Sektör İncelemeleri - 3

Kişisel Verilerin Korunması

Noterlik

Prof. Dr. Turhan MENTEŞ
Prof. Dr. Mustafa ALKAN
Mehmet Ali İNCEEFE

www.accert.com.tr

Bu Sektör İnceleme Raporu ACCERT A.Ş. Tarafından Hazırlanmıştır.

Ankara Mayıs.2020

ISBN-978-605-06236-1-1

İçindekiler

Önsöz

Çeşitli sektörlerin kendisine has yasal ve pratik durumunu kişisel veriler ve mahremiyetin korunması açılarından ele alıp ilgili sektöre bir rehberlik sunabilmek amaç ve hedefi ile hazırlayıp yayınlamaya başladığımız **ACCERT Sektörel İnceleme Raporları**nın ilk ikisi, Denizcilik ve Sağlık Sektörleri üzerine hazırlandı. Kişisel verilerin işlenmesi ve korunmasına yönelik çok yönlü bir inceleme nitelindeki 3. Raporumuz ise Noterlik mesleği üzerine.

Noterlik mesleği, niteliği itibarı ile bir kamu hizmeti sayılmaktadır. Türkiye'deki en yerleşik kurumlardan biri olan noterliklerin, iş hacim ve yöntemleri, hızla değişen teknoloji ile birlikte çeşitlenmekte ve yeniden şekillenmektedir. Bunun en somut örneği Noterlik Kanunu'nda 2/12/2014 tarihinde yapılan bir değişiklikle (*özellikle 198/A Madde*) noterlik işlemleri artık elektronik ortamda da yapılmaya ve bu işlemlerin bir kopyası merkezi olarak Türkiye Noterler Birliği'nin (*TNB*) oluşturduğu bir altyapıda saklanmaya başlanmış olmasıdır.

Tüm ülke çapına yayılmış 2.000'e yakın noterin yaptığı bu işlemlerin merkezi bir sistemde saklanıyor ve gerektiğinde diğer noterler veya noterlik çalışanları tarafından erişilebiliyor olması, bir taraftan bu işlemlerin etkin ve hızlı bir biçimde yürütülmesine olanak sağlarken, diğer taraftan da bu bilgileri çok ciddi risklere açık hale getirmektedir.

Salgın ortamında üretim ve çalışma teknik ve yöntemleri düne kadar bir tartışma konusu iken bugün tüm dünyanın yaşadığı bir olguya dönüştü. Genellikle fiziksel olarak varlığı gerektiren noterlik işlemleri de, bugün mevcut olan e-imza, KEP, uzaktan görüşme ve görüntüleme teknolojileri ile gelecekteki ihtiyaçlara göre geliştirilecek yeni teknolojilerin yardımıyla da yeni ve çevrimiçi yöntemleri kullanıyor hale gelecektir. Bu işlemlerin içerdiği kişisel verilerin paylaşılıyor olması, söz konusu verilerin saçılma olasılığını da artırmaktadır.

Noterler çeşitli belgeleri onaylayıp geçerlilik kazandırmaktan vasiyetname ve ölüme bağlı tasarruflarla ilgili işleri yapmaya kadar her türlü ve en mahrem kişisel verileri ve bilgileri içeren karmaşıklıktaki iş ve işlemleri gerçekleştirmektedirler. Bu da fotoğraf, ıslak imza ve parmak izi gibi **biyometrik verileri**, yani "***özel nitelikli kişisel veri***" işleyen noterleri kişisel verilerin korunması açısından çok daha hassas ve kırılgan bir noktaya taşımaktadır. Üstelik "*Vasiyetnamelerin tescil konusunda bir usul kurulmasına dair* ***Avrupa Sözleşmesi***[1] *uyarınca tescil gereken vasiyetnamelere ilişkin bilgiler sözleşmede yazılı olduğu şekilde bu defterlere işlenir"* olması da gerek bu işlemi yapan noterleri gerekse de bu işlemlere yönelik defterleri tutan TNB'yi doğrudan Avrupa Genel Veri Tüzüğü (*GDPR*) yükümlüsü kılmaktadır.

Diğer taraftan, bütün dünyayı istediği gibi yöneteceğini, her istediğini yapabileceğini ve her şeyi düzenleyip, denetleyip, kontrol altına alacağını sanan insanoğlu, aslında bu kadar güçlü olmadığını, aksine evrenin kanunları karşısında ne kadar çaresiz ve zayıf olduğunu da çok acı bir deneyimle görmeye başlamıştır.

Ancak insanlık tarihinin çok önemli olaylarından birisi olan bu "Korona Salgını" bir gerçeği daha net bir şekilde ortaya koydu. Bu gerçek, yakın gelecekte yani korona sonrası dünyada, insanoğlunun hayatının hemen hemen her şeyiyle sayısallaştığı, bir siber hayat ve siber dünya olacağı gerçeğidir.

Yarının "Siber Dünyasında" veri ve bilgi kavramları bugünden daha fazla anlam ve kıymet ifade edecek, bilginin ve verinin korunması ise daha önemli hale gelecektir. Kişisel verilerin korunması ve kişisel mahremiyet özelinde ise konu her zamankinden daha başka bir anlam kazanacaktır. Çünkü yeryüzünde yaşayan insanoğlunun tüm kişisel bilgileri, siber dünya içinde dolaşmaya başlayacak ve yeni bir e-insan tipi ortaya çıkacaktır.

Korona sonrası kimler hayatta kalır bilinmez ama bütün insanlığın en az kayıp ve zararla bu süreci atlatacağı umudu ve dileğiyle bu çalışmanın bundan sonraki süreçte insan için önemli bir kaynak olacağı inancını taşıyoruz.

İnsanoğlunun varlığını sürdürmesinde, sağlıklı yaşamasında, mutlu olmasında en büyük paya sahip, başta Türk Hekimleri ve sağlık çalışanları olmak üzere, tüm dünya sağlık insanlarına bu vesileyle yine ve yeniden şükranlarımızı sunuyoruz.

Noterler için hazırlamış olduğumuz bu rapor ile bugüne dek çok kritik üç sektör için İnceleme Raporu yayınlamış olduk. Bugüne kadar hedeflediğimiz katkıyı başarı ile sağlamış olduğumuzu görmekten dolayı mutluyuz. Bundan sonraki süreçte de yine farklı sektörler için hazırlamayı planladığımız Kişisel Verilerin Korunması kapsamındaki sektör inceleme raporlarını da kamuoyuyla paylaşıyor olacağız.

Raporun hazırlanması sürecinde bizlere destek olan ve bu çalışmaya katkı veren tüm kişi ve kuruluşlarımıza teşekkür ediyoruz.

Prof. Dr. Mustafa Alkan / Prof. Dr. Turhan Menteş / Mehmet Ali İnceefe
Mayıs.2020 Ankara

[1] 17.4.1975 tarih ve 1885 sayılı "Vasiyetnamelerin Tescili Konusunda Bir Usul Kurulmasına Dair Avrupa Sözleşmesinin Onaylanmasının Uygun Bulunduğuna İlişkin Kanun"

Tanım ve Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
Alt Veri İşleyen	Veri işleyen tarafından kendisine verilen yetkiye dayanarak ve yine Veri İşleyen'in talimatları doğrultusunda veri işleme faaliyetleri gerçekleştiren
ARES	Araç Sicil Ve Tescil Sistemi
AT	Avrupa Topluluğu
BT	Bilişim Teknolojileri
Direktif	Veri Koruma Direktifi (*95/46/EC Data Protection Directive*)
CCTV	Kapalı Devre Kamera Sistemi (*Closed Circuit Camera System*)
Çalışan	TNB veya Noterlikler bünyesinde istihdam edilen gerçek kişi
DTÖ	Dünya Sağlık Örgütü (World Health Organization)
GDPR	Avrupa Genel Veri Koruma Tüzüğü (*General Data Protection Regulation)*
GSYİH	Gayrisafi Yurt İçi Hâsıla
İK	4857 Sayılı iş Kanunu
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
KEP	Kayıtlı Elektronik Posta
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
NBS	Noterlik Bilgi Sistemi
OECD	Ekonomik işbirliği ve Kalkınma Teşkilatı (*Organization for Economic Cooperation and Development)*
SGK	Sosyal Güvenlik Kurumu
SİMAS	TNB bünyesinde kurulan Sicil ve Tescil İşlemleri Müdürlüğünün kullandığı Sicil Modülü
TARES	Taşınır Rehin Sicili
TBK	6098 sayılı Türk Borçlar Kanunu
TBMM	Türkiye Büyük Millet Meclisi
TCAB	T.C. Adalet Bakanlığı
TCK	5237 sayılı Türk Ceza Kanunu
TMK	4721 sayılı Türk Medeni Kanunu
TNB	Türkiye Noterler Birliği
TNBBS	TNB Bilgi Sistemleri
TÜİK	Türkiye İstatistik Kurumu
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi

1. Noterlik ve Kişisel Veriler

Kişisel verilerin hem kamusal hem de ticari açıdan çok kritik önem taşıdığı günümüzde Noterlik mesleği, 1512 sayılı Noterlik Kanunu'nda "*bir kamu hizmeti*" olarak tanımlanmıştır.

