T.C.
CUMHURBAŞKANLIĞI
Devlet Denetleme Kurulu

DENETLEME RAPORU

RAPORUN KONUSU

Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları

Bilgi Edinme Hakkı Kanunu kapsamında yer alan sınırlamalar ile Kurum denetimlerine ilişkin bilgi güvenliği kısıtları nedeniyle internet sayfamızda Raporun yalnızca Sonuç Bölümüne yer verilmiştir.

Tarihi : 27 / 11/ 2013

Sayısı : 2013 / 3

Eki : -

İÇİNDEKİLER

SONUÇ

Kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü veri olarak tanımlanmaktadır. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, cihaz kimlikleri, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.

Kişisel verilerin korunması hakkı, temel insan hak ve özgürlükleri arasında yer almakta olup, insanın şahsiyetinin korunması, hukuk devleti ilkesi ve demokrasinin derinlik kazanması açısından hayati öneme sahiptir. Kişisel veriler dâhil, özel hayatın anayasal güvence ile koruma altına alınmasında temel amaç, insan kişiliğinin serbestçe gelişmesine imkân vermek, kişiye kendisi ve yakınları ile baş başa kalabileceği, devlet veya başkaları tarafından rahatsız edilemeyeceği özerk bir alan sağlamaktır.

Kişisel verilerin korunması hakkı son kırk yılda büyük önem kazanmıştır. Bunda, bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte veri toplama ve bunları otomatik olarak işleme kapasitelerindeki artış ile bu artışa dayalı olarak kişilerin özel hayat mahremiyet alanının daha savunmasız hale gelmesi önemli bir etkendir. Özellikle, bilişim teknolojilerindeki gelişmeler sonucunda;

- Geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi,
- Daha önce dağınık yapılarca toplanan ve birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilmesi,
- Verilerin ileri teknolojik imkânlarla ve veri eşleştirme (*data matching*) ve veri madenciliği (*data mining*) gibi tekniklerle analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması,
- Verilere erişim, paylaşım ve transferin kolaylaşması ve maliyetinin düşmesi,
- Kişisel verilerin ticari işletmeler için kıymetli bir varlık ve ticari meta niteliği kazanması neticesinde özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşmış olması,
- Yabancı ülke istihbarat birimlerinin, terör ve suç örgütlerinin kişisel verileri ele geçirme veya bu sistemlere zarar verme yönündeki faaliyet ve saldırılarının artması,

• Banka ve kredi kartı dolandırıcılıkları başta olmak üzere, kişisel verileri hedef alan veya bunlar kullanılmak suretiyle işlenen suç olaylarının artması

gibi hususlar kişilerin mahremiyet alanını önemli derecede daraltmış ve kişisel verilerin korunması ihtiyacını en üst noktaya taşımıştır.

Teknolojik ve demokratik gelişmişlik seviyelerine bağlı olarak ülkeler, 1970'lerden itibaren kişisel verilerin korunmasına yönelik kanuni düzenleme ve kurumsal yapıları oluşturma yönünde önemli adımlar atmaya başlamışlardır. Kişisel verilerin korunması alanındaki öncü düzenleme İsveç tarafında yapılmıştır. İsveç Veri Kanunu 1973 tarihlidir. Günümüzde kişisel veri koruma kanununa sahip ülke sayısı 99'a ulaşmıştır.

Kişisel verilerin korunmasına ilişkin ulusal düzeydeki düzenlemelerin artması, özellikle kişisel verilerin korunması alanında yeterli düzenlemesi bulunmayan ülkelerle veri paylaşımı ve verilerin sınır ötesine aktarılmasında sorunlar yaşanmasına neden olmuştur. Ülkeler arasında veri paylaşımında yaşanan sıkıntılar ve sınırlamalar, uluslararası ticaretten vergilemeye, polisiye ve adli nitelikteki alanlara kadar pek çok işbirliği alanını olumsuz etkilemektedir. Bu nedenle, ülke düzeyinde kişisel hak ve özgürlükler alanının korunması kaygısının hâkim olduğu kişisel verilerin korunmasına yönelik düzenlemeler, uluslararası sistemin işlerliği için ülkelerin kişisel verilerin korunması sistemlerini uyumlaştırmalarını bir gereklilik haline getirmiştir. Dolayısıyla kişisel verilerin korunmasına ilişkin uluslararası düzenlemelere yönelik adımlarda, gelişen teknoloji ile birlikte artan kişisel verilerin korunması ihtiyacı yanında, uluslararası veri paylaşımı için ülke mevzuatlarının uyumlaştırılması ihtiyacı da önemli bir faktör olmuştur.

Uluslararası düzeyde Avrupa Konseyi, Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Birleşmiş Milletler başta olmak üzere çeşitli uluslararası kuruluşlar kişisel veriler konusunda uluslararası nitelikte bağlayıcı olan veya olmayan sözleşme ve benzeri metinler üretmeye başlamıştır. Avrupa Birliği de, üye ülke mevzuat ve uygulamalarını uyumlaştırmaya yönelik olarak düzenlemeler yapmıştır.

Kişisel verilerin korunması alanındaki ulusal ve uluslararası düzenlemelerin köşe taşlarını; kişisel verilerin korunması hakkının anayasal güvenceye kavuşturulması, kişisel verilerin temel ilkelere uygun olarak işlenmesi, kişisel verisi işlenen kişilerin haklarının kanun düzeyinde belirlenmesi, kişisel veri kütüğü sahiplerinin görev ve sorumlulukları ile kişisel verilerin korunması konusunda etkin rol alacak bağımsız, tarafsız ve teknik olarak yeterli veri koruma otoritesinin hayata geçirilmesi oluşturmaktadır.

Kişisel verilerin işlenmesine ilişkin ilkeler, konunun nirengi noktasını oluşturmaktadır. Uluslararası belgelerde kabul görmüş ve pek çok ülke uygulamasına yansımış olan kişisel verilerin işlenmesine ilişkin genel ilkeler aşağıdaki gibi sıralanabilir:

- Hukuka ve dürüstlük kurallarına uygunluk,
- Veri minimizasyonu veya asgarilik,
- Amacın belirliliği,
- Verilerin doğru ve güncel olması, veri kalitesi,
- Verisi işlenen kişinin veriler üzerinde kontrolünün bulunması,
- Kişisel verilerin paylaşımının sınırlandırılması,
- Bilgi güvenliği ve sorumluluk,
- Hassas veriler için özel önlemler öngörülmesi.

Kişisel verilerin korunması hakkı, demokratikleşme alanında mesafe alma çabaları, etkin kişisel veri koruma ortamının bulunmamasının uluslararası alanda bilgi değişiminde ortaya çıkardığı sorunlar, Avrupa Birliği'ne uyum sürecinde İlerleme Raporlarında sürekli eleştiri konusu yapılması gibi nedenlerle Türkiye'nin uzun yıllardır gündeminde bulunan bir konudur.

Türkiye, kişisel verilerin korunması alanında ilk uluslararası belge olan Avrupa Konseyinin 28.01.1981 tarihinde imzaya açtığı 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmeyi imzaya açıldığı gün imzalayan ilk ülkelerden birisidir. Günümüz itibariyle ise San Marino Sözleşmeyi imzalamayan, Türkiye ise imzalamasına rağmen onay sürecini işletmemiş tek ülke konumundadır.

Sözleşmenin tarafların yükümlülüklerinin belirtildiği 4. maddesinde, taraflar kişisel verilerin korunmasına ilişkin temel prensiplerin iç hukukta uygulanmasını sağlayacak önlemleri bu Sözleşmenin ülkede yürürlüğe girmesinden önce almakla yükümlü tutulmuşlardır. Bu madde uyarınca, Sözleşmenin onaylanarak yürürlüğe konulabilmesi için, öncelikle Sözleşmenin İkinci Bölümünde yer alan temel prensiplerin iç hukukta uygulanmasını sağlayacak uygun önlemlerin alınması gerekmektedir. Bu kapsamdaki en önemli önlem, kişisel verilerin korunması alanını düzenleyen çerçeve bir kanuna sahip olunmasıdır.

Türkiye'de kişisel verilerin korunması alanını düzenleyen çerçeve bir kanun bulunmamaktadır. 1989 yılından itibaren sürdürülen kişisel verilerin korunmasına ilişkin kanun hazırlama çalışmaları halen devam etmekte olup henüz kanun tasarısı, taslak halindedir.

26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunmasına ilişkin hükümlere yer verilmiştir. Ancak, kişisel verilerin korunmasına yönelik çerçeve bir kanunun bulunmaması 5237 sayılı Kanun'la getirilen ceza müeyyidesine bağlı korumaların hayata geçirilmesindeki etkiyi azaltmıştır.

Kişisel verilerin korunması hakkı 12.09.2010 tarihinde yapılan Anayasa Referandumu sonucunda kabul edilen 07.05.2010 tarih ve 5982 sayılı Kanun'un 2. maddesi ile Anayasanın Kişinin Hakları ve Ödevleri başlıklı İkinci Bölümünde yer alan "Özel hayatın gizliliği" başlıklı 20. maddesine eklenen son fıkra ile Anayasa'da güvence altına alınmıştır. Söz konusu fıkra hükmü, kişisel verilerin korunması hakkına ilişkin uluslararası belgelerde yer alan temel unsurları bünyesinde barındırması itibariyle önemli olup aşağıdaki gibidir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Söz konusu düzenleme, kişisel verilerin korunması hakkının temel ilkelerini ve kişilerin haklarını açıkça belirtmesi açısından önemlidir. Ancak, Anayasa ile güvence altına alınan bu hakkın etkin bir şekilde korunması açısından; kişisel veri, açık rıza ve benzeri tanımların, kişisel verilerin işlenmesinin genel ilke ve esaslarının, kişilerin haklarını korumalarına yardımcı olacak mekanizmaların ve ilgili kurum ve kuruluşların kişisel verilerin işlenmesi sırasında bu hakkın korunmasına aykırı davranışta bulunmamalarını sağlamak amacıyla gerekli ikincil düzenlemeleri ve denetimleri yapacak, şikâyetleri değerlendirecek, idari yaptırım uygulama yetkisine sahip kurumsal yapılanmanın ne şekilde olacağını belirleyen çerçeve bir kanunun bir an önce hukuk sistemimize kazandırılması ihtiyacı bulunmaktadır.

Türkiye'de kişisel verilerin korunması konusunun önem kazanması ve bu konuda bilgi sistemlerinin güvenliğinin öneminin ortaya çıkması ile birlikte, gerek mevzuat gerekse uygulama alanında yaşanan eksiklik ve aksaklıkların değerlendirilmesi ve alınması gerekli önlemlerin tespiti amacıyla; kamuya ait bilgi sistemlerinin bilgi güvenliği ve kişisel veri mahremiyeti açısından incelenmesi, bu kapsamda iç kontrol sistemlerinin yeterliliğinin denetimi görevi Cumhurbaşkanlığı Yüce Katı tarafından Devlet Denetleme Kuruluna tevdi edilmiştir. Bu görevlendirme kapsamında; yerli ve yabancı literatür taraması, ilgili kamu kurumlarından bilgi ve görüş alınması, seçilen bazı bilgi sistemleri üzerinde yerinde yürütülen denetim çalışmaları sonucunda işbu Rapor hazırlanmıştır.

Raporda temel eksen kişisel verilerin korunmasıdır. Ancak kişisel verilerin korunması açısından önemli bir faktör olan bilgi güvenliği konusu da bu temel eksen çerçevesinde inceleme konusu yapılmıştır.

Raporda öncelikle kavramsal ve teorik çerçeve üzerinde durulmuştur. Daha sonra Türkiye'de bu alanda yürütülen çalışmalara da ışık tutması amacıyla, konuya ilişkin uluslararası

düzenlemeler ile ülke örnekleri incelenmiştir. Türkiye'deki durum; mevzuat, kurumsal altyapı ve uygulamalar ile temel bazı bilgi sistemlerinde yürütülen denetim çalışmaları çerçevesinde analiz edilmiştir.

Bu kapsamda altı kamu kurumunda denetim çalışmaları gerçekleştirilmiştir. Kamu kurumları nezdinde gerçekleştirilen denetim çalışmalarında; kamu kesiminin, kişisel verilerin korunması ve bununla bağlantılı olarak bilgi güvenliği açısından genel durumunun ortaya konulması amaçlanmıştır. Denetlenen kurumlar bu amaca uygun olarak seçilmiş ve denetim sıralaması da dâhil olmak üzere, denetimin yöntemi, süreci gibi unsurlar da bu amaca uygun olarak belirlenmiştir.

Denetimler, sırasıyla;

1- Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü,

2- Tapu ve Kadastro Genel Müdürlüğü,

3- Gelir İdaresi Başkanlığı,

4- Sosyal Güvenlik Kurumu,

5- Sağlık Bakanlığı,

6- Adalet Bakanlığı

bünyesinde gerçekleştirilmiştir.

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünde en temel kişisel veri niteliğinde olan kimlik ve adres bilgileri tutulmakta olup, söz konusu bilgiler diğer kurum ve kuruluşlarda tutulan veriler ve veri tabanları açısından omurga niteliğini taşımaktadır. Özellikle Türkiye Cumhuriyeti kimlik numarası uygulamasının da hayata geçmesi ile birlikte bu bilgiler aynı zamanda diğer veri tabanları ve bilgi sistemleri açısından da anahtar vazifesini görmektedir. Bu nedenle Genel Müdürlük bünyesinde tutulan kişisel verilerin güvenliğinin sağlanması büyük önem taşımaktadır. Bu önem sebebiyle denetim çalışmasına Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünden başlanmıştır. Daha sonra bir diğer omurga veri tabanı olan ve taşınmazlara ilişkin mülkiyetin hukuki dayanağını oluşturan bilgilerin bulunduğu Tapu ve Kadastro Bilgi Sistemini (TAKBİS) bünyesinde barındıran Tapu ve Kadastro Genel Müdürlüğünde denetim çalışmaları gerçekleştirilmiştir. İfade edildiği üzere, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ve Tapu ve Kadastro Genel Müdürlüğü veri tabanları omurga niteliğinde veri tabanlarıdır. Bu veri tabanları marifetiyle pek çok kurum ve kuruluşla bilgi paylaşılmaktadır. Bu nedenle bu iki kuruma münhasır olmak üzere, bilgi paylaşılan kamu kurumları ve özel kurumlara yönelik de denetim çalışması gerçekleştirilmiş olup, Raporun ilgili bölümlerinde bilgi paylaşılan kurumlarla ilgili tespit ve önerilere de yer verilmiştir.

Yukarıda ifade edilen iki kurumun ardından sırasıyla, genel olarak veri alıcısı niteliğinde bulunan ve vergi mahremiyeti maddesi ile de mahrem nitelikte olduğu hususu net olarak belirlenmiş verilerin tutulduğu Gelir İdaresi Başkanlığı, sosyal sigorta ve sağlık verilerinin tutulduğu Sosyal Güvenlik Kurumu, yine sağlık verilerinin tutulduğu Sağlık Bakanlığı ile adli ve idari yargıya ilişkin tüm işlemler ile yargıya ve yargı mensuplarına ilişkin idari işlemlerin yapıldığı, tutuklama, yakalama kararı çıkartma gibi vatandaşların günlük hayatlarına etki edebilecek işlemlerin de gerçekleştirildiği UYAP'ı bünyesinde barındıran Adalet Bakanlığı nezdinde denetim çalışmaları gerçekleştirilmiştir.

