
BELEDİYELERDE VERİ YÖNETİMİNDE

KİŞİSEL VERİLERİN KORUNMASI KANUNUNA UYUM SÜRECİ RAPORU



BELEDİYELERDE VERİ YÖNETİMİNDE

KİŞİSEL VERİLERİN KORUNMASI KANUNUNA UYUM SÜRECİ RAPORU

Mart 2018



İÇİNDEKİLER

Giriş	5
Hukuki Altyapı ve Mevcut Durum	9
Hangi veriler 6698 sayılı Kişisel Verileri Koruma Kanunu kapsamındadır?	9
Belediyelerin hangi departmanları bu kanunla ilgilidir?.....	9
Kanun ve yönetmelikler ne zaman yürürlüğe girmiştir?	10
Kanundaki yükümlüklerini yerine getirmeyenlere verilecek idari para cezaları nelerdir?	10
Kanundaki yükümlülüklerini yerine getirmeyenlere Türk Ceza Kanunu kapsamında verilecek cezalar nelerdir?	10
Belediyeleri de ilgilendiren Kurul Kararı.....	11
Uyum Sürecinde Yapılması Gerekenler	13
Mevcut Durum Analizi Yapılması	13
Veri Politikalarının Oluşturulması.....	14
Yetki Matrisi Çalışmalarının Yapılması	14
Veri Paylaşım Şeması Oluşturulması	14
Kişisel Veri Envanterinin Hazırlanması	15
Kişisel Veri İşleme Sisteminde Bulunması Gerekenlerin Listesi	15
Sözleşmelerin Düzenlenmesi	16
Açık Rıza, Aydınlatma ve Bilgilendirme Metinlerinin Düzenlenmesi	16
Verbis Bildirim Sitemine Geçilmesi	17
Kurumsal İletişimin Güçlendirilmesi	17
Eğitim ve Farkındalık Faaliyetlerinin Düzenlenmesi	17
Teknik Veri Koruma Önlemlerinin Geliştirilmesi.....	18
Kişisel Veri Uyumsuzlukları ve Risk Listesi Oluşturulması.....	19
Veri Silme, Periyodik İmha ve Anonim Hale Getirme Uygulamalarının Belirlenmesi	19
Kişisel Verilerin Azaltılması	20
Sonuç ve Değerlendirme Raporunun Hazırlanması.....	20
Sonuç	23
Rapora Katkı Sağlayanlar	27



GİRİŞ

1975 yılında kurulan Marmara Belediyeler Birliđi (MBB), bölgesel ölçekte, Türkiye'nin en köklü ve kapsamlı belediyeler birliđidir. MBB, 6'sı büyükşehir olmak üzere 13 ilde faaliyet göstermektedir: Balıkesir, Bilecik, Bolu, Bursa, Çanakkale, Düzce, Edirne, İstanbul, Kırklareli, Kocaeli, Sakarya, Tekirdađ ve Yalova. Marmara Bölgesi'ndeki belediyelerin üye olduđu MBB, belediyelere yönelik eğitim hizmetlerinin yanında hukuk, finans, insan kaynakları, stratejik planlama gibi alanlarda yerel yönetimlere danışmanlık da yapmaktadır. MBB, Türkiye'de demokratik yerel yönetim hareketinin gelişmesi, belediyelerin yetki ve kaynaklarının artırılması, yerel yönetimlerde çevre bilincinin geliştirilmesi, belediyelerin ortak sorunlarına işbirliđi içinde çözüm bulunması, belediyelerin uluslararası platformlarda temsili gibi konularda öncülük yapmaktadır. MBB kuruluşundan bu yana, deđişik siyasi partilerden seçilmiş belediye başkanları ve meclis üyeleri arasında, uzlaşma ve birlikte çalışma kültürünün oluşmasında ve belediyeler arasında işbirliđinin gelişmesinde önemli roller üstlenmiştir.

MBB, Türkiye'de ve dünyada meydana gelen güncel deđişiklikleri yakından takip eden dinamik ve tecrübeli ekibi ile yerel yönetimlerin bu alanlardaki sorunlarını tespit etmekte ve bunlara ilişkin çözüm önerileri geliştirmektedir. MBB teknik, hukuk, finans ve yönetim alanlarında hazırlamış olduđu fizibilite ve çalıştay raporları, düzenlediđi eğitimler ve sunduđu kurumsal gelişim hizmetlerinde bu anlamda öncü bir bölgesel birlik olma özelliđini taşımaktadır.