Noterlerin görevleri, gayrimenkul satış va'di sözleşmesi yapmaktan, kâğıtların üzerindeki imza, mühür veya herhangi bir işareti veya tarihi onaylamaya, belgeleri bir dilden diğer dile veya bir yazıdan başka bir yazıya çevirmekten protesto, ihbarname ve ihtarname göndermeye, tespit işlerinden emanet işlerine, defter onaylamaktan vasiyetname ve ölüme bağlı tasarruflarla ilgili işleri yapmaya kadar **her türlü ve en mahrem kişisel verileri ve bilgileri** içeren karmaşıklıktaki iş ve işlemlerden oluşmaktadır.

Tanık, tercüman ve bilirkişinin andı yine noterler tarafından yaptırılmaktadır.

Diğer taraftan Noterlik Kanunu kapsamında noterlerin üst kuruluşu olarak kurulan Türkiye Noterler Birliği (*TNB*) de, yurt çapında hizmet veren 1.862 noterlikler ile birlikte ülkede kişisel veriler açısından en kapsamlı ve en karmaşık iş yükü ve iş süreçlerine sahip bir kurum niteliğindedir.

Noterlik Kanunu *"Noter ve noterlik kâtipleri, görevleri dolayısiyle öğrendikleri sırları, kanunların emrettiği haller dışında açıklıyamayacaklarına"* hükmetmektedir. Noterlik Kanununca konulan tüm bu sıkı gizlilik sorumluluklarına ek olarak 7.Nisan.2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) da ek olarak bir dizi yeni yükümlülükler getirmiştir.

KVKK, özellikle 3 açıdan Noterler ve TNB için çok kritik bir yasadır;

- ✔ Noterlik mesleğinin ana iş konusu (*ve neredeyse tüm işleri*) kişisel veriler ile ilgilidir.
- ✔ Noterlikler ve TNB'nin, yapılan işlerin doğası gereği, kendi aralarındaki bilgi aktarımının yanı sıra tercüman, tanık ve bilirkişi gibi diğer birçok kişi ve kurumla da bilgi ve veri aktarımı yapılmaktadır.
- ✔ Noterlik Yasasında yapılan değişiklikle;
    i. "*Noterler tarafından yapılan tüm işlemlere dair bilgi ve belgeler Türkiye Noterler Birliğinin Bilişim Sisteminde kaydedilmesi ve saklanması*" ve
    ii. "*Noterlik işlemlerinin elektronik ortamda yapılması sırasında işlenen kişisel verilerin korunması ve bilgi güvenliğinin sağlanması için gerekli tedbirler alınması*" yükümlülüğünü getirilmiştir.

Diğer taraftan, TNB bünyesinde "*hasta Noterlere veya Noterlerin eş ve bakmakla yükümlü oldukları çocuklarının hastalıkları halinde yardımda bulunulmasını sağlamak amacı ile ihtiyatlar hesabı kullanılması*", bu hesabın kullanımında "*belirli süreler içinde tekrarı zorunlu ve masraflı tedavi (**şua, dializ ve benzeri**) ile yurtiçi ve yurtdışında büyük masrafı icap ettiren **ameliyatları gerektiren hastalıklar** halinde, kendi imkânları ile bu tedaviyi sağlayacak durumda olmayan noterlere*" bu yardımdan yararlanmak için, ilgili dilekçeye kendisi veya eşi ve "*bakmakla mükellef olduğu hasta çocuklarına ilişkin **rapor ile nüfus kayıt örneği, yapılmış ise ameliyat ve tedaviler nedeniyle yapılan ödemelere ilişkin makbuz, fiş veya fatura asıllarının** eklenmesi zorunluluğu*" getirmektedir.[2]

TNB, üye ve yakınlarına sağladığı bu yardım için ilgili kişilerin "***özel nitelikli kişisel verileri***"ni toplamaktadır.

Bu nedenlerle, KVKK'nın ilgili tanımlarına göre Noterlikler ve TNB çoğu durumlarda doğrudan veri sorumlusu, bazı durumlarda da veri işleyen niteliğini haiz olmaktadır.

Noterlikler ve TNB, gerek doğrudan veri sorumlusu, gerekse de veri işleyen niteliği ile hem kendilerinin eylemlerinden doğrudan hem de diğer tarafın işleyeceği eylemlerden dolayı veri işleyen olarak müştereken sorumlu olacaklardır.

[2] TNB, İhtiyatlar Hesabının Kullanım Esasları (Talimatname)

KVKK tarafından TNB'nin de dâhil olduğu kamu kurumu niteliğinde Meslek Kuruluşlarına tanınmış olan bir takım muafiyetler söz konusudur. Ancak bu muafiyetler sınırlıdır. Örneğin, bazı kuruluşlar Verbis'e kayıt yükümlülüğünden muaf iken, bazıları ise bir takım yaptırımlarından muaf tutulmuştur.

Ancak, KVVK'nın diğer tüm yükümlülükleri ve cezai sorumluluklar başta olmak üzere tüm sorumluluklarına tabi durumdadırlar.

Bu kapsamda, Noterlerin ve TNB'nin**;**

- Bazı işlemleri Kanunun açık hükümleri uyarınca işlenmekte,
- Bazı işlemleri için İlgilinin **Aydınlatılması**,
- Bazı işlemler için ise **Açık Rıza** gerektirmektedir.

Bu durum, KVKK uyarınca TNB tarafından, yapılan işlemler ile ilgili çok kapsamlı ve detaylı bir "**envanter**" çıkarılmasını ve **risk/etki analizlerini** gerektirmektedir.

Kabahatlerin TNB'nin bünyesinde işlenmesi halinde, TNB'nin kendisine bir **idari para cezası kesilemeyecek**, ancak sorumlu kişilere **uyarma–meslekten men** arasında **disiplin cezaları** kesilerek ve neticesinin KVKK'ya bildirilmesi gerekmektedir**.**

Diğer yandan 2018/32 sayılı KVK Kurul Kararı ile 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler için de **Sicile kayıt yükümlülüğüne istisna** getirilmiştir. Bununla birlikte, Sicile kayıt yükümlülüğünden istisna olma durumu **KVKK hükümlerinden de istisna olmak anlamına gelmemektedir**.[3] KVKK 18. maddesinde yer alan kabahatleri işleyen Noterlere **idari para cezaları uygulanması riski** bulunmaktadır.

Benzer biçimde bazı sorumlulukların yerine getirilememesi veya yükümlülüklerin ihlal edilmesi **TCK 135-140** ile düzenlenmiş suçlar bakımından **hapis cezaları gerektirmektedir**. Bu olası risklerin bir adım ötesinde, kişisel verileri TNB veya Noterler tarafından ihlal edilenler, bundan kaynaklanan **maddi ve manevi zararlarının tazmin edilmesini** talep edebileceklerdir.

Noterler ve TNB tarafından **yurtdışına veri aktarımları** KVKK'daki koşullara ve yerine göre KVK Kurulu'nun iznine tabiidir. Bu nedenle yurtdışına veri aktarımı gerektiren tüm işlem süreçleri de KVKK'na uyum bakımından gözden geçirilmelidir.

Bu örneklerden görüleceği üzere, KVKK uyumluluğu Noterler ve TNB için hayati önemi haizdir. Aksi takdirde, telafisi mümkün olmayan maddi ve manevi sonuçlar doğuracaktır. Bu sonuçlar, idari para cezaları ve hapis cezaları başta olmak üzere güven ve itibar kayıplarına sebep olacaktır.

