm kurumların ve şirketlerin bu sorumluyu belirlemesi gerektiği açıktır. Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar para cezası öngörülmüştür. Cezanın uygulanmaya başlama tarihi 01/10/2016 dır. Bu güne kadar kurul oluşturulmuş olmadığından bildirimin yapılması mümkün değilse de, kurumların en azından alacakları bir karar ile sorumluyu belirlemeleri ve

ilan etmeleri cezai sorumluluktan kurtulmak açısından şu anda yerine getirebilecekleri sorumluluklarını yerine getirmelerini sağlayacaktır.

**Veri sahibinin açık rızası olmadan veri işlememe yükümlülüğü**

Yasa veri işlenmesi için veri sahibinin açık rızasının alınmasını zorunlu tutmuştur. Henüz yönetmelik çıkmamış olduğundan her ne kadar rıza alınmasına ilişkin detaylı tanımlama yoksa da, rızanın veri sahibinin neye rıza gösterdiğini net olarak göreceği şekilde örneğin ayrı bir beyan olarak ve bir sözleşme içerisinde veya uzun bir metin içinde değil de, veri sahibinin neye rıza gösterdiğini net olarak göreceği şekilde ayrı bir beyan olarak alınması gerektiğini düşünmekteyim. Yasa beyanın alınması için bir yöntem göstermemiştir. Yayınlanacak olan yönetmelikte özel bir yöntem düzenlemesi yer alırsa tabii ki bu yönteme uygun rıza alınması gerekecektir. Eğer özel bir düzenleme yapılmazsa, açık rıza alındığının ispatının yükümlülüğü veri sorumlusunda olduğundan kurumların ileride aksi bir iddia olduğunda rıza alındığını ispatlayabilecek bir sistem ile alınması gerekir. Burada ıslak imzalı veya nitelikli elektronik imzalı rızanın bu yükümlülüğün yerine getirildiğini ispatlayacağı açıktır. Diğer elektronik sistemlerle alınan rızalar açısından ise ispat imkanı incelenerek karar verilmesi gerekir.

Yasa bu yükümlülüğün istisnası olarak şu durumlarda açık rıza olmasa dahi kişisel verilerin işlenebileceğini belirtmiştir:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

**Veri sahibinin açık rızası olmadan veriyi paylaşmama yükümlülüğü**

Yasa verinin paylaşılması için de veri sahibinin ayrıca açık rızasının alınmasını zorunlu tutmuştur. Bu nedenle verinin paylaşılması için işleme konusunda izin yeterli olmayacak olup yine işleme için alınacak rıza gibi ayrı bir rıza alınması gerektiği görüşündeyim.

**Aydınlatma yükümlülüğü**

Veri sahibi her zaman veri sorumlusuna başvurarak kendisi hakkında hangi verilerin işlendiğini, bu verilerin paylaşılıp paylaşılmadığını ve amacına uygun kullanılıp kullanılmadığını öğrenme hakkı vardır. aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar para cezası öngörülmüştür.

**Kişisel verilerin talep halinde düzeltilmesi, yok edilmesi veya anonim hale getirilmesi yükümlülüğü**

Yasaya uygun olarak işlenmiş olsa dahi, işlenmesini gerektiren nedenin ortadan kalması durumunda re'sen veya veri sahibinin talebi üzerine veri sorumlusu tarafından kişisel veriler silinmeli, yok edilmeli veya imha edilmelidir. Bu yükümlülüğe uymayanlar 5237 sayılı Türk Ceza Kanunu'nun 138 inci maddesine göre altı aydan bir yıla kadar hapis cezası ile cezalandırılırlar.

**Yasanın yürürlüğe girmesinden önce işlemiş olan kişisel verilere ilişkin yükümlülükler**

"Yasa Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir." Düzenlemesini getirmiştir. Dolayısıyla yasadan önce yasaya uygun şekilde rıza alınmadan işlenmiş kişisel verilerin işlenmesi veya paylaşılması için yasada belirtilen şekilde rıza alınması gerekmektedir. Bu şekilde uygun hale getirilemeyen kişisel veriler derhal silinmeli, yok edilmeli veya anonim hale getirilmelidir.