Bu amaçla kurulan MBB Bilgi Teknolojileri Platformu, Marmara Belediyeler Birliđine üye yerel yönetimler arasında bilgi ve tecrübe paylaşımında bulunmak, ortak sorunlara çözüm bulmak ve var olan yapıyı geliştirmektedir. Çađımızın bilgi çađı olması ve teknolojinin yoğun kullanımını gerektirmesinden dolayı, günlük yaşam ve iş hayatı deđişmiş doğru ve sistematik bilgiye erişme ihtiyacı daha da belirginleşmiştir. Bilgi teknolojisinin amacı edinilen bu doğru bilgiyi toplamak, depolamak, korumak, işlemek ve kullanıcının hizmetine sunmaktır. Bu hizmeti sağlarken de gerek yazılım gerekse de donanım alanında sorunlarla karşılaşılmakta veya kullanılan yazılım ve donanımın geliştirilmesine ihtiyaç duyulmaktadır. Bilgi Teknolojileri Platformu gerek kamu sektörü gerekse özel sektörle işbirliđi halinde ilgili kişi ve kurumları bir araya getirmek, gerekli eğitimleri sağlamak ve paydaşlarıyla istişarede bulunarak teknolojiadaki gelişimleri yakından takip etmek gibi görevleri yürütmektedir.

Bilgi Teknolojileri Koordinatörlüğü olarak, son zamanlarda yaşanan gelişmelere uygun olarak gündemimiz, kişisel verilerin işlenmesinde elde edilen verilerin gelişen teknoloji ve yaygın internet kullanımı ile kolaylıkla çeşitli platformlara aktarılabilmesi, yetkisiz ya da kötü niyetli kişilerin eline geçmesi ihtimalini arttırdığından bu verilerin ne şekilde korunması gerektiğinin tespiti olmuştur.

Buna ek olarak, Belediye Kanununa eklenen geçici madde 10'da, belediyelerin, e-belediye bilgi sisteminin kurulduğuna dair bildirimini İçişleri Bakanlığı tarafından yapılmasından itibaren e-Belediye bilgi sistemi ile ilgili çalışmalarını bir yıl içinde tamamlayacakları hüküm altına alınmaktadır. 15/2/2018 tarihli ve 7099 sayılı Kanunun 17'nci maddesi ile eklenen bu madde, aynı Kanunun 34'üncü maddesi uyarınca Resmî Gazete'de yayımlandığı 10/3/2018 tarihinden 6 ay sonra yürürlüğe girecektir. Buradan hareketle platform üyeleri tarafından talep edilen bu verilerin neler olduğu ve yönetiminin ne şekilde olacağına dair ihtiyacı karşılamak üzere MBB Bilgi Teknolojileri Platformu ve MBB Hukuk Platformunun üyelerinden 32 katılımcı, bu konuda belediyelere yol göstermesi amacı ile Kocaeli, Karatepe'de tüm gün süren bir eğitim semineri sonucu bir yol haritası belirlemişler ve bunu bir rapor haline getirmişlerdir.

Bu raporda öncelikle belediyelerimizde veri yönetimine dayanak teşkil eden 6698 sayılı Kişisel Verilerin Korunması Kanunu, bu kanuna bağlı yönetmelikler ve ilgili kanun maddeleri ile kanuna göre yükümlülüklerini yerine getirmeyenlere uygulanacak idari para cezaları ve TCK kapsamındaki cezalar tablolar halinde belirtilmiştir. Kanuna uyum sürecinde yapılması gerekenler, temel konu başlıkları alt maddeler oluşturularak sıralanmıştır. Sonuç ve Değerlendirme kısmında ise belediyelerimiz tarafından bu konuda nihai olarak yapılması gerekenler net bir şekilde ifade edilmeye çalışılmıştır. Bu rapor, ilgili kanuni düzenlemeler ekseninde üye belediyelerimizin veri yönetiminde ne şekilde hareket edeceklerine dair bir rehber niteliğinde hazırlanmıştır.

Bu raporun hazırlanmasında emeği geçen, mesaisini tüm gün süren bu çalışmaya özgüleyen başta Eralp Danışmanlık ve ekibine, MBB Hukuk Platformuna ve tüm katılımcılarımıza çok teşekkür eder, yerel yönetimleri yakından ilgilendiren bu konuda belediyelerimizin ilgili birimlerine faydalı olmasını temenni ederiz.





HUKUKİ ALTYAPI VE MEVCUT DURUM

Temel bir insan hakkı olan kişisel verilerin korunması hakkı, özel hayatın gizliliği ile doğrudan ilişkilidir. Üçüncü kişilerin eline geçmesinde sakınca bulunan bu verilerin korunması gerekliliği, hem kamu kurumlarını hem de özel kurumları ilgilendirmektedir. Bu sebeple, kişisel verilerin korunması konusu ilk olarak 5237 sayılı Türk Ceza Kanununda 135 ve 140. maddeler arasında düzenlenmiştir. Sonrasında Anayasada 2010 yılında yapılan değişiklikle kişisel verilerin korunması anayasal güvence altına alınmıştır. 7 Nisan 2016 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu bu kapsamdaki temel düzenleme olmuştur.