Diğer taraftan, KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı Noterler ve TNB'nin Avrupa Veri Koruma Tüzüğü (GDPR) kapsamına girmesi söz konusudur. Bu nedenle GDPR gereğince ek bazı teknik sorumluluklar ile idari ve cezai yükümlülükleri de bulunabileceği, GDPR yaptırımların sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

[3] https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%BOS.pdf

2. Kişisel Verileri Koruma Kanunu (KVKK)

6698 sayılı Kişisel Verileri Koruma Kanunu 07.Nisan.2016 tarihinde yürürlüğe girmiş ve 07.Nisan.2018 tarihinde 2 yıllık geçiş sürecini de tamamlamıştır. Kanunun **amacı**;

> *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"*

olarak tanımlanmaktadır. Kanunda "***verilerin işlenmesi***" ise şöyle tanımlanmıştır:

> *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi* ***veriler üzerinde gerçekleştirilen her türlü işlem****"*

Verilerin işlenmesi ile ilgili olarak KVKK ve diğer düzenlemeler kapsamında bir dizi kurumsal ve kişisel sorumluluklar ve yeni ünvanlar getirilmiş ve yükümlülükler de ayrıntılı olarak tanımlamıştır.

Veri Sorumlusu

KVKK'da Veri Sorumlusu; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmış, ***herhangi bir kişi ya da kurum bu yükümlülükten muaf tutulmamıştır***.

Veri İşleyen

Diğer yandan KVKK, Veri İşleyeni de; *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlamaktadır.

KVKK'nın ilgili tanımlarına göre noterler ve TNB bazı durumlarda doğrudan **veri sorumlusu**, bazı durumlarda da **veri işleyen** niteliğini haiz olmaktadır.

2.1. Yükümlülükler

KVKK'nın 10. ve 12. maddeleri **Veri Sorumlusu** ile ilgili yükümlülükleri sıralamıştır:

> ***MADDE 10-****1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*
>
> *a) Veri sorumlusunun ve varsa temsilcisinin kimliği,*
> *b) Kişisel verilerin hangi amaçla işleneceği,*
> *c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,*
> *ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,*
> *d) 11 inci maddede sayılan diğer hakları,*
>
> *Konusunda bilgi vermekle yükümlüdür.*

Kişisel verilerin güvenliğine yönelik yükümlülükler:

> ***MADDE 12-*** *1) Veri sorumlusu;*
>
> *a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
> *b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
> *c) Kişisel verilerin muhafazasını sağlamak,*
>
> *Amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli* ***her türlü teknik ve idari tedbirleri almak zorundadır****.*

Diğer taraftan denetime yönelik sorumluluklar da *"Veri sorumlusu, kendi kurum veya kuruluşunda, bu* ***Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır****."* olarak açıklanmıştır.

2.2. Yaptırımlar

6698 sayılı kanun, ilgili hükümleri ihlal edilmesi durumunda, ihlalleri niteliğine göre "***suçlar***" ve "***kabahatler***" olarak ayırmış olup, kabahatler için sorumlu kişi veya kurumlara KVKK idari para cezası uygulamayı, söz konusu ihlalin bir kamu kurumu tarafından yapılması durumunda disiplin cezası uygulanması için ilgili kurumun bilgilendirilmesini öngörmektedir.

Kişisel veriler ile ilgili ihlallerin suç niteliğini haiz olması durumunda ise **TCK'nın 135-140. maddeleri** gereği işlem yapılmasını öngörmektedir.

İdari Para ve Disiplin Cezaları

6698 sayılı kanun kişisel verilere yönelik yükümlülüklerin yerine getirilmemesi durumunda Veri Sorumlusuna **5.000 TL**'ndan **1.000.000 TL**'na kadar **idari para cezası** verilir ve/veya **diğer idari işlemler** uygulanır.

Hapis Cezaları

6698 sayılı kanunun 17. maddesinde kişisel verilere yönelik yükümlülüklerin ihlal edilmesinden kaynaklanacak suçlar için uygulanacak ceza işlemleri aşağıdaki gibi tanımlanmaktadır;

Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140. madde hükümleri uygulanır.

- ✓ *Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası,*
- ✓ *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası uygulanır.*

Tazminat Hakkı

İdari para ve disiplin cezaları ile hapis cezalarının yanı sıra 6698 sayılı kanunun 14. maddesinin (3). fıkrasına göre "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre **tazminat hakkı** saklıdır.*"

2.3. KVKK Uygulama Örnekleri

6698 sayılı KVKK ile kurulan Kişisel Verileri Koruma Kurumu ve Kurulu bugüne kadar bir dizi ikincil mevzuatı düzenleyip uygulamaya koymuştur. Bu düzenlemeler gereğince bir dizi inceleme ve yaptırımları da uygulamaya başlamıştır.

KVK Kurumu, kuruluşundan bugüne kadar çeşitli uygulamaları ve yaptırımları hayata geçirmiştir. Başlıca ceza gerekçeleri;

- ✓ *Veri Güvenliğine Yönelik Gerekli Teknik ve İdari Tedbirlerin Alınmaması*
- ✓ *Kanuna Aykırı Şekilde Kişisel Verilerin Paylaşılması*
- ✓ *Kişisel Veri Güvenliğinin Sağlanması Amacıyla Uygun Güvenlik*
- ✓ *İlgili Kişinin Verilerinin Silinmesi Talebinin Yerine Getirilmemesi*
- ✓ *Açık Rızanın Hizmet Şartına Bağlanması*
- ✓ *Özel Nitelikli Kişisel Verilerin Kanuna Aykırı Şekilde İnternet ve Sosyal Medya Mecralarında Paylaşılmasıdır.*

KVKK tarafından kesilen başlıca idari para cezaları ve gerekçeleri aşağıdaki gibidir;

Tarih	Veri Sorumlusu / İşleyen	Ceza [TL]	İlgili Maddeler	Açıklamalar
18.09.2019	Facebook	**1.150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	**1.000.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	**1.000.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	**680.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
11.04.2019	Facebook	**550.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
18.09.2019	Facebook	**450.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	**450.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Click Bus	**450.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	**400.000**	m. 12/1 a-b-c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
16.05.2019	Marriott International In.	**350.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
6.02.2020	Banka	**210.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	S Şans Oyunları	**150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
14.02.2019	Teknik Servis	**150.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
9.12.2019	Gazete	**125.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
1.10.2019	Havayolu Taşımacılığı	**100.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
10.09.2019	Banka	**100.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
27.08.2019	Turizm Şirketi	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Cathay Pacific Havayolu	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
16.05.2019	Click Bus	**100.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
8.07.2019	Yatırım Şirket	**75.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	**70.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
7.11.2019	Doktor	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
18.09.2019	Sevinç Eğitim Kurumları	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
17.08.2019	Dubsmash Inc	**50.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Avukat	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
31.05.2019	Şirket	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
5.03.2019	Teknik Servis	**50.000**	m. 12/1 a	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
26.11.2019	Banka	**30.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
27.08.2019	S Şans Oyunları	**30.000**	m. 12/5	En Kısa Zamanda Bildirimde Bulunmamak
31.05.2019	Varlık Şirketi	**20.000**	m. 12/1 a	Genel Veri İşleme İlkelerine Uyumsuzluk
1.10.2019	Operatör Şirket	Talimat		
1.07.2019	M.S.G.S.Üniversitesi	Disiplin		
25.03.2019	Spor Salonu	İdari Para Cezası		
14.02.2019	Teknik Servis	Linkleri Durdurma		
2.05.2019	Ziraat Bankası	Talimat		

3. Avrupa Veri Koruma Tüzüğü (GDPR)

Noterlerin ve TNB'nin KVKK sorumluluk ve yükümlülüklerinin yanı sıra Avrupa Veri Koruma Tüzüğü (GDPR) gereğince ek bazı teknik, idari ve cezai sorumluluk ve yükümlülükleri de bulunmaktadır.

3.1. Kapsam

AB, GDPR düzenlemelerinin kapsamını AB ülkeleri ile sınırlı bırakmayıp, Avrupa vatandaşları ile ilgili kişisel verilerin işlendiği **Avrupa dışında yerleşik tüm kurum ve kuruluşları** da kapsayacak biçimde genişletmiştir.