Denetim çalışmalarındaki genel uygulama, kuruma gitmeden önce kurumun bilgi güvenliği ve kişisel verilerin korunması açısından genel durumunu ortaya koymaya yarayacak bilgi ve belgelerin, 16 adet tablo ile belirlenen formata uygun şekilde kurumlardan temin edilmesi olmuştur. Söz konusu bilgi ve belgeler ile kurumların mevzuat ve yayınları incelenmek suretiyle, yerinde yapılacak denetimlere hazırlanılmıştır. Müteakiben, her bir kurumda ortalama 6 hafta süren yerinde denetimler gerçekleştirilmiştir. Denetimlerde, konuya ilişkin tecrübe ve bilgi birikimine sahip uzmanlardan yararlanılmıştır.

Denetimde, ülkemizde kişisel verilerin korunmasına ilişkin özel bir düzenleme olmadığından konuyla ilgili uluslararası düzenlemeler, ülkemizde dağınık halde bulunan çeşitli mevzuat hükümleri ve kurumların kendi mevzuatlarında yer alan hükümler referans noktası olarak dikkate alınmıştır. Bilgi güvenliği açısından ise bu konudaki en önemli standart niteliğinde olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı esas alınarak denetim çalışmaları gerçekleştirilmiştir.

Kurumlarda gerçekleştirilen denetim çalışmaları sonucunda bilgi güvenliği ve kişisel verilerin korunması konusunda;

1- Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'ne ilişkin tespit ve önerilere Raporun Yedinci Bölümünde,

2- Tapu ve Kadastro Genel Müdürlüğü'ne ilişkin tespit ve önerilere Raporun Sekizinci Bölümünde,

3- Gelir İdaresi Başkanlığı'na ilişkin tespit ve önerilere Raporun Dokuzuncu Bölümünde,

4- Sosyal Güvenlik Kurumu'na ilişkin tespit ve önerilere Raporun Onuncu Bölümünde,

5- Sağlık Bakanlığı'na ilişkin tespit ve önerilere Raporun On Birinci Bölümünde,

6- Adalet Bakanlığı'na ilişkin tespit ve önerilere Raporun On İkinci Bölümünde,

ayrıntılı olarak yer verilmiştir.

Denetim çalışmaları kapsamında bilgi güvenliği ve kişisel verilerin korunması konusundaki risk, tehdit, eksiklik ve geliştirilmesi gerekli alanlara ilişkin bulgular; uluslararası mevzuat, ülke örnekleri, Türkiye'deki mevzuat, kurumsal yapı ve uygulamalar ile kişisel verilerin korunmasına ilişkin kanun çalışmaları bütüncül bir yaklaşımla değerlendirilmek suretiyle yapılan tespitler ile geliştirilen öneriler ise aşağıda sunulmaktadır.

A- GENEL NİTELİKLİ TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 1- Bilgi güvenliği ve kişisel verilerin korunması konusunda gerekli önlemlerin alınması ve gerekli çabanın gösterilebilmesi için öncelikle bu konuda belirli bir farkındalığın oluşması, bilinç düzeyinin gelişmesi gerekmektedir.

Konuyla ilgili olarak yapılan inceleme ve araştırmalar ile kurumlar nezdinde gerçekleştirilen denetim çalışmalarında bilgi güvenliği ile kişisel verilerin korunmasının önemi konusundaki farkındalık düzeyinin arzulanan seviyede bulunmadığı görülmüştür. Söz konusu farkındalık eksikliğinin, kurumlarda bilgi güvenliği ve kişisel verilerin korunması konusunda yaşanan pek çok eksikliğe ve yanlış uygulamaya kaynak teşkil ettiği değerlendirilmiştir.

Farkındalık eksikliğinin mevzuat ve kurumsal uygulamalara yansıdığı; bunun sonucunda bilgi güvenliği ve kişisel verilerin korunması alanında pek çok eksiklik ve açıklığın ortaya çıktığı; bu tür eksiklik ve açıkların bazen ancak çok ciddi siber saldırılar sonucu ortaya çıkabilecek türden tahribata yol açtığı veya açabildiği anlaşılmıştır.

Farkındalık düzeyinin artırılması ihtiyacını ortaya koyan mevzuat ve uygulama örneklerinden bazıları aşağıdaki gibidir:

• Basına ve adliyeye yansımış pek çok olaydan; kişilerin kimlik bilgileri ve kimlik fotokopileri kullanılmak suretiyle kişiler adına yüzlerce telefon hattı açıldığı, sahte kredi kartı çıkartıldığı, şirket kurulduğu, kişilerin dernek, kuruluş ve siyasi partilere üye olarak kaydedildiği, konusu suç teşkil eden adli soruşturmalara dâhil edildiği ve çeşitli dolandırıcılık faaliyetlerinin icra edilebildiği bilinmesine rağmen kurum ve kuruluşların pek çok işlemde kişilerin kimlik fotokopisini alma uygulamaları devam etmektedir.

• 5809 sayılı Elektronik Haberleşme Kanunu'nun 56. maddesi ve Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin 15. maddesi uyarınca, abonelik sözleşmesinin yanında T.C. kimlik numarası ile kimlik belgesinin bir suretinin abonelik sözleşmesi ile muhafaza edilmesi zorunludur. Türkiye'de Haziran 2013 itibariyle mobil abone sayısının 68.025.878 olduğu düşünüldüğünde, 9 yaş üzeri nüfusun önemli bir kısmının kimlik fotokopilerinin, değişik abonelikler nedeniyle GSM operatörlerinde bulunduğu anlaşılmaktadır.

• Kimlik Paylaşımı Sistemi Yönetmeliği'nin 11. maddesinin 3. fıkrasında; "*Kimlik Paylaşımı Sistemi çerçevesinde kimlik bilgisine erişebilen kamu kurum ve kuruluşlarınca ve 5411*

sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalarca kişilerden ayrıca nüfus cüzdanı örneği veya kimlik bilgilerine ilişkin başkaca bir belge istenemez." düzenlemesine ve Ocak 2013 itibariyle Kimlik Paylaşım Sistemine online erişebilen kamu kurumu ve özel kuruluş sayısının 2.478 olmasına rağmen, pek çok işlemde kişilerin kimlik fotokopisinin alınması uygulamasına devam edilmektedir.

• Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun'da yer alan düzenleme kapsamında her seçim döneminde, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, seçmen niteliğine sahip olan 18 yaş ve üzerindeki kişilerin nüfus ve adres bilgilerini Yüksek Seçim Kurulu ile paylaşmakta, talep etmeleri halinde de Yüksek Seçim Kurulu söz konusu verileri siyasi partilerle toplu olarak elektronik ortamda paylaşmaktadır. Dolayısıyla seçmen niteliğine sahip 50 milyonun üzerindeki vatandaşın, adı, soyadı, ana ve baba adı, doğum yılı, doğum yeri, adres bilgisi seçimlere girme yeterliliğini taşıyan onlarca partiyle paylaşılmaktadır. Paylaşılan elektronik ortamdaki verilerin çoğaltılmasını ve başkalarıyla paylaşılmasını engelleyecek hiçbir mekanizma öngörülmemiştir. Bu verileri alan partilerin bu verileri koruma yeterlilikleri ve almaları gereken önlemler konusunda da herhangi bir belirleme yapılmamıştır. Adli makamlara da intikal etmiş olan bazı olaylarda 18 yaş ve üzerindeki kişilerin T.C. kimlik numaraları ile kimlik ve adres bilgilerinin sorgulanmasına imkân veren yazılımların üretildiği ve satıldığı bilgisi, bu tür uygulamaların doğurabileceği sonuçlar açısından dikkat çekicidir.

• Seçmen listesi bilgilerinin bir siyasi partinin internet sitesi üzerinden ve mobil uygulamalarla sorgulanabildiğine ilişkin bir örnekle de karşılaşılmıştır. Söz konusu sorgulamalar T.C. kimlik numarası ve bir adet doğrulama kriteri (baba adı) ile yapılmakta, kişilerin il, ilçe ve mahalle bilgisi ile bulunduğu binadaki seçmen niteliğine sahip kişilerin listesine ulaşılabilmektedir.

• Önceki yıllarda, KEY ödemeleri ve benzeri nedenlerle kişilerin adı, soyadı, T.C. kimlik numaraları, sosyal güvenlik numaraları ve benzeri bilgilerin yayımlanması da bilgi güvenliği ve kişisel veri farkındalığı konusundaki eksikliğe örnek teşkil etmektedir.

Denetim çalışmaları sırasında da farkındalık eksikliğinden kaynaklı pek çok eksiklik ve açıklık tespit edilmiş olup bunlardan sadece birkaçına aşağıda yer verilmektedir:

• Kurumların bazılarında güvenlik, yedekleme, yama, parola politikalarının bulunmaması, bu konudaki uygulamaların çoğu kurumda kişilere bağlı ve bağımlı olarak gerçekleştirilmesi,

• Kurumların çoğunda iş sürekliliği politika ve senaryolarının bulunmaması,

• Çok önemli bazı bilgi sistemlerinin felaket kurtarma merkezinin bulunmaması,

• Kurumdaki en kritik bilgilere dahi ulaşabilen bilişim hizmeti sunan firmalarla ve bunların çalışanları ile herhangi bir gizlilik sözleşmesi yapılmaması ve firma personelinin herhangi bir güvenlik araştırmasından geçirilmemesi,

• Kaynak kodu dâhil, bilgi sistemleri üzerindeki işlemlerin kayıtlarının (log) tutulmasında ciddi eksiklikler bulunması,

• Bilgi sistem odasından otoparka açılan kapı bulunması veya sistem odasına giden fiber kablolarının açıktan geçmesi örnekleri dâhil, fiziki güvenlik konusunda ciddi eksikliklerin mevcudiyeti,

• Hassas veri içeren sistemlere erişimde kullanıcıların iki haneli sayısal şifre verebilmesi, 1111, 0000, 1234 gibi kolay tahmin edilebilir şifrelerin kullanılması,

• Bazı kurumların çağrı merkezinden sadece ad, soyad ve T.C. kimlik numarası beyan etmek suretiyle; maaş tutarları, kesintiye esas brüt ücret, gidilen sağlık kurumu, muayene olunan doktor, ilaç alınan eczane, alınan ilacın adı, ödenen katılım payı miktarı gibi birçok kişisel bilgiye ulaşılabilmesi,

• Kimlik Paylaşım Sistemi aracılığı ile özel kesim ve kamu kesiminden kimlik bilgilerine ulaşabilecek kullanıcı sayısının bir milyonun üzerinde olduğu tahmin edilmesine rağmen, bu erişimlerin güvenliği konusunda verileri alan kurumların bir kısmında; IP adresi bazında kısıtlama getirilmesi, kullanıcıların ad, soyad ve T.C. kimlik numaralarının kayıt altında tutulması, kullanıcıların yapmış oldukları sorguların kayıtlarının (*log*) tutulması, bilgisayarlar ile internet arasında güvenlik duvarı (*firewall*) bulunması, imzaları devamlı güncellenen anti-virüs programının kullanılması, güçlü parola kullanılması gibi temel güvenlik önlemlerinin alınmamış olması,

• Kişisel veri içeren bilgilerin çeşitli taşınabilir kayıt ortamları aracılığı ile bu ortamlar şifrelenmeden ve başkaca herhangi bir güvenlik önlemi alınmadan paylaşılması, bir örnekte CD ortamında 13.8 milyon kişinin kimlik ve adres bilgisinin herhangi bir güvenlik önlemi alınmadan paylaşıldığının tespit edilmesi.

Bilgi güvenliği ve kişisel verilerin korunması konusundaki farkındalık düzeyi ve bu düzeyin yetersizliği konusunda yukarıda yer alan örnekler, Türkiye'de öncelikle bu alanda farkındalık oluşturmaya yönelik çaba içine girilmesi gereğini ortaya çıkarmaktadır. Bu kapsamda, bilgi güvenliği ve kişisel verilerin korunması konusunda farkındalık artırmaya yönelik olarak kurumun en alt kademesindeki çalışanından en üst yöneticisine kadar uzanan geniş bir yelpazede eğitim veya farkındalık oluşturma çalışması yürütülmesi, mevzuat düzenlemelerinde kişisel verilerin güvenliği konusunun gözetilmesi, kurumsal uygulamalardan kaynaklı kötü uygulama örneklerinin tekrarlanmamasına yönelik gerekli tedbirlerin alınması

gerektiği düşünülmektedir. Ayrıca, farkındalık ve bilinç oluşmasının ciddi kültür ve zihniyet değişimi gerektirmesi nedeniyle, kişisel verilerin korunması konusuna her kademede eğitim müfredatında mümkün olduğunca yer verilmesinin, kamu spotu ve benzeri uygulamalarla farkındalık oluşturma çalışmalarının desteklenmesinin uygun olacağı değerlendirilmektedir.

TESPİT VE ÖNERİ 2- Bilgi güvenliği ve kişisel verilerin korunması açısından sadece teknolojik önlemler yeterli değildir. Bilgi güvenliği kültürünün oluşturulması, ilgililerin bu konudaki bilinç ve bilgi seviyesinin artırılması, idari düzenleme ve örgütlenme yapılarının bilgi güvenliği unsuru da dikkate alınarak şekillendirilmesi, hukuk altyapısının uygun hale getirilmesi gibi pek çok unsurun birlikte dikkate alınması gerekmektedir.

Bu kapsamda, kişisel verilerin toplanması, işlenmesi, kullanılması, muhafazası, paylaşılması, yeni işlemlere tabi tutulması, silinmesi gibi her aşamada etkin bir şekilde korunması amacıyla; kamu kesimi ve özel kesim, sivil toplum ve uluslararası kurum ve kuruluşlar olmak üzere tüm taraflar ile konunun teknik, idari, organizasyonel, sosyal ve ekonomik boyutlarının tamamını dikkate alan bütüncül yaklaşım ihtiyacı bulunmaktadır.

TESPİT VE ÖNERİ 3- Kamudaki bilgi sistemlerinin bir e-Devlet mimarisi genel çerçevesinde şekillendirilmemesi nedeniyle güvenlik riskleri başta olmak üzere, sistemlerin birbirleriyle konuşamaması, hizmet kalitesinin düşmesi, aynı verilerin defalarca farklı sistemlerde tutulması gibi pek çok sorun yaşanmakta, gereksiz maliyetlere katlanılmaktadır.

Kamu bilgi sistemi projelerinin yürütülmesinde kurumlara tasarım aşamasında know-how desteği verilmesi, uygun yönlendirme yapılması ve danışmanlık ihtiyacının karşılanması, şartname yazımı ve teslim veya iş kabul işlemleri, izleme ve değerlendirme, sistemin idamesi gibi alanlarda rehberlik ve gerektiğinde koordinasyon sağlayacak bir yapının en kısa süre içerisinde hayata geçirilmesi gerektiği düşünülmektedir.