■ Hangi veriler 6698 sayılı Kişisel Verileri Koruma Kanunu kapsamındadır?

6698 Sayılı Kişisel Verilerin Korunması Kanunu hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır.

Müşterilerin ve personellerin adı, soyadı, cep telefonu, e-posta, TC kimlik numarası, adres, fotoğraf, kimlik fotokopisi ve benzeri diğer bilgilerini tutan ve işleyen belediyeler bu kapsamdadır.

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 özel nitelikli kişisel veridir ve ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

■ Belediyelerin hangi departmanları bu kanunla ilgilidir?

Kişisel Verilerin Korunması Kanunu hükümleri belediyelerde başta belediye başkanı, daire başkanları, müdürleri ve şeflerini ilgilendirmekle birlikte belediye bünyesinde çalışan hukuk müşavirleri, avukatlar, insan kaynakları (İK) yöneticileri ve personeli, bilgi işlem merkezi (IT) yöneticileri ve personeli, halka ilişkiler yöneticileri ve personeli, risk bölüm yöneticileri ve personelinin iş tanımlarıyla yakından ilgilidir.

■ Kanun ve yönetmelikler ne zaman yürürlüğe girmiştir?

NO	KANUN - YÖNETMELİK ADI	RESMİ GAZETE TARİHİ	YÜRÜRLÜK TARİHİ
1	6698 sayılı Kişisel Verilerin Korunması Kanunu (Madde 1,2,3,4,5,6,7,10,12,19 ve sonrası)	07.04.2016 - 29677	07.04.2016
2	6698 sayılı Kişisel Verilerin Korunması Kanunu (Madde 8,9,11,13,14,15,16,17,18)	07.04.2016 - 29677	07.10.2016
3	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik	28.10.2017 - 30224	01.01.2018
4	Veri Sorumluları Sicili Hakkında Yönetmelik	30.12.2017-30286	01.01.2018

■ Kanundaki yükümlülüklerini yerine getirmeyenlere verilecek idari para cezaları nelerdir?

NO	EYLEM	YASAL DAYANAK	PARA CEZASI
1	Aydınlatma yükümlülüğünü yerine getirmeyenler	KVKK madde 18/1-a	5.000 TL - 100.000 TL
2	Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler	KVKK madde 18/1-b	15.000 TL - 1.000.000 TL
3	Kurul tarafından verilen kararları yerine getirmeyenler	KVKK madde 18/1-c	25.000 TL - 1.000.000 TL
4	Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler	KVKK madde 18/1-ç	20.000 TL - 1.000.000 TL

■ Kanundaki yükümlülüklerini yerine getirmeyenlere Türk Ceza Kanunu kapsamında verilecek cezalar nelerdir?

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda madde 135, 136, 137, 138, 139 ve 140 hükümleri uygulanır. Bu Kanunun madde 7 hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138'inci maddesine göre cezalandırılır.

NO	EYLEM	MADDE	CEZA
1	Kişisel verileri hukuka aykırı olarak kaydetmek	TCK madde 135/1	Bir yıldan üç yıla kadar hapis cezası
2	Kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verileri hukuka aykırı olarak kaydetmek	TCK madde 135/2	Bir yıldan üç yıla kadar hapis cezası yarı oranında artırılır.
3	Kişisel verileri, hukuka aykırı olarak bir başkasına vermek yaymak veya ele geçirmek	TCK Madde 136	İki yıldan dört yıla kadar hapis cezası
4	Bu suçlar; Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenirse	TCK Madde 137	Yukarıda verilecek cezalar yarı oranında artırılır.
5	Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemesi	TCK Madde 138/1	Bir yıldan iki yıla kadar hapis cezası
	Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması	TCK Madde 138/2	Verilecek ceza bir kat artırılır.

■ Belediyeleri de İlgilendiren Kurul Kararı

Kişisel Verileri Koruma Kurulu'nun banka ve sağlık sektörüne özgü aldığı ilke kararlarından biri 25.01.2018 tarihli resmî gazetede yayımlanmıştır.

Banko, Gişe, Masa Gibi Birden Fazla Çalışan ile Bitişik Düzende Hizmet Veren Kurumlar Hakkında Kişisel Verileri Koruma Kurulu 2017/62 Sayılı İlke Kararına göre, banko, gişe ve masa gibi vatandaşa hizmet sunulan alanlarda yaşanan kişisel veri güvenliği ihlallerine ilişkin olarak Kişisel Verileri Koruma Kurumu'na intikal eden ihbarlar değerlendirilmiş ve uygulamada yaşanan problemlerin önüne geçilmesi amacıyla aşağıdaki karar alınmıştır.