3.2. Cezalar

AB, GDPR kapsamında öngörülen idari para cezaları da oldukça ciddi miktarlara ulaşmaktadır;

Bir takım idari yükümlülüklerin yerine getirilmemesi durumunda;

- ✓ ***10.000.000 Euro****'ya kadar* ***veya*** *bir teşebbüs olması halinde, bir önceki mali yılın yıllık* ***dünya çapındaki cirosunun %2'sine kadar*** *idari para cezalarına (hangi meblağ yüksek ise, o geçerlidir)*

Bir veri saçılması durumunda ise;

- ***20.000.000 Euro'ya kadar veya bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezalarına*** *(hangi meblağ yüksek ise, o geçerlidir)*

GDPR kapsamında Mayıs.2018 tarihinden itibaren kesilen başlıca idari para cezaları aşağıdaki gibidir;

Ülke	Tarih	Ceza [€]	Veri Sorumlusu / İşleyen	İlgili Maddeler (GDPR)	Açıklamalar
İNGİLTERE	8.07.2019	**204.600.000**	British Airways	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	9.07.2019	**110.390.200**	Marriott International, Inc	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.01.2019	**50.000.000**	Google Inc.	m.13, m.14, m.6, m.5	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	15.01.2020	**27.800.000**	TIM	m.5, m.6, m.17, m.21, m.32	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	23.10.2019	**18.000.000**	Austrian Post	m.5(1) a, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	30.10.2019	**14.500.000**	Deutsche Wohnen SE	m.5, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	9.12.2019	**9.550.000**	1&1 Telecom GmbH	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSVEÇ	11.03.2020	**7.000.000**	Google LLC	m.5, m.6, m.17	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
BULGARİSTAN	28.08.2019	**2.600.000**	Ulusal Gelir İdaresi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	31.10.2019	**900.000**	UWV (Çalışan Sigorta Hizmetleri)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
POLONYA	10.09.2019	**644.780**	Morele.net	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
HOLLANDA	3.03.2020	**525.000**	Royal Dutch Tennis Association ("KNLTB")	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
BULGARİSTAN	28.08.2019	**511.000**	DSK Bank	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	21.11.2019	**500.000**	Futura Internationale	m.5, m.6, m.13, m.14, m.21	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
HOLLANDA	18.06.2019	**460.000**	Haga Hastanesi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
PORTEKİZ	17.07.2018	**400.000**	Kamu Hastanesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
FRANSA	28.05.2019	**400.000**	SERGIC (Emlak)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İNGİLTERE	20.12.2019	**320.000**	Doorstep Dispensaree Ltd. (Pharmacy)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	11.06.2019	**250.000**	Profesyonel Futbol Ligi (LaLiga)	m.5(1) a, m.7(3)	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
POLONYA	26.03.2019	**219.538**	Özel Veri Şirketi	m.14	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
NORVEÇ	29.04.2019	**203.000**	Oslo Belediyesi Eğitim Birimi	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	3.06.2019	**200.850**	IDdesign A / S	m.5(1) e, m.5(2)	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	**200.000**	Telekom Hizmet Sağlayıcısı	m.5(1) c, m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
YUNANİSTAN	7.10.2019	**200.000**	Telekom Hizmet Sağlayıcısı	m.21(3), m.25	Genel Veri İşleme İlkelerine Uyumsuzluk
ALMANYA	19.09.2019	**195.407**	Delivery Hero	m.15, m.17, m.21	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
FRANSA	25.07.2019	**180.000**	ACTIVE ASSURANCES (Otomobil Sigorta)	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
NORVEÇ	2019-03	**170.000**	Bergen Belediyesi	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
DANİMARKA	11.07.1905	**160.000**	Taxa 4x35	m.5(1) e	Genel Veri İşleme İlkelerine Uyumsuzluk
ROMANYA	9.10.2019	**150.000**	Raiffeisen Bank SA	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
LATVIA	2019-11	**150.000**	Bilinmiyor	m.6	Veri İşleme için Yetersiz Yasal Dayanak
YUNANİSTAN	19.12.2019	**150.000**	Aegean Marine Petroleum Network Inc.	m.5, m.6, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
YUNANİSTAN	30.07.2019	**150.000**	PWC Business Solutions	m.5(1),5(2), m.6(1), m.13(1)c, m.14(1)c	Veri İşleme için Yetersiz Yasal Dayanak
ROMANYA	27.06.2019	**130.000**	UNICREDIT BANK SA	m.25(1), m.5(1)c	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	27.02.2020	**120.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	3.12.2019	**105.000**	Hastane	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
MACARİSTAN	23.05.2019	**92.146**	SZIGET ve VOLT festivalleri Organizatörü	m.6, m.5(1)b, m.13	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	14.02.2020	**80.000**	Iberdrola Clientes	m.6	Veri İşleme için Yetersiz Yasal Dayanak
ALMANYA	11.07.1905	**80.000**	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
ALMANYA	11.07.1905	**80.000**	Bilinmiyor	m.32	Yetersiz İdari ve Teknik Veri Güvenliği Tedbirleri
İSPANYA	3.02.2020	**75.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	**75.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	**75.000**	EDP España S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	7.01.2020	**75.000**	EDP Comercializadora, S.A.U.	m.6	Veri İşleme için Yetersiz Yasal Dayanak
LİTVANYA	16.05.2019	**61.500**	Payment service provider UAB MisterTango	m.5, m.32, m.33	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	4.03.2020	**60.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	**60.000**	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	**60.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	21.11.2019	**60.000**	Viaqua Xestión Integral Augas de Galicia	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	19.11.2019	**60.000**	Corporación radiotelevisión espanola	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	19.11.2019	**60.000**	Xfera Moviles S.A.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	16.10.2019	**60.000**	Xfera Moviles S.A.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	16.08.2019	**60.000**	AVON COSMETICS	m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	**60.000**	Debt collecting agancy (GESTIÓN DE COBROS, YO COBRO	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	11.07.1905	**60.000**	ENDESA (Enerji Dağıtımı)	m.5(1) f	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	3.02.2020	**50.000**	Vodafone España, S.A.U.	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
SLOVAKYA	-	**50.000**	Sosyal Güvenlik Kurumu	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	17.04.2019	**50.000**	Italian political party Movimento 5 Stelle	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
ALMANYA	03.2019	**50.000**	N26	m.6	Veri İşleme için Yetersiz Yasal Dayanak
AVUSTURYA	03.2020	**50.000**	Sağlık Sektöründe Bir Şirket	m.13, m.37	Aydınlatma Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	28.02.2020	**48.000**	Vodafone ONO, S.A.U.	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.02.2020	**48.000**	HM Hastaneleri	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
POLONYA	16.10.2019	**47.000**	ClickQuickNow	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	7.01.2020	**44.000**	Vodafone España, S.A.U.	m.5(1) f	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	3.03.2020	**42.000**	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.02.2020	**42.000**	Vodafone España, S.A.U.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.03.2020	**40.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
SLOVAKYA	-	**40.000**	Slovak Telekom	m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	25.10.2019	**36.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İSVEÇ	16.12.2019	**35.000**	Nusvar AB	m.6	Veri İşleme için Yetersiz Yasal Dayanak
MACARİSTAN	5.04.2019	**34.375**	Hugarian political party	m.33(1), m.33(5), m.34(1)	Veri İhlali Bildirim Yükümlülüğünün Tam Olarak Yerine Getirilmemesi
İSPANYA	14.02.2020	**30.000**	Xfera Moviles S.A.	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	14.11.2019	**30.000**	Telefónica SA	m.5	Genel Veri İşleme İlkelerine Uyumsuzluk
İSPANYA	1.10.2019	**30.000**	Vueling Airlines	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İTALYA	23.01.2020	**30.000**	Azienda Ospedaliero Universitaria Integrata di Verona	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İTALYA	23.01.2020	**30.000**	Sapienza Università di Roma	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
BULGARİSTAN	26.02.2019	**27.100**	Telekom Hizmet Sağlayıcısı	m.6, m.5(1) a	Veri İşleme için Yetersiz Yasal Dayanak
İSPANYA	-	**27.000**	Vodafone España, S.A.U.	m.5(1) d	Veri Sahibi Hakları Sağlanama Yükümlüğünün Tam Sağlanamaması
İSPANYA	3.03.2020	**24.000**	Vodafone España, S.A.U.	m.5, m.6	Veri İşleme için Yetersiz Yasal Dayanak
İZLANDA	10.03.2020	**20.600**	National Center of Addiction Medicine ("SAA")	m.5(1) f, m.32	Veri Güvenliği için Gerekli İdari ve Teknik Tedbirlerin Alınmaması
İSPANYA	3.02.2020	**20.000**	Iberia Lineas Aereas de Espana, S.A. Operadora	m.5, m.6, m.21	Veri İşleme için Yetersiz Yasal Dayanak

4. Noterlik ve Kişisel Verilerin Korunması

KVKK sorumluluk ve yükümlülüklerinin yanı sıra, yaptığı iş ve işlemler ile aktardığı veya aktarılan bir takım kişisel verilerden dolayı Noterler ve TNB'nin Avrupa Veri Koruma Tüzüğü (GDPR) kapsamına girmesi söz konusudur. Bu nedenle GDPR gereğince ek bazı teknik sorumluluklar ile idari ve cezai yükümlülükleri de bulunabileceği, GDPR yaptırımların sonuçlarının ise daha ağır olduğu göz önünde bulundurulmalıdır.