TESPİT VE ÖNERİ 4- Bilgi sistem donanımlarının ve yazılımlarının ilgili kurumun envanterinde yer alması, söz konusu bilgi sistemlerinin sahipliğinin ilgili kurumda olması anlamına gelmemektedir. Bilgi sistemleri üzerindeki gerçek sahiplik, bu sistemler üzerinde nihai belirleyicilik ve kontrol yetkisine bağlıdır. Söz konusu bilgi sistemleri üzerindeki en üst kontrol yetkilerinin bilişim hizmeti alınan özel firma yetkililerinde bulunması durumunda ilgili kurum, bilgi sistemlerinin sahipliği konumundan, kullanıcısı konumuna düşebilmektedir. Denetimlerde Türkiye'de pek çok kurumun bilgi sistemlerinin gerçek anlamda sahibi olmadığı, tüm vatandaşların verilerini tutan bazı omurga veri tabanlarında dahi bilgi sistemleri üzerinde en üst kontrol yetkisinin bilişim hizmeti alınan yüklenici firma personelinde olduğu görülmüştür.

Bazı kurumlarda, hizmet alınan firmaların, bilgi sisteminin işletilmesi ve verilerin kullanımı, sorgu kayıtlarının tutulması ve benzeri konularda adeta sistemin sahibi gibi hareket

edebildikleri ve herhangi bir sorgu kaydı olmaksızın sistemden veri çekebildikleri bizzat gözlemlenmiştir.

Özel kuruluşlar, bilgi sistemlerinin oluşturulması ve idamesi konusunda oldukça önemli bir birikime ve insan kaynağına sahiptirler. Ancak gelinen nokta, hem bilgi güvenliği hem de sistemlerin sürdürülebilirliği açısından kurumların kendi bilgi sistemlerinin gerçek anlamda sahibi olmalarını gerektirmektedir. Söz konusu durum dışarıdan hiç hizmet alınmayacağı anlamına gelmemekte olup, önemli olan husus, kurumun bilgi sistemleri üzerinde hâkimiyet sağlaması ve özel kurumlarla olan ilişkinin doğrudan hizmetin teslimi değil, işbirliği yapma şekline dönüşmesidir.

Bu kapsamda, kurumların bilgi sistemlerinin gerçek sahibi olmalarını sağlamaya yönelik olarak;

- Bilgi sistemlerinin oluşturulması, güvenliği ve idamesi konusunda hizmet alınan firmalara bağımlı kalmayacak veya bu bağımlılığı en az düzeye indirecek yapılar oluşturulmaya çalışılmalıdır.

- Hizmet alınan firmaların personeli ile kurum personelinin birlikte çalışması ve aralarındaki iletişimin güçlü olması sağlanmalı, alınan hizmetler mümkün olduğunca, işbirliği şeklinde ve zaman içinde kurum personelinin sistemi işletebilir hale gelmesini sağlayacak şekilde olmalıdır.

- Hizmet alınan firma kurumdan ayrıldığında, hem güvenlik hem de sistemin idamesi açısından aksaklıkların ortaya çıkmasını önleyecek biçimde, yapılan işler ve süreçlerle ilgili dokümantasyon sağlanmalıdır.

- Bilgi sistemlerinin oluşturulması, güvenliği ve idamesi konusunda yetkin ve yeterli personele sahip olunmasını sağlayacak çalışmalar makro düzeyde ve kurum düzeyinde yapılmalıdır.

- Kurum personeli tarafından yapılan işler açısından da dokümantasyon sağlanmalı ve yeni göreve başlayan personele söz konusu dokümanlar sunulmalıdır.

TESPİT VE ÖNERİ 5- Güvenlik, neyin korunacağı, hangi değerin önemli olduğu, bu değere yönelmiş tehditler, mevcut zafiyetler ve alınabilecek önlemler unsurlarını bünyesinde barındıran bir kavramdır. Kişisel verilerin korunmasında, korunacak değer "veri", "bilgi" olup öncelikle korunması gereken unsurun nelerden ibaret olduğunun belirlenmesine yönelik envanter çalışması yapılması önem taşımaktadır. Bilgi sistemleri ve bu sistemlerde bulunan veri envanteri çalışması ile korunması gereken veri varlıkları ve bunların niteliği belirlenebilecek, buna göre verilerin kişisel veri, hassas veri, kritik altyapı verisi, gizli veri gibi nitelikleri dikkate alınarak niteliklerine uygun güvenlik önlemleri uygulanabilecektir.

Kamu kurum ve kuruluşlarının sahip olduğu temel bilgi sistemleri ve bu bilgi sistemleri içinde bulunan kişisel ve kritik veri türlerinin neler olduğuna ilişkin herhangi bir envanter çalışmasının, gerek kurum bazında gerekse Türkiye genelinde yapılmamış olduğu anlaşılmıştır.

Yukarıda yapılan açıklamalar çerçevesinde; kamu kesimi ile bünyesinde önemli hacimde kişisel veri barındıran ya da kritik altyapı yatırımları ile ilgili olan özel kesim ve sivil toplum kuruluşlarının sahip olduğu bilgi sistemleri, bu sistemlerde uygulanan güvenlik önlemlerinin yeterliliği, sistemlerin sahip olduğu kişisel ve kritik veri varlıklarının niteliği gibi konuları kapsayan envanter çalışmasının yürütülmesi, sahip olunan veri varlığının kritik, kişisel, gizli veya hassas olmasına göre alınması gereken güvenlik önlemlerinin belirlenmesine yönelik çalışmalar yapılması gerektiği değerlendirilmektedir.

TESPİT VE ÖNERİ 6- Denetimlerde genel olarak; uygulama, yazılım ve sistemlerin oluşturulması sırasında öncelikle günlük işlerin yürümesine odaklanıldığı, işlerin yürütülmesi ile güvenlik arasındaki denge noktasından uzak olunduğu ve kısa vadede sistemin işleyişi ve çalışır halde bulunmasının daha ön planda tutulduğu anlaşılmıştır.

Bilgi sistemlerinin güvenliğinde yaşanacak sorunların uzun vadede hizmet sunumunun verimi ve kalitesini olumsuz etkilemesi yanında günlük hizmet sunumlarında da aksamalara yol açabileceği dikkate alınarak, bilgi sistemlerinin güvenliğinin tasarım aşamasından itibaren dikkate alınması ve bu kapsamda işlevsellik ile güvenlik arasında denge oluşturulması gerektiği düşünülmektedir.

Denetim sırasında ortaya çıkan bu bulgunun, Ulusal Siber Güvenlik Tatbikatı 2011 Sonuç Raporunda da benzer şekilde yer aldığı görülmüştür. Söz konusu Raporda, sistem tasarımı aşamasında güvenliğin bir temel tasarım prensibi olarak ele alınmadığı, bu durumun ise güvenlik olaylarının yaşanmasını tetiklediği ve yaşanan güvenlik olaylarına etkin müdahaleyi zorlaştırdığı bulgusuna yer verilmiştir.

TESPİT VE ÖNERİ 7- Kamu kurumlarında bilgi güvenliği yönetim sistemi sertifikası alma yönünde ciddi gayretlerin bulunduğu, sertifika sahibi olan kamu kurumlarının bu durumu her türlü platformda belirttikleri görülmektedir. Denetimlerde, sertifikanın kapsamının genellikle kurumun küçük bir birimini kapsadığı, buna rağmen kurum üst yönetiminde tüm kurumu kapsayan güvenlik sertifikasına sahip oldukları yönünde bir algının hâkim olduğu, bu durumun kamuoyuna da aynı şekilde yansıtıldığı görülmüştür. Güvenlik sertifikalarının kapsamının olduğundan farklı gösterilmesi veya kabul edilmesi, kurumlarda güvenlik içinde bulunulduğu yanılsamasına neden olmak ve güvenlik tedbirlerini üst seviyeye çıkarma ve kuruma yaygınlaştırma noktasında gecikme veya eksikliklere yol açmak suretiyle kurum bilgi sistemleri açısından güvenlik riski oluşturmaktadır.

Bilgi güvenliği yönetim sisteminin uluslararası standartlara sahip bir yapıya kavuşması, gerekli güvenlik tedbirlerinin belirlenerek hayata geçirilmesi ve bunun bir sistem dâhilinde yürütülmesi açısından sertifikasyon süreçleri kurumlara olumlu katkılar yapmaktadır. Ancak bu tür sertifikasyonlarda nihai amaç, kurumun bilgi sistemlerinin güvenliğine katkı yapılmasıdır. Bu açıdan güvenlik amacına ulaşmada bir araç olan sertifikalar amaç mertebesine yükseltilmemelidir. Kurumda amacın, gerçek anlamda bilgi güvenliğini sağlayacak yeterli, yetkin, kurumsallaşmış ve yeni tehditlere göre sürekli güncellenen dinamik bir bilgi güvenliği yönetim sisteminin oluşturulması olduğu göz önünde bulundurulmalı, bilgi güvenliği yönetimi sertifikasının kapsamı konusunda yanlış algılara yol açabilecek uygulama ve açıklamalardan kaçınılmalıdır.

B- MEVZUATA İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 8- Kişisel verilerin korunmasına ilişkin olarak Türkiye'de son dönemde bazı temel düzenlemeler yapılmıştır. 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik özel hükümler ihdas edilmiştir. 2010 yılında ise Anayasa'nın 20. maddesinin son fıkrasına yapılan ilave ile kişisel verilerin korunması hakkı Anayasal güvence altına alınmıştır. Ancak, kişisel verilerin korunmasına yönelik çerçeve bir kanun bulunmamaktadır.

Pek çok kanunda kişisel verilerin toplanması konusunda kurumların yetkili olduğunu belirten hükümler mevcut olmakla birlikte, bu yetki çerçevesinde kişisel verilerin hangi ilkeler kapsamında toplanacağı, ne şekilde korunacağı, kimlerle ve ne şekilde paylaşılabileceği, nasıl silineceği, kişilerin Anayasa ile getirilen haklarını kullanabilmeleri için kurumların ne tür önlemler alması gerektiği gibi pek çok hususa genellikle yer verilmediği, bu hususlardan bazılarına yer veren düzenlemelerin ise yeterli düzeyde olmadığı görülmüştür. Bu nedenle, kişisel verilerin korunması konusunda çerçeve kanuna ve diğer kanunlarda kişisel verilerin güvenliğine ilişkin özel düzenlemeler yapılmasına ihtiyaç bulunmaktadır.

TESPİT VE ÖNERİ 9- Bankacılık, sigortacılık, telekomünikasyon, kargo, sağlık, turizm, eğitim, çağrı merkezi ve pazarlama hizmetleri gibi pek çok alanda faaliyet gösteren işletmelerin bilgi sistemleri büyük hacimde kişisel veriyi bünyelerinde barındırmaktadır. Bu şirketlerin, hangi tür kişisel verileri ne şekilde toplayabilecekleri, bunları hangi amaçlarla kullanabilecekleri, kimlerle paylaşabilecekleri, ne kadar süre tutabilecekleri, hangi süre sonunda silecekleri, almaları gereken güvenlik tedbirleri ile kişisel verisi bulunan kişilerin bu verilere erişim, sildirme, düzelttirme gibi haklarını nasıl kullanabileceklerine ilişkin olarak sektör bazlı düzenlemelerin bazı istisnalar dışında yapılmadığı; buna bağlı olarak kişisel veri ihlallerine yönelik denetimlerin gerçekleştirilemediği, ihlallerin tespit edilemediği ve yaptırıma

bağlanamadığı, bu nedenlerle özel kesim açısından kişisel verilerin korunmasındaki boşluk ve risklerin önemli boyutlara ulaştığı ve acil önlem alınması gerektiği değerlendirilmektedir.

C- KİŞİSEL VERİLERİN KORUNMASI HAKKINDA KANUN ÇALIŞMALARINA İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 10- Kişisel Verilerin Korunması Kanunu Tasarısı Taslağında getirilmesi öngörülen istisnalardan bazılarının veri işlemeye ilişkin genel ilkeler dâhil Kanun'un hiçbir hükmünün uygulanmayacağı alanlar ortaya çıkaracağı anlaşılmaktadır.

Bu alana ilişkin bazı uluslararası belgeler ve ülke uygulama örnekleri de göz önünde bulundurulduğunda, demokratik toplumun gerekleri dikkate alınarak ulusal güvenlik, ulusal savunma ve kamu düzeni gibi alanlarda istisnaların getirilebileceği, ancak bu istisnaların kapsam ve sınırlarının belirli ve denetlenebilir olması gerektiği düşünülmektedir. Özellikle veri işlemeye ilişkin genel ilkelere her türlü veri işleme faaliyetinde uyulmasının sağlanması uygun olacaktır.

TESPİT VE ÖNERİ 11- Kişisel Verilerin Korunması Kanunu Tasarısı Taslağında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği ilkesine yer verilmiştir. Ancak açık rızanın tanımı yapılmadığı gibi, hangi unsurları içerdiği de belirtilmemiştir. Bu haliyle, kişisel verilerin korunması hakkı açısından en temel ilkelerden olan kişinin açık rızasının bulunması ilkesinin uygulanmasında sorunlar yaşanması muhtemeldir.

Bu nedenle, uluslararası belge örneklerinde de açıkça görüldüğü üzere, açık rızanın kişinin özgürce, konuyla ilgili yeterli bilgiye sahip olarak, tereddüde mahal bırakmayacak açıklıkta ve sadece işlemin yapılmasına yetecek ve işlemle sınırlı olarak verdiği onay beyanı olarak tanımlanması gerektiği düşünülmektedir.

TESPİT VE ÖNERİ 12- Veri koruma otoriteleri kişisel verilerin korunması açısından güvence sağlayan en önemli unsurlardandır. Veri koruma kanunu bulunan 99 ülkeden 85'inde veri koruma otoritesi oluşturulmuştur. Uluslararası düzenlemelerde bu otoritelerin üzerlerine düşen görevi gerektiği şekilde yerine getirebilmeleri için bağımsız (*independent*), tarafsız (*impartial*) ve teknik kapasite açısından yetkin ve yeterli (*technically competent*) yapıda oluşturulmalarına vurgu yapılmıştır.

Kişisel Verilerin Korunması Kanunu Tasarısı Taslağında Adalet Bakanlığına bağlı, bir başkan, daire başkanları ve yeteri kadar adalet uzmanı ve uzman yardımcısından oluşan Kişisel Verileri Koruma Kurumu oluşturulması öngörülmektedir. Söz konusu yapının uluslararası standartları karşılamaktan uzak ve mevcut haliyle veri koruma otoritesi fonksiyonunu yerine getirip getiremeyeceği hususunun tartışılabilir nitelikte olduğu değerlendirilmektedir.

TESPİT VE ÖNERİ 13- Ceza hükümlerinin beklenen etkiyi doğurabilmesi için cezaların etkinlik, orantılılık ve caydırıcılık niteliklerine sahip olması gerekmektedir.

Kişisel Verilerin Korunması Kanunu Tasarısı Taslağı'nda sınırlı sayıda ihlal türü sayılarak bunlara 100 TL ile 1.000.000 TL arasında değişen idari para cezası verilebilmesi öngörülmüştür. Söz konusu idari para cezalarının, ihlalin türü, etki alanı ve süresi, ihlalin ihmal sonucu ortaya çıkması veya kasten gerçekleşmesi, ilgilinin sorumluluk derecesi ve ihlal geçmişi, alınmış teknik ve kurumsal tedbir bulunup bulunmadığı ve düzeyi, denetleyici otorite ile işbirliği düzeyi gibi hususları da dikkate alacak şekilde düzenlenmesinin cezaların daha etkili, orantılı ve caydırıcı olmasına katkı sağlayacağı değerlendirilmektedir.