2017/62 Sayılı Kişisel Verileri Koruma Kurulu Kararı'nda, bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşları, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12'nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri alacaktır.



UYUM SÜRECİNDE YAPILMASI GEREKENLER

6698 Sayılı Kişisel Verilerin Korunması Kanun ve ilgili mevzuat kapsamında belediye bünyesinde yapılması gerekenleri tespit etmek ve uyum sürecini derhal başlatmak gerekmektedir.

Uyum süreci çalışmalarının zaman ve bütçesinin doğru tespit edilerek verimli kullanılabilmesi için belediye merkezinde ilgili departman yöneticilerinin katılacağı 3 saatlik "Kişisel Verilerin Korunması Temel Bilgiler Farkındalık Eğitimi" eğitimi ve sonrasında Hukuk ve Bilgi İşlem Birimlerinin katılacağı 3 saatlik "Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Temel Eğitimi" alınmasının belediye çalışanları açısından faydalı olacağı değerlendirilmektedir.

1 | Mevcut Durum Analizi Yapılması

- Üst yönetim ile görüşme yapılması,
- Üst yönetimin desteğinin alınması,
- Şirket proje yöneticilerinin belirlenmesi ve proje ekibinin kurulması,
- Kurumun iç organizasyonu, personel sayısı, lokasyon ve iş ortaklarının vb. belirlenmesi ve işin kapsamının netleştirilmesi,
- Proje paydaşları ve iş birimleri ile görüşmeler yapılması,
- Kuruluşun iş süreçlerinin ve sahiplerinin analiz edilmesi,
- Kişisel veri işleyen anahtar faaliyetlerin anlaşılması gerekmektedir.

IT ve iş birimleri ile yapılan ilk görüşmelerden sonra kanuna uyum süreci konusunda olması gereken ile mevcut durum arasındaki farkı görmek için GAP Analiz Raporu hazırlanmalıdır.

2 | Veri Politikalarının Oluşturulması

- Kişisel Veri Toplama, İşleme, Saklama ve Erişim Politikası,
- Kişisel Veri Silme, Yok Etme, İmha ve Anonimleştirme Politikası,

- Kişisel Verilerin Kullanılması ve Paylaşılması Politikası,
- Kurumsal Bilgi Güvenliği Politikası.

3 | Yetki Matrisi Çalışmalarının Yapılması

- Yetki matrisi analiz çalışmalarının yapılması,
- Yetki kontrolü,
- Erişim loglarının oluşturulması,
- Kullanıcı hesap yönetimi,
- RACI matrisi oluşturulması,
- Responsible (İş Yapmakla Sorumlu): İş yapan ve görevi tamamlamada aktif bireylerin belirlenmesi,
- Accountable (Genel Sorumlu): Faaliyet veya kararın sonuçlarından sorumlu olan onay ve veto yetkisi olan bireyin belirlenmesi,
- Consulted (Danışılan): Nihai kararlar ve görevlerde danışılan kişinin belirlenmesi,
- Informed (Bilgilendirilen): Bir karar veya eylem sonrası haberdar olma ihtiyacı olan bireyin belirlenmesi gerekmektedir.

4 | Veri Paylaşım Şeması Oluşturulması

- Kurum dışına gönderilen / paylaşılan kişisel veriler,
- Kişisel verinin paylaşım sebebi,
- Kişisel veriyi hangi birimin paylaştığı,
- Paylaşım yapılan firma/iş ortağı/bayi vb.
- Paylaşım yöntemi (ftp, e-posta, kargo vb.),
- Bu paylaşım için müşteri izinlerinin gerekip gerekmediği,
- Kişisel verinin yurtdışı ile paylaşılıp paylaşılmadığı,
- Hangi sıklıkla paylaşım yapıldığı,
- Veri paylaşılan 3. taraf ile gizlilik sözleşmesinin olup olmadığı belirlenmelidir.

5 | Kişisel Veri Envanterinin Hazırlanması

- Kişisel verinin hangi servis noktalarından hangi yöntemle toplandığı,
- Kişisel verilerin toplanma ve işleme amaçları,
- Kişisel verinin toplanması, saklanması için açık rıza gerekip gerekmediği,
- Toplanan kişisel verilerin tutulduğu ve işlendiği sistemler,
- Kişisel verinin sahibi kimler olduğu (grup bazlı),
- Kişisel verinin formatı (ses, basılı kağıt, dijital ortam, manyetik kartuş vb.),
- Varsa nitelikli kişisel veriler,
- Kişisel verilerin saklama sürelerinin hangi mevzuat, kanun ya da yönetmeliği göre belirlendiği hususu,
- İlgili talep ederse bu verilerin hangi durumlarda silinebileceği,
- İlgili izni gerekmesine rağmen izin alınmadan kişisel veri işlenen süreçleri,
- Varsa yurtdışı veri paylaşımı yapılan süreçlerinin belirlenmesi,
- Bulut - cloud sistemlerinde tutulan ve paylaşılan veriler belirlenmelidir.