Noterlik Kanunu *"Noter ve noterlik kâtipleri,* ***görevleri dolayısiyle öğrendikleri sırları****, kanunların emrettiği haller dışında açıklıyamayacaklarına"* hükmetmektedir.

> ***Noterlik Mesleği:***
> *Madde 1 –Noterlik bir kamu hizmetidir. Noterler, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek için işlemleri belgelendirir ve kanunlarla verilen başka görevleri yaparlar.*
>
> ***Meslek sırrı:***
> *Madde 54–Noter ve noterlik kâtipleri, görevleri dolayısiyle öğrendikleri sırları, kanunların emrettiği haller dışında açıklıyamazlar.*
>
> ***Evrak ve defterlerin gizliliği:***
> *Madde 55–Noterlik evrak ve defterleri mahkeme, sorgu hâkimliği ve Cumhuriyet savcılıklarınca veya resmi daireler tarafından, konusu da belirtilmek suretiyle, noterlikte soruşturmaya yetkili kılınan kimselerce incelenebilir.*
>
> *Noterlik evrak ve defterlerinin daire dışına çıkarılabilmesi, mahkemenin veya sorgu hâkiminin kararıyle mümkündür.*
>
> *Mahkeme veya sorgu hâkimi evrakın dava sonuna kadar dosyada kalmasına karar verirse, bu takdirde evrakın bir örneği çıkartılıp aslına uygunluğu onaylanarak, aslının yerinde saklanmak üzere notere verilir.*
>
> *Noterin bulunduğu yerde inceleme imkânı bulunmaması sebebiyle evrakın başka bir yere gönderilmesi gerekiyorsa, noterin bulunduğu yer hukuk hâkimliğinin onaylıyacağı örnek, aynı şekilde saklanır.*

Noterlik Yasasında Elektronik işlemler ile (*198/A maddesi*) yapılan değişiklikle;

- ✓ *"Belirlenen bu noterlik işlemlerine ilişkin tüm bilgi ve belgeler güvenli elektronik imzayla elektronik ortamda işlenebilir, saklanabilir ve gerektiğinde ilgili diğer kişi veya kurumlara elektronik ortamda gönderilebilir."*
- ✓ "*Noterler tarafından yapılan tüm işlemlere dair bilgi ve belgelerin* ***Türkiye Noterler Birliğinin Bilişim Sisteminde kaydedilmesi ve saklanması***" ve
- ✓ "*Noterlik işlemlerinin elektronik ortamda yapılması sırasında işlenen* ***kişisel verilerin korunması ve bilgi güvenliğinin sağlanması*** *için gerekli tedbirler alınması*"

yükümlülüğü getirilmiştir. Ayrıca;

- ✓ *"Noterlik işlemlerinin elektronik ortamda yapılmasına, saklanmasına ve paylaşılmasına ilişkin usul ve esaslar yönetmelikte düzenlenir."*
- ✓ *"Yabancı memleketlerde, noterlik işlemlerinin elektronik ortamda yapılması için sağlanması gerekli olan teknik ve idari şartlara dair usul ve esaslar yönetmelikte düzenlenir."*

4.1. KVKK/GDPR ve Noterlerin Yükümlülükleri

KVKK düzenlemelerine göre, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan her gerçek veya tüzel kişi "**veri sorumlusu**"dur. Noterliklerde yapılan işlemlerde işlenen kişisel veriler bakımından veri sorumlusu "**noter**"dir.

TNB genel olarak işlediği kişisel veriler (*örneğin, personel kayıtları*) ile ilgili olarak veri sorumlusu iken, Noterlik Kanunu'nun 198/A maddesi uyarınca "*Noterler tarafından yapılan tüm işlemlere dair bilgi ve belgeler*"i kendi bilişim sisteminde kaydedip saklamakla yükümlü olduğu için bir veri işleyendir.

Veri sorumlusu sıfatıyla noterler ve TNB Kişisel Verilerin Korunması Kanunu'nda sayılan "*ilkeler*"e ve "*veri işleme şartları*"na eksiksiz uymakla yükümlüdürler. Örneğin, kanunlarda "*açıkça*" öngörülen hallerde noter o verinin ilişkili olduğu kişinin (***ilgili kişi***) "açık rızası" almadan veri işleyebilecektir. Bunun gibi Kanun'da sayılan istisnai işleme şartlarından herhangi birinin bulunmaması halinde ise noterin veri işleyebilmesi için ilgili kişinin açık rızasını alması bir zorunluluktur.

Veri sorumlusunun yükümlülükleri, koşulları oluştuğunda kişisel verilerin "**silinmesi**", "**yok edilmesi**" veya "**anonim hale getirilmesi**"ni de içermektedir. Keza, Kanun kişisel verilerin yurt içinde veya yurt dışına aktarılması bakımından (*örneğin, noterler arasında, noterler ile TNB arasında, noterler/Birlik ile kamu-özel üçüncü kişiler arasında, başka ülkelere (konsolosluklara) veri gönderilmesi esnasında*) ek yükümlülükler getirmekte, hatta belirli durumlarda Kişisel Verilerin Korunması Kurulu'nun iznini şart koşmaktadır.

Noterlerin ve TNB'nin kişisel verileri işlenen veri sahiplerine (*ilgili kişilere*) yönelik doğrudan yükümlülükleri de bulunmaktadır. Veri sahiplerinin kendileriyle ilgili olarak işlenen veriler bakımından tam ve doğru şekilde noter ve yerine göre TNB tarafından işleme öncesinde (*en geç veri işlemesi esnasında*) aydınlatılması gerekir. Bu işlemin yapılmaması veya gereği gibi yerine getirilmemesi noterin veya TNB'nin sorumluluğunu doğurur. Aynı şekilde veri sahiplerinin Kişisel Verilerin Korunması Kanunu ile özel olarak koruma altına alınmış olan haklarına noter veya TNB tarafından riayet edilmemesi yine sorumluluklara yol açacaktır.

Veri güvenliğinin Kanun'da öngörülen çerçevede tesis edilmesi gerek noterler gerekse TNB için başlı başına bir yükümlülüktür. Bu yükümlük sadece teknik tedbirler alınmasını gerektirmemekte, aynı zamanda çeşitli idari tedbirlerin alınmasını zorunlu kılmaktadır. Noterlik hizmetinin daire dışında da yerine getirilmesinin mümkün olduğu düşünüldüğünde veri güvenliğine ilişkin alınması gereken tedbirlerin sadece noterlik dairesinde ve TNB'de alınması gereken tedbirlerden ibaret olmadığı açıktır.

4.5. KVKK/GDPR ve Noterlerin Riskleri

Noterlerin işlediği özel nitelikli kişisel veriler, Kanunun 6. maddesinde öngörülmüş olan özel işleme şartlarına tabidirler. Noterlerin ve noterlik çalışanlarının kişisel verilerin korunmasına ilişkin genel bilincin ötesinde bu gibi detayları ayırt edebilecek durumda olmaları gerekmektedir. Noterler birçok noterlik işlemi için fotoğraf, bazen de parmak izi alırlar. **Fotoğraf, ıslak imza ve parmak izi biyometrik verilerdir** ve dolayısıyla "***özel nitelikli kişisel veri***"dir.

Bu kişisel verilerin işlenmesi, gerek KVKK gerekse TCK kapsamında bir takım hukuki, idari ve cezai müeyyideler ile güvence altına alınır. KVKK uyumun gereği yükümlülükleri yerine getirmeyenler de gerek ceza hukuku (*TCK*) gerek idare hukuku (*KVKK*) gerekse özel hukuk (*MK, BK ve diğer kanunlarda*) ile öngörülen yaptırımlara maruz kalacaklardır.

Kanunun 17. maddesinde işaret edildiği üzere, TCK 135 ile 140 arasında düzenlenmiş olan suç ve cezalar öncelikle kişisel verilen korunmasını ihlal eden fiilleri kapsar. Kişisel verilerin korunması ile ilgili suç teşkil eden fiilleri işleyenleri her bir fiil için 1 yıldan 6 yıla kadar hapis cezaları beklemektedir. Örneğin, kişisel verileri hukuka aykırı olarak bir başkasına veren bir noter veya noter/TNB çalışanı, TCK 136'daki **suçun nitelikli halini işlemiş olacağından** 3 ile 6 yıl arasında bir hapis cezasına çarptırılacaktır.