TESPİT VE ÖNERİ 14- Raporun önceki bölümlerinde Kişisel Verilerin Korunması Kanunu Tasarısı Taslağı'nda yer alan hükümler detaylı olarak değerlendirilmiş ve kişisel verilerin işlenmesi ve korunması açısından ön plana çıkan hususlara da yukarıdaki tespit ve önerilerde yer verilmiştir. Taslak metinle ilgili diğer tespit ve öneriler ise aşağıda özet olarak sunulmuştur.

Bu kapsamda;

• Taslak metinde yer alan bazı tanım ve kavramlar konusunda belirsizlikler bulunmakta olup, söz konusu kavram ve tanımların gözden geçirilerek yeniden düzenlenmesinin,

• Toplumsal değerler açısından değerlendirildiğinde; kişinin sosyal yardım alıp almadığına veya muhtaçlık durumuna ilişkin verileri ile mahkûmiyet bilgilerinin de hassas veri olarak nitelendirilmesinin,

• Kimlik numarasının diğer pek çok veri ile ilişkiyi ortaya koyma açısından anahtar rol üstlenmesi nedeniyle bu verinin işlenme usul ve esasları bakımından diğer kişisel verilerden farklı olarak değerlendirilmesine yönelik belirleme yapılmasının,

• Özel nitelikli kişisel verilerin işlenme şartlarından bir tanesi olan "ilgili kişinin kendisi tarafından alenileştirilmiş olması" ibaresinin "ilgili kişinin kendisi tarafından sözlü ya da yazılı olarak alenileştirilmiş olması" şeklinde yeniden düzenlenmesinin,

• Verisi işlenen kişinin hakları ile ilgili olarak; veri kütüğü sahiplerinin şeffaf ve kolayca ulaşılabilir politika belgelerinin bulunmasını temin edecek bir düzenlemenin taslağa ilave edilmesinin,

• Taslakta yer alan otomatik işleme ile karar alınmasına yönelik itiraz hakkı, bu konuda yeterli güvence sağlamamakta olduğundan uluslararası düzenlemelere uygun bir yapı oluşturulmasının,

• Kişisel veri ihlaline yönelik olarak Kişisel Verileri Koruma Kurumuna bildirim yükümlülüğü konusunda bir zaman sınırının getirilmesinin,

• Kişisel veri güvenliğine ilişkin yükümlülüklerin veri sorumluları (veri kütüğü sahibi) tarafından benimsenmesini ve alınacak güvenlik önlemlerine ilişkin ilkelerin belirlenmesini sağlamak üzere, veri sorumlularının ayrıca kişisel veri güvenliği politika belgesine sahip olmalarına yönelik bir düzenleme yapılmasının,

• Sivil toplum kuruluşlarına Kişisel Verileri Koruma Kurumuna şikâyet hakkı verilmesinin,

• Kişisel Verileri Koruma Kurumunun şikâyet üzerine ya da re'sen inceleme yetkisinin yalnızca bu Kanun ile sınırlanmamasının, kişisel verilere ilişkin ihlallerin tamamının Kurumun inceleme yetkisi kapsamına dâhil edilmesinin,

• Kişisel Verilerin Korunması Kanunu, uluslararası düzenlemeler ve Avrupa Konseyi tavsiyeleri dikkate alınarak yapılacak sektörel düzenlemelerin belli bir süre içinde yürürlüğe konulmasına ilişkin bir geçiş hükmünün Tasarı Taslağı'nda yer almasının

faydalı olacağı düşünülmektedir.

D- KURUMSAL YAPIYA İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 15- Uluslararası düzenlemeler ve ülke örnekleri incelendiğinde; kişisel verilerin korunması açısından kişisel veri koruma otoritelerinin oluşturulduğu ve bunlara etkin roller verildiği görülmektedir. Türkiye'de kişisel verilerin korunması ile ilgili herhangi bir otorite veya bu konuyla doğrudan görevlendirilmiş bir birim bulunmamaktadır. Kişisel verilerin korunmasına yönelik çerçeve kanun çalışmaları kapsamında bir kurumsal yapılanma üzerinde çalışıldığı bilinmektedir. Kişisel verilerin korunması açısından ön koşul niteliğinde olan bilgi güvenliği konusunda ise, çeşitli kurum ve kuruluşlara bir takım görev ve sorumluluklar yüklendiği, son dönemde bu alanda önemli adımlar atılmasına rağmen, dağınık yapının tam olarak giderilemediği değerlendirilmektedir.

Ulusal bilgi güvenliğini sağlama konusunda dünyada uygulanan kurumsal yapılanma modelleri ve Türkiye'deki mevcut uygulamalar ve yürütülen çalışmalar da dikkate alınarak;

• Mevcut yapıda kurumlar arasındaki yetki çakışması veya görev ve yetki açısından belirsizlikler gibi eksikliklerin giderilmesi,

• Ulusal bilgi güvenliğini sağlama amacına yönelik strateji, politika ve standartların belirlenmesi ve belli zaman aralıklarıyla güncellenmesi,

• Bilgi sistemlerinin tasarımından, ihale süreci, kabulü, işletilmesi, diğer sistemlerle entegrasyonu veya veri paylaşımı gibi bilgi sistemi aşama ve süreçlerinde kurumlara gerekli teknik ve tecrübe desteğinin sunulması,

• Ulusal bilgi güvenliği risklerinin zamanında ve hızlı şekilde tespit ve analiz edilmesine ilişkin mekanizmanın oluşturulması,

• Gerek özel gerek kamu kesiminde yapılacak güvenlik testlerinin niteliği, periyodu, testi yapacak kurumların yetkilendirilmesi, test sonuçlarının değerlendirilmesi gibi konulara ilişkin uygun sistemlerin oluşturulması,

• Kurumlar arasında koordinasyon ve etkin işbirliği imkânlarının artırılması,

• Türkiye'de bilgi sistemleri envanterinin çıkarılması ve bunların önem ve karşı karşıya bulundukları risk derecelerine göre sınıflandırılarak alınması gerekli önlemlerin belirlenmesi ve takibinin sağlanması,

• Bilgi güvenliği ve kişisel verilerin korunması açısından farkındalık oluşturulması ve kültür değişimi büyük önem taşıdığından, bu konuya ilişkin özel çalışmaların yürütülmesi,

• Ulusal bilgi güvenliği alanında uzman personelin önemi dikkate alınarak, yeterli ve yetkin bilişim personeli yetiştirilmesine yönelik önlemlerin geliştirilmesi,

• Yazılımda dışa bağımlılığın oluşturduğu güvenlik riskleri göz önünde bulundurulmak suretiyle, Türkiye'de bilgi sistemleri yazılımlarında yerlilik oranını artırmaya yönelik Ar-Ge çalışmaları başta olmak üzere gerekli adımların atılması,

• Yukarıdaki hususlarda temel belirleyici olarak seçilecek bakanlık veya kurumun yeterli personel, mali ve diğer imkânlarla desteklenmesi

gerektiği değerlendirilmektedir.

TESPİT VE ÖNERİ 16- Bilgi güvenliği uzun süre sadece teknolojik boyutu ile dikkate alınmıştır. Bilgi sistemlerinin kurumların iş süreçlerinin ana unsuru haline geldiği günümüzde ise organizasyonel boyut büyük önem kazanmıştır. Denetim çalışmalarında, kurumların bilgi güvenliğine yönelik olarak organizasyon yapılarında yeterli değişikliğe gitmedikleri görülmüştür.

Kurumların sahip oldukları bilgi sistemlerinin büyüklüğü, önemi ve bu sistemlerde tutulan verilerin niteliği dikkate alınmak suretiyle;

• Kurumun bilgi varlıklarını içeriden veya dışarıdan gelebilecek tehditlere karşı korumak maksadı ile Bilgi Güvenliği Yönetim Sistemi kurmak ve çalıştırmak,

• Güvenlik politikasını oluşturmak, güvenlik standartlarını belirlemek ve güncel tutmak,

• Güvenlik politika ve standartlarını uygulamak, uygulatmak, uygulandığının denetim ve takibini yapmak,

• Bilişim sistemlerinin her türlü iç ve dış tehdide, yetkisiz erişime ve zararlı yazılımlara karşı korunmasına yönelik tedbirlerin alınmasını ve uygulanmasını sağlamak,

• Bilişim sistemleri üzerinde uygulanacak güvenlik kontrollerinin planlanmasına, hazırlanmasına ve uygulanmasına ilişkin çalışmaları yönetmek, uygulanmasını sağlamak, uygulandığının denetimini ve takibini yapmak,

• Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapmak,

• İşlenen, kaydedilen ve saklanan verilerin güvenliğinin sağlanması amacıyla sistem üzerindeki kullanıcı, sunucu, network, uygulama, veri tabanı ve güvenlik donanımı erişim kayıtlarını (log) toplamak, takip ve analizini yapmak,

• Bilişim sistemleri içerisinde meydana gelebilecek güvenlik ihlallerine veya bilgisayar güvenlik olaylarına ilişkin delilleri toplamak, analizini yapmak ve rapor hazırlamak,

• Kullanıcıların bilgi güvenliği konusundaki farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapmak,

• Bilgi güvenliği konularında teknolojinin getirdiği yenilikleri sürekli takip etmek, incelemek ve araştırmak

üzere bilgi güvenliği birimleri oluşturulmalıdır.

Ayrıca bilgi güvenliği birimleri;

• Bağlı oldukları birim ya da içinde bulundukları yapıdan bağımsız olarak çalışabilme kapasitesine sahip olmalıdır.

• Yetkin ve yeterli sayıda personelle güçlendirilmelidir.

• Kurumdaki verilerin yapısı, kurumun görevleri gibi unsurlar dikkate alınarak uzmanlaşmış alt birimlerden oluşmalıdır.

• Üst yönetimin desteğine sahip olmalı, bu birimlerin tespitleri mutlaka değerlendirilmeli ve tespit edilen hususlarla ilgili gerekli önlemler alınmalıdır.

E- KİŞİSEL VERİ PAYLAŞIMINA İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 17- Diğer kamu kurumları ve özel kesim ile veri paylaşımında, hukuki dayanağın bulunup bulunmadığı, verilerin talep eden kurum için gerekliliği, talep edilen verinin

ilgili kurumun hizmet gerekleri ile orantılı düzeyde olup olmadığı gibi hususlarda yeterli analizin yapılmadığı ve etkin karar mekanizmalarının oluşturulmadığı görülmüştür.

Bu nedenle günümüzde kurum ve kuruluşların en değerli varlıklarından biri haline gelen kişisel verilerin paylaşımında öncelikle;

• Paylaşımın amacının net olarak belirlenmesi,

• Bilgi paylaşmanın ya da paylaşmamanın kişiler, kurumlar ve toplum için oluşturduğu potansiyel yararların ve maliyetlerin tespit edilmesi,

• Bilgi talebinde bulunan kurumun söz konusu kişisel veriler ile sunduğu hizmet arasındaki ilişki ve bu verilerin paylaşımına ilişkin gereklilik durumu,

• Talep edilen verilerin mahiyeti itibariyle hassas kişisel veri içerip içermediği,

• Veri talebinde bulunan kurum veya kuruluşların yasal olarak bu verileri almaya yetkili olup olmadıkları, hukuki dayanakları ve gerekçeleri, talep edilen verinin türü, şekli ve miktarının yürütülen iş ve işlemler ile orantılılığı

gibi hususların değerlendirilmesi ve değerlendirmenin, konunun hukuki, idari ve teknik boyutlarının tümünü kavrayacak bilgi ve uygun yetki düzeyine sahip bir kurul tarafından gerçekleştirilmesi gerekmektedir.

TESPİT VE ÖNERİ 18- Bazı kamu kurumlarının sahip olduğu verileri çevrimiçi (online) olarak kamu ve özel kesim kurum ve kuruluşları ile paylaştıkları görülmüştür. Ancak veri paylaşım talebinde bulunan kurum ve kuruluşların kişisel veriler dâhil çevrimiçi olarak ilgili kurumdan alacağı verilerin güvenliğini sağlama konusundaki yeterliliğinin araştırılmadığı, bu hususun veri paylaşım protokollerine de ya hiç, ya da yeterince yansıtılmadığı, paylaşılan verileri alan kurumdaki güvenlik düzeyi ile ilgili olarak, genellikle herhangi bir çalışma ve araştırmanın yapılmadığı tespit edilmiştir.

Kişisel verilerin güvenliği açısından hayati öneme sahip olan, bilginin paylaşıldığı kurum ve kuruluşlardaki güvenlik önlemlerine ilişkin olarak veri paylaşımına ilişkin sözleşmelerde aşağıdaki hususlara yer verilmesi gerektiği değerlendirilmektedir:

• Her ortam ve bilgisayardan çevrimiçi veri paylaşımının doğurabileceği güvenlik risklerini minimize etmek amacıyla, veri erişimlerinin sabit IP adresleri üzerinden gerçekleştirilmesi,

• Çevrimiçi sorgu yapılacak bilgisayar ve sorgulama yapacak kişi sayısı,

• Çevrimiçi veri erişim yetkisi verilen tüm kullanıcıların ad, soyad ve T.C. kimlik numaralarının kayıt altında tutulması,

• Çevrimiçi veri erişim yetkisi verilen personelin görev ve yetkilerine göre ulaşabilecekleri verilerin kategorilere ayrılması,

• Kullanıcıların yapmış oldukları sorguların kayıtlarının (log) tutulması ve bunların belirlenecek bir süre için uygun güvenlik önlemleri alınarak saklanması,

• Sorgu sonucunda elde edilen kişisel bilgilerin ayrı bir veri tabanı oluşturacak şekilde kurum sistemlerine kayıt edilip edilemeyeceği ve kayıt edilecekse alınacak güvenlik tedbirlerine ilişkin detaylı düzenlemeler,

• Sorgulama yapılan bilgisayarlar ile internet arasında mutlaka güvenlik duvarı (firewall) ve Saldırı Tespit ve Önleme Cihazı (IPS) bulundurulması gibi güvenlik sağlayıcı önlemler,

• Sorgulama yapılan bilgisayarlarda güncellenen anti-virüs programı olması,

• Sorgulama ekranına giriş için kullanıcı adı ve güçlü şifre aranması, yazılı parola politikasının bulunması,

• Sorgulama yetkisi verilmiş olanlara, "sistemden sadece kurumun tanımlanmış iş ve işlemleri için sorgu yapacakları sistemi ve sistemdeki verileri başka amaçlar için kullanmayacakları, kullanmaları durumunda Türk Ceza Kanunu, kamu görevlisi ise ilgili disiplin hükümleri ve diğer tazminat hükümlerinin söz konusu olacağı" hususunun yazılı olarak imza karşılığında mutlaka bildirilmesi,

• Sistemi amacı dışında kullandığı tespit edilen personelin vakit kaybetmeksizin yetkili makamlara ve veri sağlayan kuruma bildirilmesi gerektiği,

• Çevrimiçi veri sağlayan kurumun veri talep eden kurum veya kuruluşun yukarıdaki şartları sağlayıp sağlamadığı ve uygulamanın söz konusu hususlara uygun olarak yapılıp yapılmadığı konusunda kontrol yetkisinin ve gerektiğinde dava açma ve tazminat talep etme yetkisinin bulunduğu.