6 | Kişisel Veri İşleme Sisteminde Bulunması Gerekenlerin Listesi

Veri adı	Veri sahibi kategorisi / alt kategorisi
Veri kategorisi	Veri erişim durumu
Verinin toplanma amacı / ilgili iş süreci	Veri erişim gerekçesi
Verinin toplanma türü	Veriye erişen birim
Veriyi toplayan birim	Veriye erişen kişi sayısı
Verinin işleme amacı / ilgili iş süreci	Veri paylaşım durumu
Verinin işleme türü	Veri paylaşım gerekçesi (ilgili yasa, sözleşme vs.)
Verinin işleme sıklığı	Verinin paylaşıldığı kişiler (özel/tüzel)
Verinin işlendiği yer	Veri transferi durumu
Verinin işlendiği birim	Veri transferi gerekçesi (ilgili yasa, sözleşme vs)
Verinin saklanma amacı / ilgili iş süreci	Verinin transfer edildiği kişiler (özel/tüzel)
Verinin saklanma süresi	Açık rıza durumu
Verinin saklandığı yer	Açıklamalar
Veriyi saklayan birim	
Veri sorumlusu	
Veri sahibi	

7 | Sözleşmelerin Düzenlenmesi

- Kişisel veri paylaşımı yapılan ya da kişisel verilere erişim bulunan iş ortakları, bayiler vb. ile gizlilik sözleşmelerinin güncellenmesi yoksa düzenlenmesi,
- Yönetmelik ve kanunlardan doğan risklerin transfer edilmesi için hizmet sözleşmeleri, bayilik anlaşmaları vb. hukuki metinlerin güncellenmesi,
- Çalışanlar ile kişisel verilerin gizliliği ve bilgi güvenliği yönetmelik ve politikalarına uyum ile ilgili olarak sözleşmelerin hazırlanması,
- İş Sözleşmelerine ve Disiplin Yönetmeliğine Kanuna uygun hükümler ilave edilmesi,
- Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen arasındaki sözleşmelerin gözden geçirilmesi,
- Gizlilik taahhütnamelerinin hazırlanması gerekmektedir.

8 | Açık Rıza, Aydınlatma ve Bilgilendirme Metinlerinin Düzenlenmesi

- Kişisel verilerin toplandığı her kanalda açık rıza gereken durumlar için kanuna, yapılan işe, amaca uygun olarak açık rıza metinlerinin hazırlanarak açık rızaların alınması,
- Kişisel verilerin toplandığı kanallardan bildirim yapılması için (dijital ortamlar, çağrı merkezi, fiziksel temas noktaları vb.) içeriği kanunda belirtilen esaslara uygun aydınlatma ve bilgilendirme metinlerinin hazırlanması,
- Reklam, pazarlama, yeni ürün tanıtımları vb. için iletişim izni muvafakat metni hazırlanması,
- 3. taraf firmalar ve iş ortakları ile veri paylaşım ve yurtdışı veri paylaşım muvafakat metinlerinin hazırlanması,
- İnternet sitesi üzerinden paylaşılacak aydınlatma yazısının hazırlanması,
- Politikaların belirlenecek bölümlerinin kurumsal internet sitelerinde yayınlanmasının sağlanması gerekmektedir.



6698 sayılı KVKK madde 5/1 gereğince kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.



6698 sayılı KVKK madde 6/2 gereğince özel nitelikteki kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesi yasaktır.



6698 sayılı KVKK madde 8/1 ve 9/1 gereğince kişisel veriler ana kural olarak ilgili kişinin açık rızası olmaksızın yurt içine veya yurt dışına aktarılamaz.

9 | VERBİS Bildirim Sistemine Geçilmesi

- Veri sorumlusunun ve veri sorumlusu temsilcisi ve irtibat kişinin seçilmesi, Veri Sorumluları Sicili'ne kayıt işlemlerinin yapılması,
- Veri sorumluluğu görev tanımlarının oluşturulması,
- Kişisel Veri Yönetimi sürecinin oluşturulması,
- Veri Sorumluları Sicil Bilgi Sistemi'ne kayıt esnasında gereken dokümanların hazırlanması ve kayıt konusunda hukuki destek verilmesi gerekmektedir.



6698 sayılı KVKK madde 16/2 maddesi gereğince kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır.



6698 sayılı KVKK madde 18/1-ç gereğince Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir.

10 | Kurumsal İletişimin Güçlendirilmesi

- Kriz yönetimi planının,
- Kurumu bilgilendirme süreçlerinin,
- Kişiyi bilgilendirme süreçlerinin,
- Kişisel verileri koruma kanunu çerçevesinde bilgi edinme hakkı ve veri silinmesi başvurusunda bulunan kişisel veri sahiplerine kanuna uygun olarak verilecek cevapların taslak içeriklerinin hazırlanması gerekmektedir.