Kanunun 18. maddesinde çeşitli kabahatler tanımlanmıştır. Bu kabahatleri işleyen veri sorumlularına **5.000 TL** ile **1.000.000 TL** arasında idari para cezaları uygulanır. Her bir ihlal bakımından ayrı ayrı söz konusu olacak olan bu cezalar kişisel verilerin korunmasına ilişkin yükümlüklerini yerine tam olarak getirmeyen noterler bakımından önemli bir risktir. Örneğin, veri güvenliğine ilişkin yükümlülüklerini yerine getirmeyen bir notere **1.000.000 TL**'sına kadar idari para cezası verilmesi mümkündür.

Söz konusu kabahatlerin TNB'nin bünyesinde işlenmesi halinde Birliğin kendisine bir idari para cezası kesilmeyecektir. Ancak, kabahat teşkil eden bir fiilin işlenmesine iştirak eden TNB görevlileri hakkında disiplin hukuku hükümleri işletilecek ve neticesi KVK Kurulu'na bildirilecektir. Noterlik Kanunu bu noktada "uyarma"dan "meslekten men"e uzanan bir dizi ceza öngörmektedir.

Son olarak kişisel verilerin korunmasına ilişkin yükümlüklerin ihlali beraberinde özel hukuk hükümlerine göre noterlerin ve yerine göre TNB'nin sorumluluğunu doğuracaktır. Kanunun 14. maddesinde bu hususa "*Kişilik hakları ihlal edilenlerin, genel hükümlere göre* ***tazminat hakkı*** *saklıdır*" demek suretiyle işaret edilmektedir. Kişisel verilerin korunması bilinci yaygınlaştıkça Noterler ve TNB, her geçen gün sayısı artarak devam edecek olan **tazminat taleplerine** muhatap olacaklardır.

Noterlik Kanunu'nun 198/A maddesi "*Noterlik işlemlerinin elektronik ortamda yapılması sırasında işlenen kişisel verilerin korunması ve bilgi güvenliğinin sağlanması için gerekli tedbirler alınır.*" hükmünü içermektedir.

T.C. Adalet Bakanlığı'nca çıkarılan "*Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik*"te ise;

> ***MADDE 8 –*** *(1) Birlik, elektronik ortamda güvenli elektronik imza ile işlem yapılmasına imkân sağlayacak altyapıyı kurar ve işletir.* ***Bu altyapının güvenli olarak kurulması ve işletilmesi için gerekli tüm tedbirleri alır.***
>
> *2) Bu Yönetmelik kapsamında diğer* ***kurum ve kuruluşlarla yapılacak bilgi ve belge paylaşımlarında kullanım ve erişim standartları ile diğer gerekli şartlar Birlik tarafından belirlenir.***
>
> ***İşlemlerin elektronik ortamda kaydedilmesi ve saklanması***
>
> ***MADDE 9*** *– (1) İşleme katılanların tamamının güvenli elektronik imzası ile elektronik ortamda yapılan bir işlem için talep edilmedikçe fizikî olarak belge düzenlenmez ve bu işleme ilişkin olarak elektronik ortam dışında bir saklama yapılmaz.* ***Bu kayıtlar iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak, yedekli ve güvenli bir şekilde saklanır.***
>
> *(2) Birinci fıkra kapsamında kalmayan diğer noterlik işlemlerinde ise işleme ait belgenin imzaya açılan son hâli noter tarafından güvenli elektronik imza ile imzalanarak TNBBS'ye kaydedilir. Belgenin ilgililerce imzalı hâli ise Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine göre saklanır.*
>
> ***İşlemlerin elektronik ortamda paylaşılması***
>
> ***MADDE 10*** *– 1) İşleme katılanların tamamının güvenli elektronik imzası ile yapılan işlemlere ilişkin bilgi ve belgeler gerektiğinde* ***noterler ile diğer kişi ve kurumlarla paylaşılabilir****.*
>
> *2) El ürünü imza ile hazırlanıp güvenli elektronik imza ile TNBBS'ye kaydedilen işlemlere ilişkin bilgiler gerektiğinde* ***noterler ile diğer kişi ve kurumlarla paylaşılabilir****.*
>
> *3)* ***Birlik, noterlik işlemlerinin elektronik ortamda yapılması sırasında kişisel verilerin korunması ve bilgi güvenliğinin sağlanması için gerekli tedbirleri alır****.*
>
> *4) Noterlik işlemlerine ilişkin bilgi ve belgenin paylaşılmasının sağlanması için Bakanlığın görüşü alınarak Birlik tarafından ilgili kurum ve kuruluşlar ile protokol imzalanır. Paylaşıma ilişkin ücretler protokolde düzenlenir.*
>
> *5)* ***Paylaşıma ilişkin iz bilgileri güvenliği, gizliliği ve bütünlüğü sağlanarak TNBBS'de tutulur. Saklanacak iz bilgisi içeriği Birlik tarafından belirlenir****.*
>
> ***İlgilinin talebiyle belgenin elektronik ortamda gönderilmesi veya paylaşılması***
>
> ***MADDE 11*** *– (1) İlgilisi tarafından bir belgenin* ***üçüncü kişi ile elektronik ortamda paylaşılmasının istenmesi*** *durumunda belge, gerekli ücretlerin ödenmesi koşuluyla;*
>
> *a) Üçüncü kişinin KEP adresine gönderilmesi,*

*b) Üçüncü kişinin Birlik tarafından bilgi ve belge paylaşımı için protokol imzalanan bir kurum veya kuruluş olması durumunda **ilgili protokol hükümleri çerçevesinde belgeye erişim sağlanması**,*
c) İlgiliye erişim kodu verilmesi hâlinde bu kod ile TNBBS üzerinden erişiminin sağlanması,

yöntemlerinden biri veya birkaçı ile paylaşılır.

*2) Belgeye birinci fıkranın (c) bendinde belirlenen erişim kodu ile talep edilen **üçüncü kişi yerine başka bir kişinin erişmesinden noter veya Birlik sorumlu tutulamaz**.*

3) Birlik, kendi kuracağı sistem gereği ilgili kurumdan bilgi veya belge paylaşımı için, protokol imzalanmasını isteme, paylaşım alt yapısını belirleme hak ve yetkisine sahiptir. İlgili kurum veya kuruluş bu gerekleri karşılamadan bilgi ve belgenin elektronik ortamda paylaşılmasını talep edemez.

Yabancı memleketlerde noterlik işlemlerinin elektronik ortamda yapılması ve Dışişleri Bakanlığı ile bilgi ve belge paylaşımı

***MADDE 12** – (1) **Yabancı memleketlerde noterlik işlemleri bu Yönetmelikte gösterilen usullere göre elektronik ortamda güvenli elektronik imza ile de yapılabilir, işlenebilir, saklanabilir, paylaşılabilir ve gönderilebilir**.*

2) Yabancı memleketlerde noterlik işlemlerinin elektronik ortamda yapılması için sağlanması gerekli olan teknik ve idarî şartlara dair usul ve esaslar Birlik ve Dışişleri Bakanlığı arasında yapılacak protokol ile belirlenir.

Bu hükümler KVKK düzenlemeleri bağlamında TNB'nin Noterler ile gerek yurtiçinde gerekse de yurtdışındaki diğer kamu kurum ve kuruluşları ve bazı durumlarda 3. kişiler arasındaki kişisel veri paylaşımındaki ilişkilerde, **ciddi bir risk unsuru** olarak dikkate alınmalıdır.

Ayrıca, Kanun kapsamına sadece otomatik olarak işlenen kişisel veriler değil, bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel veriler de girmektedir. Bu nedenle basılı veya dijital ortamda işlenip işlenmediğine bakılmaksızın TNB veya Noterlerde işlenen ve kişisel veri niteliği taşıyan her türlü veriler bakımından Kanun tarafından belirlenmiş yükümlükler ve bu uygulamalara bağlı riskler mevcuttur.

Diğer taraftan Noterlik Kanunu Yönetmeliği;

Madde 32 - Türkiye Noterler Birliğinde aşağıda gösterilen defterlerin tutulması zorunludur.

1 - Karar defterleri,
2 - Sicil defterleri,
3 - Vasiyetnamelerin tesciline dair uluslararası sözleşmelere göre tutulacak defterler,
4 - Muhasebe defterleri,
5 - Diğer defterler,
6 - Disiplin Kurulu defterleri

Madde 35: Vasiyetnamelerin tescili sözleşmesine göre tutulacak defterler

*Vasiyetnamelerin tescil konusunda bir usul kurulmasına dair **Avrupa Sözleşmesi**[4] **uyarınca tescil gereken vasiyetnamelere ilişkin bilgiler sözleşmede yazılı olduğu şekilde bu defterlere işlenir.***

Bu defter de 33 üncü maddedeki usule göre onaylanır.