Yukarıdaki hususlara ilaveten;

• Sözleşme yapılmadan önce veri paylaşılan kurumun bilgi güvenliği ve kişisel verilerin korunması açısından yeterli altyapıya sahip olup olmadığı hususunun değerlendirilmesi, gerekli görülen durumlarda yerinde incelenmesi,

• Bilgi paylaşımının verilerin güvenliği için gerekli ve belirlenen asgari kriterleri yerine getiren kurumlarla gerçekleştirilmesi,

• Bilgi paylaşımı gerçekleştikten sonra da sözleşme hükümlerine uygun hareket edilip edilmediğinin tespitine yönelik mekanizmaların oluşturulması,

• Gerekli şartları kaybettiği ya da ihlal ettiği tespit edilen kurum ve kuruluşlarla yapılan anlaşmaların feshedilmesi ve ihlalin niteliğine göre gerekli idari veya adli prosedürlerin başlatılması

gerektiği düşünülmektedir.

TESPİT VE ÖNERİ 19- Gerek bilgi sistemleri incelenen kamu kurumları gerekse bu kurumların çevrimiçi olarak kişisel veri paylaştığı kamu ve özel sektör kurum ve kuruluşları üzerinde yapılan incelemelerde çevrimiçi olarak yapılan sorgulara ilişkin kayıtların (log) tutulmasına ilişkin aşağıdaki eksiklikler tespit edilmiştir:

• Sorgu kayıtlarının veriyi sağlayan kurumlarca genellikle tutulduğu ancak bazı kurumlarda sorgu kaydı tutma mekanizmasının yeterince etkin olmadığı, bazı kurumlarda ise sorgu kaydının veri paylaşılan tüm kurumları kapsamadığı görülmüştür.

• Bazı kurumlarda sorgu kaydı olarak tutulan kayıtların, sorgunun yapılış zamanı, sorguyu yapan kişi ve sorgu sonucunda ulaşılan veriler konusunda yeterli içeriğe sahip olmadığı, bu haliyle gerçek bir sorgu kaydı hüviyetinden ve sorgu kayıtlarının tutuluş amaçlarına hizmet etmekten uzak olduğu tespit edilmiştir.

• Erişim kayıtlarına ilişkin sorgu kayıtları hem veri paylaşan hem de veri alan kurumlar nezdinde çapraz incelemeye tabi tutulmuş, iki kurumdaki sorgu kayıtları arasında tutarsızlık ve farklılıkların bulunduğu görülmüştür. Bu durum sorgu kaydı tutma mekanizmalarının güvenilirliği konusunda ciddi şüphe uyandırmıştır.

• Veri paylaşılan kamu ve özel sektör kurum ve kuruluşlarının kendi bünyelerinde tutmaları gereken sorgu kayıtlarına ilişkin 36 kurum ve kuruluşta yapılan incelemede; kurumların 7'si sistemi kullanan kullanıcıların yapmış oldukları sorguların kayıtlarının tutulmadığını, 4'ü de erişim kayıtlarının bir yıl ve altında süreyle tutulduğunu ifade etmiştir.

• Tutulan erişim kayıtları üzerinde hemen hemen hiçbir kurumda herhangi bir takip ve analiz çalışması yapılmamaktadır. Kurumlar yalnızca erişim kayıtlarını tutmakla yetinmekte olup, kurumlarda erişim kayıtları üzerinde düzenli olarak çalışma yapan personel bulunmamasının yanı sıra, takip ve analizi otomatik olarak yapacak merkezi kayıt yönetim yazılımı ve benzeri uygulamalar da genellikle kullanılmamaktadır.

Kişisel verilere yetkisiz erişimlerin tespiti, önlenmesi ve bu tür erişimlerde bulunanların adli ve idari olarak cezalandırılabilmesi açısından çevrimiçi olarak yapılan sorgu kayıtlarının sağlıklı bir şekilde tutulması önem taşımaktadır. Bu kapsamda aşağıdaki hususlara riayet edilmesi gerekmektedir:

• Çevrimiçi veri paylaşımlarına ve kurum içi sorgulamalara ilişkin erişim kayıtları mutlaka veri paylaşılan kurumların ve kurum içi sorgulama yapan kişilerin tamamını kapsayacak şekilde tutulmalıdır.

• Tutulan erişim kayıtları, kaydın tutuluş amacını yerine getirecek düzeyde olmalı, erişim kaydı verileri hangi verinin, kim tarafından, ne zaman görüntülendiği konusunda yeterli ve sağlıklı veriyi sunacak biçimde tutulmalı, silinmeyi ve değiştirilmeyi önleyecek şekilde ve bu konuda yapılabilecek adli ve idari soruşturma ve kovuşturma aşamasındaki zamanaşımı süreleri dikkate alınarak belirlenecek bir süreyle muhafaza edilmelidir.

• Veri paylaşan kurumlar sadece tanımlanan IP adresi üzerinden yapılan erişim kayıtlarını tutmaktadırlar. Bununla birlikte veri alan kurumların personel bazında kimin, hangi veriye, ne zaman, nereden eriştiği gibi bilgileri içeren sorgu kayıtlarını tutması beklenmektedir. Bu nedenle, sorgu kayıtları sadece veriyi sağlayan kurum nezdinde değil veriyi alan kurum nezdinde ve personel bazlı olarak da tutulmalı, sözleşmelerde açıkça belirtilecek sürede ve güvenli olarak saklanmalı, istenildiğinde veriyi sağlayan kuruma sunulmalıdır.

• Kişisel verilerin güvenliği ve bu konuda oluşabilecek suiistimallerin tespit ve önlenmesi açısından çevrimiçi sorgu kayıtları üzerinde düzenli olarak takip ve analiz çalışması yapılmalı, söz konusu takip ve analiz çalışmasını otomatik olarak yapacak merkezi kayıt yönetim yazılımı ve benzeri uygulamalar kullanılmalıdır.

TESPİT VE ÖNERİ 20- Denetim çalışmaları sırasında kamu kurumlarının sahip oldukları pek çok kişisel ve hassas veriyi CD, DVD, taşınabilir bellek gibi taşınabilir elektronik ortamlar kullanarak çevrimdışı paylaştıkları görülmüştür. Çevrimiçi veri paylaşımında sorgu kayıtları aracılığı ile kontrol imkânı bulunmasına rağmen, çevrimdışı paylaşılan veriler üzerinde herhangi bir kontrol imkânı da kalmadığından, bu verilerin paylaşımına ilişkin gerekli güvenlik önlemlerinin alınması büyük önem taşımaktadır. Buna rağmen, bazı örneklerde milyonlarca kişinin kimlik ve adres bilgisinin bulunduğu bilgilerin şifrelenmeden, kopyalanmaya karşı herhangi bir güvenlik önlemi alınmadan CD ortamında iletildiği; söz konusu verilerin ilgili kurumda hangi güvenlik önlemleri alınarak muhafaza edileceği ve kullanılabileceği, çoğaltılıp çoğaltılamayacağı, söz konusu bilgilere olan ihtiyacın ortadan kalkması durumunda taşınabilir elektronik ortamın ne şekilde imha edileceği gibi hiçbir güvenlik hususunun belirlenmediği tespit edilmiştir.

Kişisel verilerin çevrimdışı olarak paylaşımının ortaya çıkarabileceği güvenlik riskleri dikkate alınmak suretiyle aşağıdaki hususlara uygun davranılması gerektiği düşünülmektedir:

• Çevrimiçi veri paylaşımlarında olduğu gibi, düzenli olarak gerçekleştirilecek çevrimdışı veri paylaşımları mutlaka bir sözleşmeye bağlanmalıdır. Söz konusu sözleşmelerde, verilerin

hangi kayıt ortamlarında, hangi aralıklarla, hangi güvenlik önlemleri alınarak paylaşılacağı, veri içeren kayıt ortamlarının hangi vasıtalarla iletileceği hususları aşağıda ifade edilen hususları da kapsayacak biçimde mutlaka yer almalıdır.

• Talep edilen verilerin veri tabanından kim veya kimler tarafından çekileceği, çekilen verilerin nasıl muhafaza edileceği önceden belirlenmelidir.

• Veri paylaşımı gerçekleştirilirken kişisel veri içeren dosyalar uygun şifreleme programları kullanılarak şifrelenmeli, değiştirilmeye karşı önlem olarak dosyaların parmak izi sayılan "hash" değeri alınmalıdır.

• Kişisel veri paylaşımlarında mümkün olduğunca verinin elden yetkili kişilere imza karşılığı teslimi yöntemi tercih edilmelidir. E-posta, posta, kargo ve benzeri vasıtaların kullanımından mümkün olduğunca kaçınılmalıdır.

• Veriyi alan kurumda söz konusu verinin kime ya da kimlere teslim edileceği, çoğaltılıp çoğaltılamayacağı, çoğaltılacak ise kaç kopya yapılabileceği, kopyaların kimler tarafından hangi yöntemlerle muhafaza edileceği önceden belirlenmelidir. Özellikle hacimli ve hassas kişisel veri içeren elektronik kayıt ortamlarının sadece belli bir bilgisayar üzerinde çalışabilmesi ve bu bilgisayarda değiştirilemez şekilde verilere kimlerin eriştiğine ilişkin kayıtları tutabilecek sistemlerin oluşturulması imkânları kullanılmalıdır.

• Kullanım amacı ortadan kalkan kişisel verileri içeren elektronik kayıt ortamlarının ne şekilde imha edileceği ilgili kuruma bildirilmelidir.

• Yukarıdaki hususlara aykırı davranışların ne tür hukuki, cezai veya idari yaptırıma konu olabileceği, kişisel verilerin kurumun yetersiz güvenlik önlemleri nedeniyle amaç dışı kullanımı veya yetkisiz kişilerin eline geçmesi durumunda ilgili kurumun sorumluluklarının neler olacağı hususu ilgili kurum yetkililerine bildirilmelidir.

TESPİT VE ÖNERİ 21- Kurumlar tarafından gerek çevrimiçi gerekse çevrimdışı olarak hem kamu hem de özel kesim ile veri paylaşımı yapılmasına rağmen, pek çok kurumda kişisel verilerin paylaşımında uyulacak usul ve esasları belirleyen herhangi bir düzenlemenin bulunmadığı, buna bağlı olarak veri paylaşımlarında büyük oranda kişisel takdir ve değerlendirmelerin etkili olduğu, standartları önceden belirlenmiş güvenlik önlemleri alınmaksızın veri paylaşımları yapıldığı görülmüştür.

Bu nedenle Anayasa'nın 20. maddesi hükmü ve Avrupa Konseyi Bakanlar Komitesince yayımlanan Kamu Makamlarının Elinde Bulunan Kişisel Verilerin Üçüncü Kişilere İletilmesine İlişkin Tavsiye Kararı da dikkate alınarak;

• Kurumların sahip olduğu kişisel verileri paylaşma yetki, usul ve esaslarına ilişkin temel çerçevenin kanun düzeyinde belirlenmesi,

• Kanuni düzeyde belirlenen yetki, ilke, usul ve esaslara uygun olmak şartıyla, veri paylaşımlarının gerekli güvenlik önlemleri de alınmak suretiyle yerine getirilmesini sağlamaya yönelik ikincil düzenlemelerin yapılması,

• Veri paylaşımına ilişkin olarak kurumlara ve paylaşılan kişisel verilerin niteliğine göre standart sözleşme formatlarının geliştirilmesi

gerektiği değerlendirilmektedir.

F- BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİNE İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 22- Bir kurumun bilgi güvenliği hedefini ve bu hedefe ulaşmak için uygulanacak kural ve metotların çerçevesini çizen yazılı bilgi güvenliği politikasının bulunması ve bu politika belgesinin tüm çalışanlar ile ilgililere duyurulması gerekmektedir. Denetimlerde kurumların çoğunun bilgi güvenliği sistemi oluşturma açısından başlangıç noktası olarak kabul edilen bilgi güvenliği politikasına sahip olmadığı veya bu isimle sunulan bazı belgelerin politika belgesi niteliğini taşımadığı, bilgi güvenliği politika belgesi bulunan kurumlarda ise kurum personelinin politika belgesinden yeterince haberdar olmadığı tespit edilmiştir.

Bilgi güvenliği açısından temel teşkil eden bilgi güvenliği politikası konusunda yapılması gerekenler ana başlıkları ile aşağıda sunulmaktadır:

• Kurumlar tarafından, sahip oldukları bilgi sistemlerinin ve bilgi varlıklarının niteliği, yaygınlığı, karşı karşıya bulunduğu risk ve tehditler gibi unsurlar analiz edilmek suretiyle kurum ihtiyaçlarına uygun yazılı bilgi güvenliği politikası oluşturulmalıdır.

• Güvenliğin ancak bir bütün halinde sağlanabileceği hususu dikkate alınarak, bilgi güvenliği politikası kurumun tüm birimlerini kapsamalıdır.

• Oluşturulan politika belirli aralıklarla gözden geçirilmeli, değişen yapı ve ihtiyaçlar çerçevesinde güncellenmelidir.

• Bilgi güvenliği politikaları ve politikalarda gerçekleştirilen güncellemeler kullanıcılara ulaştırılmalı ve kullanıcıların ilgili dokümanları okuduğunu ve kabul ettiğini kayıt altına almaya yönelik uygun mekanizmalar oluşturulmalıdır.

TESPİT VE ÖNERİ 23- Denetimlerde, yazılı bir yedekleme politikası bulunmayan veya politika belgesi ile yedekleme uygulaması arasında uyumsuzluk bulunan kurumların olduğu tespit edilmiştir. Bu nedenle, yedeklemelerin kişilere bağlı ve bağımlı olarak gerçekleştirildiği, yapılan yedeklemelerin başarılı olup olmadığını tespite yönelik kontrol ve uyarı mekanizmalarının ya hiç bulunmadığı ya da zayıf olduğu anlaşılmıştır. Bilgi sistemlerinde

oluşabilecek yazılım ve donanım arızaları, sistem kesintileri, doğal afetler veya saldırılar gibi nedenlerle kurum bilgi sistemlerindeki veri kayıplarını önlemek açısından verilerin yedeklenmesi büyük önem taşımaktadır.

Bilgi güvenliği ve bu kapsamda bilgi sistemlerinin sürekli çalışabilirliğinin sağlanması açısından yedekleme konusunda aşağıdaki tedbirler alınmalıdır:

• Hangi bilgi sisteminin, ne şekilde, ne sıklıkta ve nasıl yedeğinin alınacağını içeren yazılı bir yedekleme politikası oluşturulmalıdır.

• Oluşturulan politikaya uygun bir yedekleme sistemi kurulmalıdır. Bu sistem tüm kritik sistemlerden yedek almalıdır.

• Yapılan yedekleme işlemlerine dair kayıtlar tutulmalı ve düzenli olarak kontrol edilmelidir.

• Yedekleme ve alınan yedeklerden geri dönüş testleri düzenli olarak yapılmalı ve uygun yöntemlerle kayıt altına alınmalıdır.

• Yedeklerin teyp kartuşlarına da alınması sağlanmalı ve bu kartuşlar bilgi işlem merkezinden farklı bir yerde gerekli güvenlik önlemleri alınmak suretiyle muhafaza edilmelidir.