6698 Sayılı KVKK madde 13/2 gereğince veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır.



6698 Sayılı KVKK madde 14/1 Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetle bulunabilir.

11 | Eğitim ve Farkındalık Faaliyetlerinin Düzenlenmesi

- Kanun ve yönetmeliklerle ilgili farkındalık eğitimleri,
- Bilgi ve veri güvenliği temel eğitimler,
- Kurum İnternet sitesi ve sosyal medya hesapları kullanım eğitimleri,
- Veri sorumlusu eğitimi,
- Veri işleyen eğitimi düzenlenmelidir,
- Kurum politikalarının kurum çalışanlarına bildirilmelidir.



6698 Sayılı KVKK madde 10 gereğince Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11'inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.



6698 sayılı KVKK madde 18/1-a gereğince aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar idari para cezası verilir.



6698 sayılı KVKK madde 12 gereğince veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.



6698 sayılı KVKK madde 18/1-b gereğince veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası verilir.

12 | Teknik Veri Koruma Önlemlerinin Geliştirilmesi

İş birimleri ve IT ile görüşmeler yaparak aşağıdaki veri koruma için gereken teknik korumanın hangi seviyede olduğunun belirlenmesi, raporlanması gerekmektedir:

- Ağ güvenliği,
- Uygulama güvenliği,
- Şifreleme,

- Sızma testi,
- Saldırı tespit ve önleme sistemleri,
- Veri kaybı önleme yazılımları,
- Yedekleme,
- Güvenlik duvarları,
- Güncel antivirüs sistemleri,
- Erişim yönetimi (Yetkisiz erişimler, Geniş Yetkiler, Kullanılmayan hesaplar),
- Loglama (Veri sistemlerinde rapor, görüntüleme vb. işlemlerin kayıtları),
- Veri sızmasının engellenmesi,
- Veri paylaşım yöntemleri,
- Taşınabilir cihaz kullanımı,
- Fiziksel güvenlik önlemleri,
- Veri koruma yöntemleri.

13 | Kişisel Veri Uyumsuzlukları ve Risk Listesi Oluşturulması

- Etkilenen veri,
- Verinin etki değeri,
- Veri sahibi,
- İlgili iş süreci grubu,
- Etkilenen sistemler (Turna vb.),
- Tehdit tanımı,
- Zafiyet tanımı,
- Risk tanımı,
- Tehdidin oluşma olasılığı,
- Tehdidin etki derecesi,
- İlk risk değeri,
- Risk işleme faaliyetleri (teknik ve hukuki),
- Faaliyetler sonrası tehdidin oluşma olasılığı,
- Faaliyetler sonrası tehdidin etki derecesi,
- Son risk değeri listede yer almalıdır.

14 | Veri Silme, Periyodik İmha ve Anonim Hale Getirme Uygulamalarının Belirlenmesi

- IT ve iş birimleri ile yapılan görüşmelere göre ilgili yönetmeliklere uygun bir şekilde silinmesi gereken dijital ve basılı verilerin tespit edilmesi.
- Silme, anonim ve imha yöntemlerinden uygun olan yöntem konusunda pratik uygulamalarla destek verilmesi gerekmektedir.



6698 sayılı KVKK 4/2-d maddesine göre kişisel verilerin ilgili mevzuatta öngörülen ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir.



6698 sayılı KVKK 7/1 maddesine göre bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.



6698 sayılı KVKK 4-1-ğ maddesi gereğince Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi ifade eder.

15 | Kişisel Verilerin Azaltılması

- Veri Ambarı Projelerinde Veri Eşleştirme (Data Mapping) yapılması,
- Kullanılmayan fiziki depolama araçlarının tespiti,
- Fiziki depolama araçlarında kullanılmayan verilerin tespiti,
- Bulut cloud sistemlerinde kullanılmayan verilerin tespiti,
- Birden fazla yerde dağınık şekilde bulunan verilerin tespiti,
- Kullanılmayan elektronik arşivlerin tespiti,
- Kullanılmayan yedeklerin tespiti,
- Üçüncü kişi ve kurumlarla paylaşılmış kullanılmayan verilerin tespiti gerekmektedir.



6698 Sayılı Kişisel Verilerin Korunması Kanun'un GEÇİCİ MADDE 1/3 gereğince Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu kanun 07.04.2016 tarihinde yayınlandığından 07.04.2018 tarihi itibarıyla şirketlerin iş-lemiş oldukları kişisel verileri bu kanuna uygun hale getirmeleri gerekmektedir.