TNB, Noterlik Kanunu Yönetmeliği'nde yer alan 32.maddeki; Türkiye Noterler Birliğinde tutulacak defterler ve ***35.maddedeki; Vasiyetnamelerin Tescili Sözleşmesi'ne göre tutulacak defterler*** kapsamında ve benzeri Avrupa yerleşik kişilere yönelik diğer işlemlerden dolayı da ayrıca **GDPR düzenlemeleri kapsamında da bazı idari ve hukuki yükümlülükler ile idari para cezası risklerini** taşımaktadır.

Ayrıca GDPR düzenlemelerine göre de "*bir ihlal sonucu **maddi veya manevi zarar gören** herhangi bir kişi, yaşanan zarara ilişkin olarak veri sorumlusu veya veri işleyenden **tazminat alma hakkına** sahiptir.*"

[4] 17.4.1975 tarih ve 1885 sayılı "Vasiyetnamelerin Tescili Konusunda Bir Usul Kurulmasına Dair Avrupa Sözleşmesinin Onaylanmasının Uygun Bulunduğuna İlişkin Kanun"

4.6. Uyumluluğa Yönelik Adımlar

Günlük çalışma süreçlerine etkili veri koruma denetimleri uygulamak büyük bir zorluktur, ancak KVKK ve GDPR düzenlemeleri yürürlüğe girdiğinden bu yana, kişisel verilerin toplanması, işlenmesi ve paylaşılması, bu düzenlemeler açısından bazı uyumsuzluklara yol açabileceğinden noterlikleri büyük para cezaları ve itibar gibi ciddi riskler beklemektedir.

Noterlerin KVKK/GDPR düzenlemelerine uyumluluk için yapması gereken iş ve işlemler temel aşağıdaki gibidir:

Farkındalık

Noterlikler ve TNB'nin KVKK/GDPR uyumluluk projelerini ve bu düzenlemeler göre nelere ihtiyacı olduğu ve kendi kuruluşları için önemli risklerin ne olduğu konusunda özellikle üst yönetim arasında farkındalığı artırarak başlatmaları çok önemlidir.

Kurumun gerekli zamanı ve kaynakları taahhüt etmesini ve mahremiyete saygı duyan bir kültür geliştirmesini sağlamak için doğru insanları en üst yönetim seviyesine dâhil etmek gerekir.

Eğitim

KVKK/GDPR uyumluk projesinin başlangıcında farkındalığa yönelik ve daha uyumluluk politika ve planlarının uygulanmasına yönelik tüm personele ve mürettebata gerekli eğitimler verilmelidir.

Gemilerde seyahat belgeleri ve diğer kişisel veriler tutulmaktadır. Bu nedenle gemideki görevlilere belirli aralıklarla ve uygun ölçüde eğitimlerin verilmesi de önemlidir.

Veri Koruma Takımının Oluşturulması

KVKK/GDPR uyumluluk projesini yürütmek için yönetimin tam desteğiyle, risk, yasal ve bilişim teknolojileri çalışanlarından oluşacak bir ekip kurmaları gerekir.

Güvenilir harici danışman desteği; teknik uzmanlık, maliyet ve zaman kazanmanıza yardımcı olacaktır.

Hesap Verebilirlik ve Yönetişim Çerçevesi

KVKK/GDPR uyumluluğu, en üst düzeyde destek gerektiren bir süreçtir. Bu nedenle noterlerin bizzat kendilerinin KVKK/GDPR düzenlemelerinin gereklerini, yükümlülüklerini, risklerini ve sonuçlarını iyi anlaması gerekmektedir. KVKK/GDPR uyumluluğunun sağlanması ve daha da önemlisi sürdürülebilmesi için gerekli kaynakların uygunluğu sağlamak ve sürdürmek için gereken kaynakların tahsis edilmesi noterlerin bu konudaki bilgisi ile yakından ilgilidir.

Veri İşleme Envanterinin Hazırlanması

Veri işleme faaliyetlerini belirlemesi ve veri işleme envanterinin hazırlanması ciddi bir iş yükü getirir ancak özellikle noterlikler için yasal bir zorunluluk niteliğindedir.

Veri işleme envanterinin hazırlanması, her faaliyet için veri toplamadan yok etmeye kadar tüm veri yaşam döngüsünün anlaşılmasını ve hazırlanmasını sağlar.

Fark Analizi ve Uyumluluk Planı

Kişisel verilerin işlenmesi sürecinde kuruluşlar veri akışlarındaki bir dizi zayıflık ve kırılganlıkların oluşması olasıdır. KVKK/GDPR uyumluluk çalışmaları kapsamında bu zayıflıklar ve kırılganlıklar dikkatlice aranmalı ve bunların yol açacağı olası riskler değerlendirmelidir. Daha sonra bu riskleri kabul edilebilir bir seviyeye indirgeyecek veya ortadan kaldıracak pratik eylem planları oluşturulmalıdır.

Zayıflıkları uzun soluklu izlenmesi ve yeni kırılganlıkların oluşmasını engellemek için uygulama planları ve prosedürler belirlenmelidir.

Veri Koruma ve Gizlilik Politikalarının Hazırlanması

Belirli eylem planı tamamlandığında, uyumluluk için uygulama aşamasına geçebilir. Bu normalde gizlilik politikalarında değişiklik yapılmasını, personel acenteleriyle yapılan sözleşmeleri, liman acentelerine, personele ve mürettebata bilgi bildirimlerinin yanı sıra uygun rıza formlarının hazırlanmasını içerir.

Uygulama, manuel prosedürler, BT güvenliği (*güvenlik duvarları, şifreleme vb.*) ve iş sürekliliği ile olağanüstü durum kurtarma planındaki değişiklikleri de içermelidir.

Dış danışmanlar uygulamanın çeşitli yönlerini yerine getirmeye yardımcı olabilir, fakat aynı zamanda çabayı yönetmeye de yardımcı olabilirler.

Veri İhlal Süreçlerinin Hazırlanması

Noterlikler, ihlal durumunda Kişisel Verileri Koruma Kurumuna ve veri sahiplerine (*veri ihlalinin tespitinden itibaren 72 saat içinde*) söz konusu ihlali ve olası etkileri ile ilgili bildirimde bulunmak zorundadırlar.

Bildirimin zamanında gönderilebilmesi için yapılması gereken ayrıntılı eylemleri içerecek bir Olay Raporu Planı tasarlaması çok önemlidir. Plan, önceden belirlenmiş net bir dizi ardışık eylem ve bu eylemler için açık bir sorumluluk tahsisi ve bildirim şablonları, araştırma gereksinimleri, raporlama, medya ve iletişim yönetimi vb. İçermelidir. Noterler ve TNB'nin ayrıca ayrıntıları içeren bir olay günlüğü tutacak teknik altyapıyı da hazırlamalıdırlar.

Risk Değerlendirmesi

Gizlilik ve veri güvenliği alanında çok sayıda "risk" tanımı ve kavramı olmasına rağmen, KVKK/GDPR kapsamında sadece verileri işlenen kişiler için gündeme gelecek olan riske odaklanılmaktadır.

KVKK/GDPR düzenlemeleri, veri sorumlularının belirli proje ve faaliyetlerde bulunan riske uygun bir güvenlik düzeyi sağlamasını gerektirir. Noterlikler, kişisel verilere, özellikle de kişisel verilere yönelik riskleri azaltmak için uygun seviyede teknik ve idari önlemleri uygulamadan önce riski belirlemek için gerekli çalışmaları yapmalıdırlar.

Veri sorumluları karşılaşacakları tek riskin sistemlerine girmeye çalışan siber suçlular olduğunu düşünmemelidirler, kişisel verilerin kazara veya kasıtlı imha, kayıp veya ifşaya karşı savunmasız olduğunu da göz önünde bulundurmalıdır.

Kişisel Verilerin Güvenliğine Yönelik Teknik Önlemlerin Alınması

KVKK/GDPR düzenlemelerinin öngördüğü teknik ve idari önlemlerin alınması, idari ve hukuki önlemlerin tamamlayıcı ve zorunlu tamamlayıcısı durumundadır.

Bunun için var olan bir bilgi güvenliği politikalarına ek olarak kişisel verilerin korunmasına yönelik politika ve süreçlerin tanımlanması gerekmektedir.

Ayrıca, kişisel verilere erişim içim yetki matrisinin de hazırlanması, veri keşif ve kişisel verilerin sınıflandırılması ile veri korumaya yönelik şifreleme, anonimleştirme ve bulanıklaştırma (*pseudonymization*) tekniklerinin uygulaması, KVKK/GDPR uyumluluk sürecinin zorunlu parçalarıdır.