• Yedeklemeler şifreli olarak gerçekleştirilmelidir.

TESPİT VE ÖNERİ 24- Günümüzde pek çok kurumun iş ve işlemlerini yürütmesi, bilgi sistemlerinin işler tutulmasına bağlıdır. Bu çerçevede bilgi sistemlerinin iş sürekliliği ve bir felaket durumunda ayrı bir merkezden hizmet vermeye devam edebilmesi önem kazanmıştır. Denetimlerde, iş sürekliliği ve felaket kurtarma konusundaki farkındalığın yetersiz olduğu, çoğu kurumun iş sürekliliği ve felaket kurtarma politika ve senaryolarına sahip olmadığı, omurga veri tabanına sahip bazı kurumların felaket kurtarma merkezinin dahi bulunmadığı tespit edilmiştir.

İş sürekliliği ve felaket kurtarma merkezleri oluşturma konusunda aşağıdaki hususların göz önünde bulundurulması gerektiği düşünülmektedir:

• Normal çalışma zamanı ile ilgili iş sürekliliği politikası oluşturulmalıdır.

• Bu politikada kritik sistemlere ait idame süreçleri yazılı hale getirilmelidir.

• Oluşturulan bu süreçler düzenli olarak gözden geçirilmeli, değişen şartlara ve eklenen sistemlere uygun olarak güncellenmelidir.

• Kritik sistemlere yönelik tehdit ve riskler ile bu riskleri ortadan kaldırmak için gerekli önlemler ve sorumluların belirlendiği acil durum politikası oluşturulmalı ve bu politikalar belirli aralıklarla gözden geçirilmelidir.

• Acil durum politikasında felaket durumunda yapılacak işlemler de belirlenmelidir.

• Büyük çaplı doğal felaket durumları için kuruma ait ve fiziksel olarak ayrı bir yerde felaket kurtarma merkezi kurulmalıdır.

• Kurulan bu merkezde kurum bilgi sistemlerinin bir örneği olmalıdır.

• Kurum ana bilgi işlem merkezi ile felaket kurtarma merkezinin düzenli aralıklarla senkronize olması ve bu sayede güncel kurum verilerinin felaket kurtarma merkezinde de bulunması sağlanmalıdır.

• Felaket kurtarma merkezinin etkinliğini ölçmek amacıyla tatbikatlar yapılarak kurum hizmetleri belirli aralıklarla felaket kurtarma merkezindeki bilgi sistemleri üzerinden verilmelidir.

TESPİT VE ÖNERİ 25- Denetimlerde, bilgi işlem personeli ve kurum çalışanlarında güvenlik konusundaki farkındalığın çok düşük olduğu görülmüştür. Güvenlik farkındalığının artırılmasına yönelik olarak, kurum personeline düzenli olarak bilgi güvenliği farkındalık eğitimlerinin verilmesi, farkındalığı ölçmek amacıyla düzenli aralıklarla sosyal mühendislik sızma testleri yapılması ve benzeri çalışmaların gerçekleştirilmesi gerekmektedir.

TESPİT VE ÖNERİ 26- Bilişim sistemlerine yetkisiz erişimlerin engellenmesi açısından, bu sistemlere erişimlere ilişkin yetkilendirmeler ile bu yetkilerin kaldırılması süreçlerinin belirlenmesi gerekmektedir. Denetimlerde; gerek bilişim hizmeti satın alınan firma personelinin gerekse kurum çalışanlarının yetkilendirilmesi ve işten ayrılma, uzun süreli izin veya ara verme durumunda bilgi sistemine giriş yetkilerinin kaldırılması konusunda süreçlerin net bir şekilde belirlenmediği, bu nedenle de emeklilik, istifa, işten çıkarılma gibi nedenlerle, işten ayrılma ve aylıksız izin, askerlik, doğum izni gibi uzun süreli işe ara vermelerde gerek firma personelinin gerekse kurum çalışanlarının sisteme erişim yetkilerinin dondurulması veya kaldırılmasında uzun süreli gecikmelerin yaşandığı tespit edilmiştir.

Bilgi sistemlerine yetkisiz erişimlerin önüne geçmek ve bu alanda oluşabilecek güvenlik açıklarını en aza indirmek amacıyla aşağıdaki hususların göz önünde bulundurulması gerektiği değerlendirilmektedir:

• Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların işten ayrılma, uzun süreli ara verme, sözleşmelerin sonlandırılması durumları göz önünde bulundurularak, bu kişilerin erişim hakları dondurulmalı veya iptal edilmelidir. Bu sayede ilgili personelin görevli olmadığı zamanlarda personele ait parola ve erişim haklarının kendisi veya kötü niyetli başkaları tarafından bilgi sistemlerine erişmek ve zarar vermek için kullanılması önlenmiş olacaktır.

• Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların yetkilerinin düzenlenmesi için; personelin işe girme, işten ayrılma ve geçici işe ara verme işlemlerinde bilgi sistemlerindeki yetkilerinin alınması veya dondurulması ile ilgili süreç ve politika belirlenmelidir. Belirlenen bu

politika masaüstü bilgisayarlar, kritik sunucu sistemleri, kurumsal uygulamalar gibi tüm bilgi sistemlerine uygulanmalıdır.

• Kurumların insan kaynakları birimleri ile bilgi işlem birimleri eşgüdüm halinde çalışmalı, personelin işten ayrılma, uzun süreli ara verme (askerlik, aylıksız izin, uzun süreli sağlık izni, doğum izni ve benzeri), sözleşmelerin sonlandırılması durumlarında otomatik olarak bu personele ait sisteme giriş yetkilerinin dondurulması veya kaldırılmasına yönelik mekanizma geliştirilmelidir.

TESPİT VE ÖNERİ 27- Kurumların çoğunun, bilişim sistemlerinin kurulması veya işletilmesi nedeniyle bilişim sistemlerine ve bu sistemlerde bulunan verilere ilişkin bilgilere sahip olan bilişim hizmeti alınan firmalarla gizlilik sözleşmesi imzalamadıkları, imzalanan bazı gizlilik sözleşmelerinin ise içerik olarak yeterli güvenceyi sağlamaktan uzak olduğu tespit edilmiştir.

Bu nedenle bilişim hizmeti alınan firmaların gizliliğe uymalarını temin amacıyla; ilgili kurum ile kuruma hizmet veren firma arasında yasal yönden bağlayıcı olan ayrı bir gizlilik anlaşması imzalanmalı ve gizlilik anlaşmasında en az aşağıdaki hususlara yer verilmelidir:

• Kuruma ait ve anlaşmaya konu veri ve bilgilerin neler olduğu,

• Bu bilgilerin yetkisiz olarak ifşa edilmesini engellemek için tarafların yükümlülükleri ve alacakları tedbirler,

• Anlaşmanın sona ermesi durumunda bilgi ve veriler ile ilgili olarak yapılacak işlemler ile kuruma iade edilecek ve imha edilecek bilgiler,

• İhtiyaç halinde anlaşmaya uygun hareket edilip edilmediğinin tespiti için firma nezdinde izleme ve denetim yapma konusunda kurumun yetkili olduğu,

• Bilgi ve verilerin yetkisiz ifşası veya gizliliğin ihlali durumunda ifşa ve ihlallerin raporlanması ve bildirimi ile ilgili süreçler,

• Anlaşmanın ihlal edilmesi durumunda uygulanacak müeyyideler ile bu konuda yetkili olacak mahkemeler,

• Kuruma özgü ilave unsurlar.

TESPİT VE ÖNERİ 28- Pek çok kamu kurumu bilgi sistemlerinin kurulması ve işletilmesi amacıyla özel ticari işletmelerden hizmet satın almaktadır. Söz konusu işletme çalışanlarının bazıları, kurum bilgi sistemlerinde üst düzey erişim yetkileri ile çalışmakta, bilgi sistemleri üzerinde önemli kontrol yetkisine sahip olmakta ve pek çok kişisel, hassas, hatta kritik veriye ulaşabilmektedir. Buna rağmen, kurumların büyük ekseriyetinde kurumlarda çalışan yüklenici firma personeline ilişkin güvenlik araştırması dahi yapılmadığı, bu personelle, bilgi sistemleri ve

buradaki verilere ilişkin edindikleri bilgilerin gizliliğini koruyacaklarını ve korumamaları durumundaki yükümlülüklerini belirtilen bir gizlilik sözleşmesinin de imzalanmadığı tespit edilmiştir.

Kurum bünyesinde bilgi sistemlerinin kurulması veya işletilmesinde istihdam edilecek yüklenici firma personeli ile ilgili olarak aşağıdaki hususlara riayet edilmesi önem taşımaktadır:

• Kurumda yer alan verilerin hassasiyeti göz önünde bulundurularak; firma çalışanları güvenlik açısından detaylı araştırılmalı ve şartnamelere sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

• Kurumun bilgi sistemlerinde çalışacak ve kritik bilgilere erişme ihtimali bulunan firma personeli için güvenlik araştırması yapılmalıdır.

• Kurumun bilgi sistemlerinde çalışacak ve kritik veya kişisel verilere erişme ihtimali olan tüm personel (kurum ve firma personeli dâhil) ile yasal sorumlulukların açıkça belirtildiği gizlilik sözleşmeleri imzalanmalıdır.

TESPİT VE ÖNERİ 29- Parola, bilgi sistemlerine girişte güvenliğin sağlanmasında kullanılan araçlardan birisidir. Denetimlerde; pek çok kurumda güçlü parola oluşturulması, parolaların belli periyotlarla değiştirilmesi, parolaların gizliliğine ilişkin personelin yükümlülükleri gibi hususları içeren yazılı parola politikasının bulunmadığı; parola politikası bulunan bazı kurumlarda ise söz konusu politikanın yeterince uygulamaya geçirilmediği tespit edilmiştir. Parola politikasının bulunmaması veya etkin bir şekilde uygulanmaması sonucunda, kurumlarda iki haneli veya 1111, 0000, 1234 gibi kolayca tahmin edilebilir parolalar ile ilk kez verilen parolaların değiştirilmeden kullanılması, parolanın e-posta ile iletilmesi, diğer personelle sıklıkla paylaşılması gibi bilgi güvenliği açısından önemli risk oluşturabilecek pek çok uygulamanın ortaya çıktığı görülmüştür.

Bu kapsamda; aşağıdaki hususların dikkate alınması gerektiği değerlendirilmektedir:

• Politikanın oluşturulmasında kurumun sahip olduğu bilgi sistemlerinin ve bilgi varlıklarının niteliği, yaygınlığı, karşı karşıya bulunduğu risk ve tehditler gibi unsurların analizi yapılmalı ve bu analizler sonucunda kurum ihtiyaçlarına uygun bir parola politikası oluşturulmalıdır.

• Belirlenecek politika en azından internete açık kurumsal uygulamalar, masaüstü işletim sistemleri, kritik sunucular, veri tabanı sistemleri, ağ donanımları ve güvenlik cihazlarını kapsamalıdır.

• Politikaya uygun olarak, tüm bilgi sistemlerinde ilgili yetkilendirme mekanizmaları devreye alınmalıdır.

• Özellikle saldırı ihtimali daha yüksek olan internete açık kurumsal uygulamalar ile hassas veri bulunduran sunuculara girişler için SMS, e-imza, akıllı kart ve biyometrik yöntemler gibi güçlü yetkilendirme mekanizmaları kullanılmalıdır.

• Güvenlik testleri ile parola politikaları ve yetkilendirme mekanizmalarının etkinliği düzenli olarak denetlenmeli, yeni risk ve tehditlere yönelik önlemler geliştirilmelidir.

TESPİT VE ÖNERİ 30- Bilgi sistemlerinin zaman içinde gelişip büyümesine paralel olarak, kurumlarda birden fazla sistem veya uygulama devreye sokulmaktadır. Bunun sonucunda da farklı sistem veya uygulamalar için birbirinden bağımsız yetkilendirme mekanizmaları oluşturulmaktadır. Bu durumda, aynı kurumun farklı sistemlerine giriş yetkilendirmeleri ve bu sistemler üzerindeki denetimler güçleşmekte, güvenlik açıkları ortaya çıkabilmektedir. Bu tür sorunları aşabilmek için merkezi kimlik yönetimi sistemleri devreye sokulmaktadır. Denetimlerde, kurumların çok sayıda uygulamayı, farklı yetkilendirme mekanizmaları kullanarak yetkilendirdiği, merkezi kimlik yetkilendirme sistemi kullanmadığı, konuya ilişkin olarak farkındalığı nispeten yüksek bir kurumda bu amaçla bir yazılım alındığı, ancak yazılımın lisans kısıtlaması ve teknik özelliklerinin kısıtlılığı nedeniyle tüm sistemlere entegre edilemediği tespit edilmiştir.

Yetkilendirme mekanizmalarına etkinlik kazandırmak ve bu suretle bilgi güvenliğini artırmak amacıyla, bilgi sistemlerinin büyüklüğü ve veri varlıklarının önemi gibi hususlar da dikkate alınarak, aşağıda sayılan önlemlerin alınabileceği değerlendirilmektedir:

• Kurumlarda sunucu, veri tabanı, son kullanıcı bilgisayarları, ağ cihazları, web uygulamaları da dâhil olmak üzere kullanılan tüm bilgi sistemlerini kapsayan merkezi kimlik yönetim sistemi kurulmalıdır.

• İnsan kaynakları sisteminin merkezi kimlik yönetim sistemi ile entegre edilmesi, personelin işe giriş ve işten ayrılması esnasında personele ait tüm hakların (kullanıcı bilgisayarı, iç/dış uygulamalar, sunucular) merkezi olarak verilmesi ve kaldırılması sağlanmalıdır.

• Self-servis portal sistemi kurularak, kurum uygulamalarını kullanan kullanıcılara parolalarını kurum parola politikasına uygun şekilde belirli aralıklarla değiştirebilme imkânı sunulmalıdır.

• Yapılan tüm yetkilendirme ve kimlik yönetimi işlemlerine ait kayıt bilgilerinin tutulması ve bu kayıt bilgilerinin merkezi kayıt yönetim sisteminde saklanması sağlanmalıdır.

TESPİT VE ÖNERİ 31- Bilgi sistemlerinde kullanılan yazılımlarda ortaya çıkan hata ve açıklıkların giderilmesi amacıyla, düzenli olarak yama programları yayımlanmaktadır. Bu yamaların ilgili programlara uygulanmaması verilerin geçici veya kalıcı olarak zarar görmesine veya sistemlerin saldırılara açık hale gelmesine neden olmaktadır. Denetimlerde, yama yönetimi

süreçlerini açık şekilde tanımlayan yazılı hale getirilmiş yama yönetimi politikasının çoğu kurumda bulunmadığı, yama yönetimi politikası bulunan kurumlarda ise sürecin politikaya uygun şekilde işletilmediği, yama yönetim süreçlerinin tüm sistemleri kapsamadığı ve büyük oranda kişilere bağlı ve bağımlı şekilde yürütüldüğü görülmüştür. Bünyesinde hassas kişisel veriler bulunan bir kamu kurumundaki güvenlik testi sonucunda, yama eksiğinden dolayı kuruma ait 500 sunucunun bir saat gibi kısa bir sürede ele geçirilebildiğinin görülmesi, kurumların yama politika ve süreçlerine vermeleri gereken öneme işaret etmektedir.