16 | Sonuç ve Değerlendirme Raporunun Hazırlanması

- Tespit edilen bulguların ve uyumsuzlukların iyileştirilmesi için önerilerin yer alacağı Risk Analiz Raporu yayınlanacaktır.
- Risk Analiz Raporunun ilgili IT ve iş birimleri ile görüşülerek eksikliklerin ne zaman ve nasıl tamamlanacağına dair geri bildirimleri içerecektir.
- Hazırlanmış Kurumsal Veri Matrisinin güncel tutulması için öneriler geliştirilecektir.
- Kanuna uyum için gereken teknik tedbirler için bilgi güvenliği iyileştirme çalışmaları yapılacaktır.
- Teknik tedbirler sağlanması için gereken bilgi güvenliği ürün ve yazılımları konusunda danışmanlık alınacaktır.
- Kişisel veri işleyen birimlerin kanuna uygun olmayan süreçlerinin yeniden düzenlenmesi sağlanacaktır.
- Veri saklama, işleme, paylaşımına dair iyileştirmeler yapılacaktır.
- Kişisel verilere erişim sağlayan çalışan, bayi, 3.taraf firma vb. hesapların gözden geçirilecektir.
- Proje, ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO 31000 Kurumsal Risk Yönetim Sistemi ve BS 10012 Kişisel Bilgi Güvenliği Sistemi Standartlarına uygun olarak denetlenebilecektir.



6698 sayılı KVKK madde 12/3 gereğince veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

"Sonuç ve Değerlendirme Raporu"nun belediye başkanı tarafından onaylanması ile uyum süreci tamamlanmış olarak kabul edilecektir.



SONUÇ

Kişisel verilerin ilgililere daha iyi hizmet sunulması amacı ile işleme ihtiyacı, verileri bir ekonomik değer haline getirmektedir. Güncel durumda bu verilerin aktarılması ve saklanması noktasında uygun güvenlik tedbirlerinin alınması zorunlu olmaktadır. Bu amaçla kişisel verilerin sınırsız biçimde toplanması, yetkisiz kişilerin erişimine izin verilmesi, ifşa edilmesi ya da amacı dışında veya kötüye kullanılması sonucu kişilik haklarının muhtemel ihlallerinin önüne geçilmek üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu çıkarılmıştır. Bu kanun, kişisel verilerin hangi kurallarla ve hangi şartlarda işlenebileceğini kontrol altına almakta, bu verilerin işlenmesine ilişkin denetim mekanizmalarını getirerek, hukuka aykırı olarak işlenmelerini engelleyen hükümler getirmektedir.

6698 sayılı KVKK kamu kurumları ile özel kuruluşlar açısından herhangi bir ayırım yapmamaktadır. Bu sebeple kamu kurumlarının işlediği veriler açısından da kanunun belirlediği usul ve esaslar geçerli olacaktır. Ayrıca bu kanun kapsamında korunan verilerin sadece gerçek kişilere ait olduğu tüzel kişilere ait verilerin bu kapsamda olmadığına dikkat etmek gerekmektedir. Ancak tüzel kişiye ilişkin verilerin elde edilmesinde bir veya birden fazla gerçek kişinin kimliğinin belirlenmesi sonucunu doğuruyor ise bu tür veriler de kanun kapsamında korunacaktır. 6698 sayılı kanunda kişisel verilerin kısmen veya tamamen otomatik olan veya herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesinde de bir ayırma gidilmemiştir. Buna ilişkin olarak, kişisel verilere ulaşımı kolaylaştıracak şekilde, belirli bir kriterlere göre yapılandırılmış her türlü sistemin Kanun kapsamında olduğu unutulmamalıdır.

Yerel yönetimlerde bu Kanuna ilişkin uyum süreci; başta belediye başkanı, daire başkanları, müdürleri ve şefleri ile birlikte belediye bünyesinde çalışan hukuk müşavirleri, avukatlar, insan kaynakları (İK) yöneticileri ve personeli, bilgi işlem merkezi (IT) yöneticileri ve personeli, halka ilişkiler yöneticileri ve personeli, risk bölüm yöneticileri ve personeli ile ilgilendirmektedir. Bu doğrultuda 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat kapsamında belediye bünyesinde yapılması gerekenleri tespit etmek ve uyum sürecini başlatmak gerekmektedir. Uyum süreci çalışmalarının zaman ve bütçesinin doğru tespit edilerek verimli kullanılabilmesi için belediye merkezinde ilgili departman yöneticilerinin katılacağı "Kişisel Verilerin Korunması Temel Bilgiler Farkındalık Eğitimi" eğitimi ve sonrasında hukuk ve bilgi işlem birimlerinin katılacağı "Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Temel Eğitimi" alınması ihtiyacı tespit edilmiştir.