İzleme ve Raporlama

KVKK/GDPR düzenlemeleri gereğince Noterler ve TNB'nin gerektiğinde politikalarını ve prosedürlerini güncelleyerek, personelini ve mürettebatını eğitmeli ve gerekli resmi belgelerini ve anlaşmalarını güncelleyerek uyumluluklarını sürekli olarak izlemelidirler.

Ayrıca olası bir denetim için bu uyumluluk altyapılarını da gösterebilmelerinin en sağlıklı yolu da düzenli olarak ilgili raporların üretilmesi ve arşivlenmesidir.

Yönetişime Yönelik Bir Kültürün Geliştirilmesi

Noterlikler ve TNB'nin iç denetim ortamında kişisel verilerin korunmasına yönelik güvenlik tedbiri, etkili risk azaltma yöntemleri her zaman sonunda insanların bu önlemleri ne kadar iyi anladıkları ve uyguladıklarına bağlı olacaktır.

Noterliklerin kendilerini aktif olarak korumaları için yönetişim odaklı bir kültürün oluşturulması ve sürdürülmesi gerekmektedir. Bu kişisel verilerin saçılma tehditlerine karşı çok daha etkili bir kalkan oluşturur.

Noterlikler ve TNB'nin, gerçekten risk odaklı, etkili ve verimli bir şekilde uyumluluk çalışmaları ile hem uyumluluk maliyetlerini hem de olası riskleri ve etkilerini en aza indirgemelidirler.

5. Uyumluluk ve Denetim

Kişisel verilerin korunmasıyla tutarlı bir uygulama için tüm bu yapıları uçtan uca kapsayacak uygulama projesine gerek vardır. Bu, KVKK ve GDPR için uygulama projesinin tüm bileşenlerini kapsayan sürecin izlenmesi ve değerlendirilmesi için **tam bir çözüm** olmalıdır.

Bu nedenle; Kişisel Verilerin Korunmasına yönelik gerçekleştirilecek bir çalışmada hukuki, idari ve teknik olmak üzere üç farklı eksenli çalışmalarının bütünleşik olarak hep birlikte yapılması zorunludur.

5.1. Hukuki Çalışmalar

Hukuki değerlendirmeler;

- ✓ Aydınlatma ve açık rıza metinlerinin düzenlenmesi,
- ✓ Çalışanlar, tedarikçiler, müşteriler, işortakları ve benzeri 3. taraflarla düzenlenen sözleşmelerin gözden geçirilip KVKK /GDPR mevzuatına uyumlu hale getirilmeleri,
- ✓ Kişisel verilerle çalışan personel ile yine mevzuata uygun sözleşmelerin düzenlenmesi,
- ✓ Veri sahiplerinin KVKK/GDPR kapsamındaki taleplerinin incelenmesi ve değerlendirilmesi,
- ✓ KVKK/GDPR ilgili diğer konulardaki hukuki değerlendirmelerin yapılması konularını içerir.

5.2. İdari Çalışmalar

İdari değerlendirmeler;

- ✓ Veri koruma ve güvenlik politikalarının belirlenmesini,
- ✓ Risk yönetimini,
- ✓ Proje metodolojisini ve değişim/uyum sürecinin KVKK/GDPR düzenlemelerine göre yönetilmesini içerir.

Ayrıca,

- ✓ KVKK/GDPR mevzuatına göre kişisel verilerin korunmasına yönelik gerekli kurum içi organizasyonun oluşturulması,
- ✓ Görev ve sorumluluk matrisinin hazırlanması ve süreçlerin düzenlenmesi
- ✓ KVKK/GDPR kurumları ile iletişim ve başvurularda gerekli desteklerin sağlanması konularını da içerir.

Bu kapsamda yapılacak uyumluluk çalışmaları;

- ☑ KVKK Önleyici ve Düzeltici Danışmanlık
- ☑ Politikalar / Süreçler / Belgeler
- ☑ Gizlilik ve Mahremiyet Politikaları
- ☑ Veri Koruma Etki Analizi
- ☑ Eğitim

kapsamaktadır.

5.3. Teknik Çalışmalar

Müşteri verilerinin teknik kontrolü, uyumluluğunun anahtarıdır;

- ✔ Yapılandırılmış (*veritabanları*), yarı yapılandırılmış (*Excel vb.*) ve yapılandırılmamış (*dokümanlar, PDF vb.*) veri analizi uygulamaları,
- ✔ Kullanılan uygulamalar ve veri tabanları,
- ✔ Veri merkezi, güvenlik duvarı sistemi, veri depolama,
- ✔ Bulut servisi, e-posta hizmetleri ve güvenlik sistemlerini içerir.

Ancak tümü bunlarla sınırlı olmayıp, KVKK/GDPR zorunlu kıldığı analizlerin ve değerlendirmelerin yapılması ve Müşteri tarafından kullanılan diğer özel uygulamalar da bu sürece dâhil edilmektedir. *(Kişisel Veri Yönetişimi, Müşteri Talep Yönetimi, Şifreleme vb.)*

KVKK/GDPR Uyumluluk çözümünün ikinci aşaması, idari ve hukuki süreçlerin belirlenen tespitlerin gözden geçirilmesi ve tamamlanması ile tüm teknik altyapının uyum otomasyonunu sağlayarak ***bütünleşik çözümü*** gerçekleştirecek bir aşamadır. Bu teknik uygulama süreçlerini tamamlamak, düzenli ve sürekli bir süreç otomasyonu ile uyum için hazır hale gelinmesinin ön koşuludur. Bu kapsamda;

- ☑ Yapılandırılmış / Yapılandırılmamış Ortamlarda Veri Keşfi
- ☑ Veri Sınıflandırılması / Süreç Yönetimi / Veri Yönetişimi
- ☑ Şifrelendirme / Anonimleştirme / Silme / Yok Etme
- ☑ Veri Sahibi Talep Yönetimi
- ☑ Risk Yönetimi / Veri Koruma Etki Analizi
- ☑ Uyumluluk
- ☑ Denetim

çalışmaları "İkinci Aşamada" gerçekleştirilmesi gereken ve temel bir teknik altyapıyı gerektiren iş ve işlemlerdir.

Kişisel verileri korumanın ve korumada sürekliliğin sağlanması ancak uçtan-uca izleme ve denetleme olanağı sağlayan teknik bir çözüm ile mümkündür ve **bu da KVKK/GDPR uyumluluğunun gerçek anahtarıdır.**

■

ACCERT A.Ş.

ACCERT A.Ş. 2018 Yılında sadece Kişisel Verilerin Korunması ile ilgili çalışmalar yapmak için kurulmuştur.

Kurucuları: Bilişim Teknolojileri, Bilgi Güvenliği ve Regülasyon alanında 30 yılın üzerinde deneyimli uzman ve akademisyenlerden oluşmaktadır.

Vizyonu: Kişi, kurum ve kuruluşları ulusal ve uluslararası kişisel verilerin korunması süreçlerine hazırlamaktır.

Misyonu: Kişilerin gizlilik hakları ile meşru iş fırsatları arasında adil denge kurmak için en uygun çözümleri sunmaktır.

Kişisel Verilerin Korunması Kanunu (*KVKK*) ve Avrupa Veri Koruma Tüzüğü (*GDPR*) gereklilikleri ve yükümlülükleri ile kurum ve kişiler arasında adil denge kurmak için farkındalığı artırmak ve güven ortamının devamlılığını sağlamak amacıyla bütünsel çözümler sunmaktır.

ACCERT A.Ş. Vizyon ve Misyonuna bağlı olarak konusunda uzman ulusal ve uluslararası kuruluşlar ile işbirliği yaparak kişisel verilerin korunması konusunda çözüm sunma çalışmalarını ilerletmiştir.

KVKK ve GDPR düzenlemelerine yönelik uyumluluk çalışmalarında danışmanlık, denetim ve eğitim hizmetleri sunmaktadır.

Bugün iş ortakları ile bu alanda uçtan uca çözüm sunabilen Türkiye'deki öncü kuruluşlardan biridir .

ACCERT Sertifikasyon, Belgelendirme, Danışmanlık, Eğitim ve Denetim A.Ş.

Uğur Mumcu'nun Sokağı No:39/7
Büyükesat Mahallesi, Çankaya / Ankara

Telefon : + 90 (312) 436 41 93
E-Posta : accert@accert.com.tr

ISBN-978-605-06236-1-1

ACCERT