Yama yönetimi, bilgi sistemlerinin ve bu sistemlerdeki kişisel veriler dâhil veri varlıklarının güvenliği açısından gerekli bir unsurdur. Bu konudaki eksiklik veya gecikmeler, kurumların temel fonksiyonlarını yerine getirememesi, verilerin zarar görmesi veya yetkisiz kişilerin eline geçmesi gibi pek çok güvenlik riskini bünyesinde barındırmaktadır. Türkiye'de bu alandaki mevcut durumun yeterli seviyede olmadığı hususu özellikle dikkate alınarak, aşağıdaki adımların ivedilikle atılması gerektiği değerlendirilmektedir:

- Kurumlarda kullanılan tüm bilgi sistemlerini kapsayacak, belirlenen aralıklarla tüm bilgi sistemlerinin güvenli şekilde güncellenmesini sağlayacak ve kurum ihtiyaçlarını karşılayacak bir yama yönetim süreci tanımlanmalıdır.

- Bilgi sistemlerinin iş sürekliliğinin devam ettirilmesi ve güvenliğinin sağlanması açısından işletim sistemleri, veri tabanı yazılımları, ağ ve güvenlik cihazları ve kullanıcı bilgisayarlarındaki masaüstü uygulamaları da belirlenen yazılı süreçler doğrultusunda düzenli olarak güncellenmelidir.

- Güncellemeler uygun ortamlarda test edildikten sonra çalışan sistemlere uygulanmalıdır.

TESPİT VE ÖNERİ 32- Kayıt tutma (log) mekanizmaları bilgi sistemlerinin izlenebilirliği ve durumsal farkındalık (*situational awareness*) tespiti için gerekli bir araçtır. Kurum bilgi sistemlerinde kimin, ne zaman, neleri sorguladığı ve bu sorgulama sonucunda dönen bilgilerin neler olduğuna ilişkin sorgu kayıtlarının tutulması, sisteme her türlü erişimin takibi, güvenlik ihlallerinin tespiti ve delillendirilmesi açısından önem taşımaktadır. Denetimlerde, kayıt yönetimi politikalarının oluşturulmadığı veya tüm sistemleri kapsamadığı, sıkı bir şekilde korunması ve sınırlı sayıda kişinin erişimine açık olması gereken kurum yazılımlarının kaynak kodlarına erişim kayıtlarının denetim kapsamındaki kurumların %70'ine yakınında tutulmadığı, bazı kurumlarda sorgu kaydı olmaksızın firma personelince sorgular yapılabildiği, sorgu kaydı tutan kurumlarda, bu kayıtların belirli zamanlarda incelenmesi veya analize tabi tutulması yönünde herhangi bir çalışmanın yapılmadığı, kayıtların daha çok kuruma ulaşan ihbarlar üzerine değerlendirildiği tespit edilmiştir.

Kayıt tutma mekanizmalarının bilgi güvenliği açısından arz ettiği önem dikkate alınarak aşağıdaki hususlarda gerekli adımlar atılmalıdır:

• Kurumsal bir kayıt yönetim politikası belirlenmelidir.

• Belirlenen bu politikada kritik sistemler tespit edilerek, bu sistemlerden ne şekilde, hangi kayıtların ne kadar süre ile alınacağı belirlenmelidir.

• Belirlenen politika, bilgi sistemlerine uygulanarak her bir sistem için kayıt tutma mekanizmaları devreye sokulmalıdır.

• Özellikle kurumsal uygulamalar, kurum dışıyla paylaşılan verilere ilişkin sorgu kayıtları, kurumsal uygulamalara ait kaynak kodu erişimleri ile sistemlere erişimlere ait kayıtlar tutulmalıdır.

• Tutulan kayıtların silinmeye ve değiştirilmeye karşı korunması yönünde zaman damgası, elektronik imza gibi mekanizmalar devreye alınmalıdır.

• Tutulan kayıtlar düzenli aralıklarla incelenmeli ve olası saldırılar ve yetkisiz erişimler tespit edilebilmelidir.

• Düzenli olarak güvenlik denetimleri yapılarak, kayıt tutma mekanizmalarının işlevselliği ve etkinliği kontrol edilmelidir.

TESPİT VE ÖNERİ 33- Kurumlara ait bilgi sistemlerinin çeşitlenmesi ve büyümesine paralel olarak; birbirinden farklı ve bağımsız kayıt tutma mekanizmaları uygulanmakta, bu kayıtlar kendine özgü formatlarda olabilmekte ve birbirleriyle ilişkilendirilememektedir. Ayrıca çeşitli nedenlerle bu kayıtlar silinebilmekte ve zarar görebilmektedir. Yukarıda sayılan sorunlara çözüm olarak, sistemlerdeki tüm kayıtları merkezi bir veri tabanında toplayan ve diğer sistemlerden fiziksel olarak ayrı tutan merkezi kayıt yönetimi ve güvenlik izleme sistemleri geliştirilmiştir. Bu sayede bir yandan kayıtların güvenliği sağlanmakta, diğer yandan farklı sistemlerdeki kayıtların karşılaştırılması, otomatik analiz ve incelemeye tabi tutulması mümkün hale gelmektedir. Denetimlerde iki kurum dışındaki kurumlarda merkezi kayıt yönetim ve izleme sisteminin bulunmadığı görülmüştür. Kayıt yönetim sistemi olan kurumlarda ise tüm sistemlerdeki kayıtların etkili bir şekilde toplanıp analiz edilmesinde eksiklikler olduğu görülmüştür.

Merkezi kayıt yönetim sistemlerinin bilgi sistemlerinin güvenliği açısından sağladığı imkânlar dikkate alınarak, özellikle kritik altyapı bilgi sistemleri ile kişisel veriler dâhil, önemli veri varlığına sahip kurumlarda aşağıdaki hususların göz önünde bulundurulmasının faydalı olacağı değerlendirilmektedir:

• Hangi kayıtların tutulacağını, tutulacak kayıtların nasıl ve ne kadar süre ile saklanacağını, farklı sistemlerden toplanan kayıtların nasıl ilişkilendirileceğini ve hangi yöntem ve tekniklerle analize tabi tutulacağını belirleyen süreç dokümanı oluşturulmalıdır.

• Belirlenen sürece uygun olarak tüm kritik bilgi sistemi bileşenlerinin (güvenlik bileşenleri, sunucu işletim sistemleri, veri tabanları, uygulamalar, ağ cihazları) güvenlik kayıtları merkezi olarak toplanıp kayıt altına alınmalıdır.

• Toplanan kayıtların değişmezliğini sağlayacak mekanizmalar sisteme dâhil edilmelidir.

• Toplanan kayıtlar üzerinde otomatik analizler ve sorgulamalar yapılmalı ve farklı sistemlerden elde edilen kayıtlar birbirleri ile ilişkilendirilerek, farklı türde saldırıları saldırı esnasında veya sonrasında tespit edebilecek takip ve analiz sistemi kurulmalıdır.

TESPİT VE ÖNERİ 34- Kişisel verilerin üçüncü kişilerin eline geçmemesi için, kullanım dışı kalan veya mülkiyeti devredilen üzerine kişisel veri kaydedilmiş donanımların güvenli şekilde imhası veya bu donanımlar üzerindeki verilerin güvenli şekilde silinmesi gerekmektedir. Denetim kapsamındaki kurumlardan sadece birinde kullanım dışı kalan elektronik kayıt ortamlarının güvenli imhası ile ilgili yazılı politikanın bulunduğu, ancak bu kurumda da imha işlemini yerine getirmesi gereken personelin politikadan habersiz olduğu ve politikayı uygulamadığı tespit edilmiştir. Bir kurumda, çalışanlara dizüstü bilgisayar dağıtıldığı, yazışma ve kurumun bilgi sistemlerine erişimin bu bilgisayarlar üzerinden yapıldığı, bu nedenle hassas kişisel veri niteliğine sahip pek çok verinin bu bilgisayarlar üzerindeki kayıt ortamında bulunduğu, söz konusu bilgisayarların mülkiyetinin beş yıllık kullanımın sonunda çalışanlara bilgisayarlardaki hassas verilerin güvenli şekilde silinmesi yönünde herhangi bir işlem yapılmadan devredildiği anlaşılmıştır.

Kullanım dışı kalan veya herhangi bir şekilde mülkiyeti başkasına devredilen bilgi sistemi unsurlarının imhası veya içlerindeki kişisel veriler dâhil kuruma ait veri varlıklarının geri döndürülemez şekilde silinmesine ilişkin olarak, aşağıdaki hususlarda gerekli önlemlerin alınması gerektiği değerlendirilmektedir:

• Kamu kurumlarında uygulanmak üzere, kullanım dışı kalan veya mülkiyeti devredilen her türlü kişisel veri ve yazılım/donanım sistemi için güvenli silme/imha etme standartları oluşturulmalıdır. Bu standartlarda sistemlerin işledikleri verinin gizlilik derecesine uygun olarak geri döndürülemeyecek şekilde yok edilmesine ilişkin mekanizmalar tarif edilmelidir. Bu mekanizmalar güvenli silme ve fiziksel imha gibi yöntemleri içermelidir.

• Kurumlar tarafından kullanım dışı kalan her türlü kayıt ortamının imhasına ilişkin olarak süreç dokümanı hazırlanmalıdır.

• Hazırlanan süreç dokümanları; kullanım dışı kalan yedekleme teyp kartuşları, CD/DVD, sunucu ve masaüstü sabit diskleri, diz üstü ve tablet bilgisayarları, USB diskler ve diğer taşınabilir ortamların tamamıyla ilgili yapılacak işlemleri içermelidir.

• Kişisel veri içeren elektronik kayıt ortamları güvenli bir şekilde saklanmalı, kullanım dışı kalan kayıt ortamları bu ortamlardaki veriye ulaşılamayacak şekilde imha edilmelidir.

• Her bir kayıt ortamının imhasına ilişkin süreç belirlenmelidir.

• Kayıt ortamlarının imhasına yönelik kurum dışından hizmet alınması durumunda, hizmet sağlayıcının uygunluğuna ve yeterliliğine ilişkin kriterler öngörülmelidir.

• İmha işlemi, imha edilen kayıt ortamının niteliğini belirtecek şekilde tutanak ile kayıt altına alınmalıdır.

• Herhangi bir şekilde kâğıt ortamına aktarılan kişisel verilerin korunması amacıyla bunların güvenli olarak saklanması ve imhası konusunda süreçler belirlenmelidir.

TESPİT VE ÖNERİ 35- Bilgi güvenliğinin bir boyutu, bilgi sistemlerinin fiziki güvenliğinin sağlanmasıdır. Bilgi sistemlerine fiziki erişim; bu sistemlerdeki verilere erişim, bunları silme, değiştirme veya bu sistemlere fiziki olarak zarar verme riskini artırmaktadır. Çeşitli kuruluşların yaptıkları güvenlik denetimlerinde fiziksel olarak güvenliği sağlanmamış sistemlere saldırı denemeleri yapıldığında, bu sistemlerin beş dakika gibi kısa bir sürede ele geçirilebildiği ve içindeki verilere ulaşılabildiği görülmüştür.

Denetimlerde;

• Bazı kamu kurumlarının sistem odaları ile çalışan ofislerinin oldukça iyi korunduğu, sistem odasına girişlerin parmak izi, şifre ve yüz tanıma sistemleri ile yapıldığı,

• Bazı kurumlarda çalışanların ofislerine de yetkilendirilmiş manyetik kartlar ile giriş yapılması ve giriş çıkışların video kamera sistemi ile kayıt altına alınması gibi iyi uygulama örnekleri yanında sistem odasına giriş çıkış yapanların bir kayıt defterine manuel olarak isimlerini yazması gibi etkin kontrole imkân vermeyen iptidai uygulamaların da bulunduğu,

• Bazı kurumların sistem odalarının fiziksel güvenliğinin zayıf olduğu, giriş kapılarının ahşap gibi zayıf bir malzemeden yapıldığı ve kısa sürede kırılabilecek asma kilit ile korunduğu,

• Bir kurumda, sistem odasından doğrudan açık otoparka açılan bir kapı ile çıkış yapılabildiği,

• Bir kamu kurumuna ait sistem odasının yaya ve araç trafiğinin yoğun olduğu ve çok sayıda kitlesel eylemin yapıldığı yerlere çok yakın olduğu ve donanım yüklemesi için kullanılan kapının hemen yanında kişi trafiği yoğunluğu olan PTT şubesinin bulunduğu,

• Aynı kamu kurumunun tüm internet erişimini sağlayan kabloların bina dışından açık bir şekilde taşındığı ve fiziksel müdahaleye açık olduğu,

• Başka bir kamu kurumunun, kendine ait bilgi işlem merkezinin bulunmadığı ve tüm sistemlerinin ticari bir firmadan kiralanan bir bilgi işlem merkezinde çalıştığı, bu merkezde başka kurum ve firmalara ait sistemlerin bulunduğu ve başka firma elemanlarının kurum sunucularına fiziksel olarak erişebildiği

görülmüştür.

Bilgi sistemlerinin fiziksel güvenliğinin sağlanmasına yönelik olarak aşağıdaki hususlara riayet edilmesi gerektiği değerlendirilmektedir:

• Kurum binalarının fiziksel olarak korunması, farklı koruma mekanizmaları ile donatılması temin edilmelidir.

• Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binalarda ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilmelidir.

• Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili güvenlik görevlileri gözetiminde gerçekleştirilmelidir.

• Kritik bilgilerin bulunduğu alanlara girişlerin kontrolü akıllı kartlar veya biyometrik sistemler ile yapılmalı ve izlenmelidir.

• Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin güncelliği sağlanmalıdır.

• Personel kimliği ve yetkilerini belirten kartların ve ziyaretçi kartlarının düzenli olarak taşınması sağlanmalıdır.

• Kritik sistemler özel sistem odalarında tutulmalıdır.

• Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzeri felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.

• Fotokopi, yazıcı ve benzeri cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.

• Çalışma alanlarının kullanılmadığı zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

G- İÇ KONTROL VE İÇ DENETİM SİSTEMİ İLE DİĞER DENETİMLERE İLİŞKİN TESPİT VE ÖNERİLER

TESPİT VE ÖNERİ 36- İç kontrol sistemlerinin bilgi sistemlerinin güvenliğini sağlama açısından oldukça yetersiz olduğu ve etkin bir şekilde çalışmadığı, denetimlerde tespit edilen pek çok güvenlik açığı ve eksiklikle teyit edilmiştir.

Bilgi güvenliği ve kişisel verilerin etkin bir şekilde korunması açısından kurumların;

• Bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontrolleri yazılı olarak belirlemeleri ve uygulamaları,

• Bilgi sistemine veri ve bilgi girişi ile bunlara erişim konusunda yetkilendirmeler yapılmasını, hata ve usulsüzlüklerin önlemesini, tespit edilmesini ve düzeltilmesini sağlayacak mekanizmalar oluşturmaları,

• Bilişim yönetişimini sağlayacak mekanizmaları geliştirmeleri ve

• Bilgi sistemlerine yönelik tehditlerin sürekli değişen ve gelişen özelliği dikkate alınmak suretiyle iç kontrol sistemlerini bu değişime hızlı adapte olacak bir yapıda kurgulamaları

gerekmektedir.