Öncelikli olarak yapılması gereken belediyelerde mevcut durum analizidir. Bu analizden sonra veri politikaları oluşturulmalıdır. Bu ekseninde yetki matrisi çalışmaları yapılarak, veri paylaşım şeması oluşturulmalıdır. En önemli aşamalardan biri olan kişisel veri envanteri hazırlanmalıdır. Kişisel veri işleme sistemi ile veriye ilişkin tüm bilgilerin yer alması sağlanmalıdır. Bu verilerin paylaşımı veya saklanması paydaşı olan iş ortaklarıyla yapılan sözleşmeler güncellenmeli veya yenilenmelidir. Bu verilerin korunmasını sağlayacak olan ve kanunen zorunlu olan açık rıza, aydınlatma ve bilgilendirme metinlerinin hazırlanmalı ve ilgililere iletilmelidir. Veri işleme ile ilgili kimseler Verbis'e bildirilmeli; kurumsal iletişim, kurumu ve kişileri bilgilendirme süreçlerini yönetmelidir. Her alanda olduğu gibi bu alanda da eğitim ve farkındalık faaliyetleri geliştirilmelidir. Teknik veri koruma önlemlerinin ne seviyede olduğu tespit edilmelidir. Kişisel veri uyumsuzlukları ve risk listesi belirlenerek; veri silme, periyodik imha ve anonim hale getirme uygulamaları geliştirilmeli, depolanan kişisel verilerin azaltılması yoluna gidilmelidir.

Yukarıda belirtilen aşamalar tamamlandıktan sonra bir değerlendirme raporu hazırlanarak bu rapor belediye başkanının onayına sunulmalıdır. Raporun belediye başkanı tarafından onaylanması sonucu, uyum sürecinin tamamlanmış olacağı kanaatine varılmıştır.





RAPORA KATKI SAĞLAYANLAR

MODERATÖR VE GENEL RAPORTÖRLER

AV. ÖZGÜR ERALP.....ERALP DANIŞMANLIK
İBRAHİM SARUHAN.....DİGİSECURE

RAPORTÖRLER

YUNUS DEMİRYÜREK.....MARMARA BELEDİYELER BİRLİĞİ
AV. GAMZE GÜLER.....MARMARA BELEDİYELER BİRLİĞİ
KEREM ULUSOY.....MARMARA BELEDİYELER BİRLİĞİ

KATILIMCILAR

AHMET NARİN.....BAĞCILAR BELEDİYESİ
AV. ORHAN YILMAZ.....BEYLİKDÜZÜ BELEDİYESİ
SERKAN KOÇ.....BOZYÜK BELEDİYESİ
YÜCEL AKKUL.....BURSA BÜYÜKŞEHİR BELEDİYESİ
UÇUR YILDIRIM.....ÇEKMEKÖY BELEDİYESİ
OSMAN ORHAN.....ÇEKMEKÖY BELEDİYESİ
SELÇUK BALLI.....DARICA BELEDİYESİ
NUH DURSUN OZAN.....ESENLER BELEDİYESİ
YAKUP PALA.....GÜRSU BELEDİYESİ
ŞEHABETTİN ÇAĞLAR.....İSTANBUL BÜYÜKŞEHİR BELEDİYESİ
TOLGA YETİŞGİN.....KADIKÖY BELEDİYESİ
AV. İSHAK KÜSKÜ.....KAĞITHANE BELEDİYESİ
AV. ABDÜLKADİR ALTUNTAŞ.....KAĞITHANE BELEDİYESİ
AV. MEHMET PARLAK.....KAĞITHANE BELEDİYESİ
İSMAİL GÜLSOY.....KOCAELİ BÜYÜKŞEHİR BELEDİYESİ
MESUT TAŞKIN.....KOCAELİ BÜYÜKŞEHİR BELEDİYESİ
GÖNÜL İŞILDAK.....KÜÇÜKÇEKMECE BELEDİYESİ
DAVUT KAHYA.....OSMANELİ BELEDİYESİ
AV. HÜSEYİN HAYAL.....PENDİK BELEDİYESİ
TAYFUN YORTANLI.....SAKARYA BÜYÜKŞEHİR BELEDİYESİ
AV. GÖNÜL ÇELİK.....SANCAKTEPE BELEDİYESİ
SÜHEYLA ÖZTÜRK.....SULTANBEYLİ BELEDİYESİ
AV. ŞEYDA KESKİNKILIÇ.....SULTANBEYLİ BELEDİYESİ
MURAT MERT ERENGİL.....ŞİŞLİ BELEDİYESİ
YUSUF YAMAÇ.....TUZLA BELEDİYESİ
AHMET YÜCE.....YENİŞEHİR BELEDİYESİ
YUNUS GÜRSOY.....ZEYTİNBURNU BELEDİYESİ





www.marmara.gov.tr