TESPİT VE ÖNERİ 37- Kurumların bir kısmında bilgi sistemlerinin güvenliği konusunda herhangi bir iç denetim çalışması yapılmamıştır. Bazı kurumlarda gerçekleştirilen bilgi güvenliği alanındaki iç denetimlerin sınırlı sayıda ve dar kapsamda olduğu ve düzenlilik arz etmediği tespit edilmiştir. Bunda; kamu kurumlarının bazılarında iç denetim biriminin oluşturulmaması, bilgi teknolojileri denetimine yönelik ayrıntılı hukuki düzenleme ve kamu iç denetçilerinin bilgi teknolojileri denetimlerinde kullanabilecekleri bir rehber, yönerge ve benzeri bir çalışmanın bulunmaması, bilgi sistemlerinin denetimini yapacak yetkinlikteki iç denetçi sayısının yetersizliği, bu konudaki ihtiyaca ilişkin üst yönetimin farkındalığının yeterli düzeyde olmaması gibi etkenlerin önem taşıdığı değerlendirilmektedir.

Bu çerçevede; kullanılan bilgi sistemlerinin kurumun faaliyetlerini ne ölçüde destekleyebildiğinin ve ayrıca bilgi sistemlerinin kullanımı ile ilgili risklerin iç kontrollerle ne derece kontrol altına alınabildiğinin anlaşılması açısından bilgi sistemlerine ilişkin iç kontrol ortamının denetlenmesi gereği bulunmaktadır. Ayrıca;

• Bilgi teknolojileri denetimine yönelik hukuki düzenleme yapılması ve kamu iç denetçilerinin bilgi teknolojileri denetimlerinde kullanabilecekleri rehber çalışmasının bir an önce tamamlanması,

• Kamu idarelerinde, bilgi teknolojileri denetimi alanında yetkinliğe sahip iç denetçi sayısının artırılmasına yönelik olarak,

- Eğitim,

- Bilgi sistemleri denetim sertifikasyonu uygulaması,

- Bilgi sistemi denetimi yapması öngörülen denetçilere ilişkin ayrı bir denetçi aday belirleme sınavı yapılması, bu kapsamda mevcut denetçi eğitim geçmişlerinden farklı alanlardan denetçi alımı sağlanması ve ilerleyen aşamada kurumların bilgi sistemlerinin büyüklüğü, önem derecesi gibi hususlar dikkate alınarak iç denetçi kadrolarının belli bir oranının bilgi sistemi denetim yeterliliğine sahip denetçilere tahsis edilmesi,

- Bilgi sistemleri denetiminde idare içinden ve dışından uzman istihdam etme imkânlarının kullanılması,

- Bilgi sistemleri denetiminde yetkin hale gelen denetçilerin diğer kurumlarda da değerlendirilebilmesi

yönünde adım atılması veya atılmakta olan adımların desteklenmesi ve hızlandırılması gerektiği değerlendirilmektedir.

TESPİT VE ÖNERİ 38- Özel sektör kurum ve kuruluşları üzerinde düzenleme ve denetim yetkisi bulunan kurumların, ilgili sektörlerde gerçekleştirecekleri denetimlerin kapsamını, Bankacılık Düzenleme ve Denetleme Kurumu ile Bilgi Teknolojileri ve İletişim Kurumu örneklerinde olduğu gibi, bilgi sistemlerinin güvenliği ve kişisel verilerin korunması alanını da kapsayacak şekilde belirlemelerinin, özel kesimde kişisel veri ihlallerinin önlenmesi açısından önemli bir boşluğu dolduracağı değerlendirilmektedir.

TESPİT VE ÖNERİ 39- Kurumlarda yapılan güvenlik testlerinin kalitesinde ciddi farklılıklar bulunduğu, hiçbir kurumun testleri düzenli aralıklarla yaptırmadığı, yapılan bazı test sonuçlarında bilgi sistemleri açısından çok ciddi güvenlik riski oluşturacak kritik güvenlik açıkları tespit edilmesine rağmen kurumların hiçbirinde testlerde tespit edilen açıklıkların kapatılmasına yönelik "Teknik Açıklık Yönetimi" süreçlerinin olmadığı, tespit edilen açıkların kapatılması konusunda önemli gecikmelerin bulunduğu, bazı kurumlarda açıkların gerçek anlamda kapatılmadığı halde üst yönetime veya denetim yapanlara "kapatıldı" olarak raporlandığı tespit edilmiştir.

Kurum bilgi sistemleri ve kişisel veriler dâhil bilgi varlıklarının karşı karşıya bulunduğu risk ve tehditlerin tespiti ve gerekli önlemlerin alınması açısından önem taşıyan güvenlik testleri konusunda aşağıdaki hususların göz önünde bulundurulması gerektiği değerlendirilmektedir:

• Belirli bir standarda bağlı olmadan, genel olarak kurumun tercihleri veya testi yapan birim ya da firmanın önerileri doğrultusunda gerçekleştirilen güvenlik testleri güvenilir olmamaktadır. Bu nedenle, kamu kurumlarında belirli aralıklarla güvenlik testleri yapılmasını da

sağlayacak şekilde ulusal düzeyde "Kamu Kurumları Güvenlik Testleri Standardı" dokümanı oluşturulmalı ve uygulanması sağlanmalıdır.

• Özellikle hassas kişisel veriler ile kritik altyapılara ilişkin verilere sahip kamu kurumlarına ait bilgi sistemleri belli periyotlarla düzenli şekilde sızma testleri dâhil güvenlik denetimlerine tabi tutulmalıdır.

• Güvenlik denetimlerinin yapılması kadar, standart olması, denetimi yapacak kurum veya kuruluşun kalitesi ve gizliliğe riayeti önem taşımaktadır. Bu hususlar göz önünde bulundurulmadan herhangi bir kuruluşa yaptırılacak güvenlik testlerinin kendisi önemli bir güvenlik riski oluşturabilecektir. Bu nedenle, güvenlik testi yapma konusunda yetkili ve yeterli teknik eleman ve donanıma sahip kamu kurumlarının geliştirilmesi, özellikle kritik altyapı ve hassas kişisel veri barındıran kamu bilgi sistemlerinin denetiminin yine kamu kaynaklı bu kurumlarca gerçekleştirilmesi; diğer kamu kurum ve kuruluşları ile başta finans, sağlık ve telekomünikasyon gibi alanlarda özel kesimde bilgi sistemleri güvenlik denetimi yapacak kuruluşların sertifikasyona tabi tutulması ve denetim standartları ile raporlama usul ve esaslarının belirlenmesi gerekmektedir.

• Gerçekleştirilen güvenlik denetim ve sızma testi sonuçlarının üst yönetimle doğru ve açık bir şekilde paylaşılması sağlanmalıdır.

• Testler sonucunda tespit edilen ancak kapatılmayan açıklıkların, hiç tespit edilmemiş açıklıklara göre kurum açısından daha fazla güvenlik riski oluşturacağı hususu göz önünde bulundurularak, açıklıkların kapatılması için mutlaka "Teknik Açıklık Yönetimi" süreci belirlenmeli ve bu süreç çerçevesinde açıklıklar mümkün olan en kısa süre zarfında kapatılmalıdır. Özellikle kurum dışından erişilebilen uygulamalarda bulunan açıklıklar öncelikli olarak kapatılmalıdır.

Gerçekleştirilen denetim, inceleme ve araştırma çalışmaları kapsamında ulaşılan sonuçlara yukarıda maddeler halinde yer verilmekle birlikte;

• Bilgi güvenliği ve kişisel verilerin korunması konusundaki farkındalık eksikliği,

• Hizmetlerin kaliteli ve hızlı sunulmasına odaklanılırken, uzun vadede hizmetlerin hiç sunulamaması sonucunu da doğurabilecek olan bilgi sistemlerinin güvenliği konularına yeterince önem verilmemesi,

• Mevzuat alanındaki boşluk ve kurumsal yapılanma eksikliği,

• Kişisel verilerin korunmasının kamu bilgi sistemleri ile sınırlı olmaması, özel kesimde kişisel verilerin karşı karşıya bulunduğu risklerin gittikçe artması ve buna

karşılık özel kesimde kişisel verilerin korunmasına ilişkin mevzuat ve denetim boşluğunun bulunması,

• Kurumlarda bilgi sistemleri güvenliği ile kişisel verilerin korunması konusunda büyük önem taşıyan iç kontrol ve iç denetim müesseselerinin işlememesi

hususlarının, bilgi güvenliği ve kişisel verilerin korunması alanındaki sorunlara kaynaklık teşkil ettiği değerlendirilmektedir.

Bu nedenle, yapılan inceleme ve araştırma çalışmaları ile yürütülen denetim faaliyetleri sonucunda ulaşılan ve yukarıda yer verilen tespitlerin, tüm kurum ve kuruluşların kişisel verilerin korunması ve bilgi güvenliği uygulamalarında görülmesinin muhtemel olduğu göz önünde bulundurulduğunda, kişisel verilerin korunması ve bu çerçevede bilgi güvenliğine ilişkin eksikliklerin ve yanlış uygulamaların ortadan kaldırılması veya asgari düzeye indirilebilmesi açısından;

• Kişisel verilerin toplanması, işlenmesi, kullanılması, paylaşılması, silinmesi gibi her aşamada korunmasına yönelik olarak farkındalığın artırılması ve bilinç düzeyinin yükseltilmesi,

• Kişisel verilerin korunmasına ilişkin olarak kişisel veri, açık rıza ve benzeri tanımların, kişisel verilerin işlenmesinin genel ilke ve esaslarının, kişilerin haklarını korumalarına yardımcı olacak mekanizmaların ve ilgili kurum ve kuruluşların kişisel verilerin işlenmesi sırasında bu hakkın korunmasına uygun davranışta bulunmalarını sağlamak amacıyla gerekli ikincil düzenlemeleri ve denetimleri yapacak, şikâyetleri değerlendirecek, idari yaptırım uygulama yetkisine sahip kurumsal yapılanmanın ne şekilde olacağını belirleyen çerçeve bir kanunun bir an önce hukuk sistemimize kazandırılması; sektörel bazda bilgi güvenliği ve kişisel verilerin korunmasına yönelik özel düzenleme çalışmalarının yürütülmesi,

• Kişisel verilerin korunması için bağımsız, tarafsız ve teknik açıdan yetkin bir kurumsal yapının önemi dikkate alınarak, bu alandaki kurumsal yapı eksikliğinin uluslararası standartlara uygun şekilde giderilmesi; bilgi güvenliği konusunda kurumlar arasındaki görev çakışmaları ile işbirliği ve koordinasyon eksikliklerinin ortadan kaldırılması,

• Kişisel verilerin korunması hakkına ilişkin önemli bir tehdit alanını ticari işletmeler ve sivil toplum kuruluşları gibi özel kesimin elindeki kişisel verilerin işlenmesi, kullanılması, paylaşılması ve güvenliği konularının teşkil ettiği dikkate alınarak, bu alana yönelik düzenlemelerin yapılması ve denetimlerin gerçekleştirilmesi,

• Bilgi sistemlerinin güvenliği ve kişisel verilerin korunması açısından önem taşıyan etkin bir bilgi güvenliği yönetim sisteminin oluşturulması ve sürekliliğinin sağlanması için kurumların öz savunma mekanizması niteliğinde olan iç kontrol ve iç denetim müesseselerinin etkin şekilde işletilmesi

hususlarının bu alandaki sorunların çözümü konusunda yapılacak çalışmalarda esas alınması gerektiği değerlendirilmektedir.

Bu kapsamda;

A- Kurumlar nezdinde gerçekleştirilen denetim çalışmalarına ilişkin olarak;

• Raporun Yedinci Bölümünde yer alan tespit ve önerilerin gereğinin Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü,

• Raporun Sekizinci Bölümünde yer alan tespit ve önerilerin gereğinin Tapu ve Kadastro Genel Müdürlüğü,

• Raporun Dokuzuncu Bölümünde yer alan tespit ve önerilerin gereğinin Gelir İdaresi Başkanlığı,

• Raporun Onuncu Bölümünde yer alan tespit ve önerilerin gereğinin Sosyal Güvenlik Kurumu,

• Raporun On Birinci Bölümünde yer alan tespit ve önerilerin gereğinin Sağlık Bakanlığı,

• Raporun On İkinci Bölümünde yer alan tespit ve önerilerin gereğinin Adalet Bakanlığı,

B- Raporun Genel Değerlendirme ve Öneriler başlıklı On Üçüncü Bölümü ile Sonuç Kısmında yer alan;

• 1 numaralı tespit ve önerinin gereğinin, Ulaştırma, Denizcilik ve Haberleşme Bakanlığının koordinatörlüğünde, Kalkınma Bakanlığı, Milli Eğitim Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu ve TÜBİTAK,

• 3, 4 ve 6 numaralı tespit ve önerilerin gereğinin Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Kalkınma Bakanlığı,

• 8, 10, 11, 12, 13 ve 14 numaralı tespit ve önerilerin gereğinin Adalet Bakanlığı,

• 36 ve 37 numaralı tespit ve önerilerin gereğinin Maliye Bakanlığı,

• Yukarıda belirtilenler dışındaki tespit ve önerilerin gereğinin ilgili kurum ve kuruluşlarla işbirliği içerisinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

tarafından yapılmasının temini maksadıyla, işbu Raporun 2443 sayılı Devlet Denetleme Kurulu Kurulması Hakkında Kanun'un 6. maddesi uyarınca Başbakanlığa gönderilmesi,

Raporun gereğinin yapılması için Başbakanlık tarafından ilgili kurum ve kuruluşlara dağıtımında Raporun;

• Yedinci Bölümünün sadece Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü,

• Sekizinci Bölümünün sadece Tapu ve Kadastro Genel Müdürlüğü,

• Dokuzuncu Bölümünün sadece Gelir İdaresi Başkanlığı,

• Onuncu Bölümünün sadece Sosyal Güvenlik Kurumu,

• On Birinci Bölümünün sadece Sağlık Bakanlığı,

• On İkinci Bölümünün sadece Adalet Bakanlığı

ile paylaşılması, elektronik ortamdaki paylaşımlarda dosyanın şifrelenmesi ve benzeri güvenlik tedbirlerinin alınması,

Kurum denetimlerine ilişkin 7, 8, 9, 10, 11 ve 12. Bölümlerde yer alan hususların, bilgi güvenliği açısından gizliliği dikkate alınarak, Raporun ilgili diğer kurumlara dağıtımında, 4982 sayılı Bilgi Edinme Hakkı Kanunu ve diğer mevzuat kapsamında herhangi bir şekilde paylaşımında söz konusu bölümlerin Rapordan çıkartılması

gerektiği sonuç ve kanaatine varılmıştır.

Saygılarımızla arz ederiz. 27/11/2013

(İmza)	(İmza)	(İmza)
Cemal BOYALI Başkan	Faik CECELİ Üye	Mehmet İLHAN Üye
(İmza)	(İmza)	(İmza)
Mehmet Ali ÖZKILINÇ Üye	Metin ARSLANBAŞ Üye	Dr. Hasan AYKIN Üye
(İmza)	(İmza)	
Abdülkadir DERE Üye	Abdurrahman ÖZÇELİK Üye	