Üye Etkinliği: Kişisel Verilerin Korunması Kanunu Sivil Toplum Kuruluşlarını Nasıl Etkileyecek?

Toplantı Notları

5 Nisan 2018 tarihinde, Minerva Han'da düzenlenen "Kişisel Verilerin Korunması Kanunu Sivil Toplum Kuruluşlarını Nasıl Etkileyecek?" başlıklı TÜSEV üye etkinliğinde, konuşmacı olarak davet edilen Avukat Sadife Karataş Kural ve Avukat Gözde Aracı tarafından yapılan sunumlarda Kanun'un getirdiği yükümlülükler genel hatlarıyla ele alındı ve Kanun kapsamında, sivil toplum kuruluşlarını (STK) ilgilendiren konular, Kanundaki istisnalar ve kişisel verilerin hukuka uygun olarak işlenmesi konularına değinildi.

Avukat Sadife Karataş Kural sunumuna, isimden başlayarak, bireylere ait verilerin ne kadar önemli olduğunu belirterek başladı. Günümüzde ise, verilerimizin her yerde olduğunu, veri dolaşımının çok geniş olduğunu ve bunun kişisel alanı korumanın zorlaştırdığını açıkladı.

E-ticaret işlemlerini düzenleyen ticari elektronik ileti mevzuatının kişisel veriler mevzuatından farklı olduğuna değinen Kural, ticari elektronik iletilerinde posta, SMS, çağrı, faks gibi iletişim araçlarını kullanan özel sektör, kamu kurumu veya STK'ların, iletişime geçilen alıcının onayını almaları gerektiğini belirtti. E-posta, SMS, çağrı, faks gibi iletişim araçları yoluyla yapılan pazarlama, ya da kutlama ve temenni gibi içerik gönderimi yapan kuruluşların, gönderimlerinin alıcıdan alınan onaya uygun olmasına dikkat etmeleri gerektiğini söyledi ve bu mevzuat kapsamında alıcının herhangi bir neden göstermeden ticari elektronik almayı reddedebileceğini, bunu göz ardı eden kurum ve kuruluşların idari para cezasına tabi tutulacağını ekledi.

Sunumuna sosyal medya gibi mecralar aracılığıyla kolaylaşan serbest veri dolaşımına değinerek devam eden Kural, konunun Facebook'un kullanıcılardan elde ettiği verileri kullanması sebebiyle Amerikan başkanlık seçimlerinin manipüle edildiği iddialarına kadar uzandığını hatırlattı. Kural, Facebook gibi sosyal mecralarda sadece beğenilerimizle bile kendimizle ilgili birçok veriyi sanal dünyaya aktardığımıza dikkat çekti ve Stanford Üniversitesi'nden Michal Kosinski isimli araştırmacının bir bireyin Facebook'taki 10 beğenisinin incelenmesiyle, bu kişinin ortalama iş arkadaşlarından daha iyi tanınabileceğini, 70 beğenisinin incelenmesiyle, bu kişinin arkadaşlarından daha iyi tanınabileceğini, 150 beğenisinin incelenmesiyle, beğeni sahibi kişinin ailesinden daha iyi tanınabileceğini konu alan çalışmasını referans gösterdi.

AVRUPA BİRLİĞİ'NDE (AB) KİŞİSEL VERİLERİN KORUNMASI

Kural, kişisel bilgilerin ve özel hayatın korunması kaygısıyla alakalı, 1970'lerden beri Almanya başta olmak üzere birçok Avrupa ülkesinde verilerin işlenmesine ilişkin kanunların yürürlüğe sokulduğunu aktardı ve Avrupa Birliği'nin kişisel verilerin korunması kapsamında attığı adımlara kısaca değindi. 1980'de Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından *Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri* çalışmasının yayımlanmasının ardından, 1981 tarihinde *Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin Sözleşme*'nin imzalandığını aktardı. Avrupa Birliği'nde mal ve hizmet dolaşımının serbestliğine verilen öneme değinen Kural, kişisel verilerin de bu kapsamda serbestçe dolaşabilmesi için, 1995

tarihli *Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif*'in yayımlandığını belirtti. Kural, AB tarafından bu konuda yapılan son düzenlemenin 2016 *Avrupa Birliği Genel Veri Koruma Düzenlemesi* olduğunu ve bununla Avrupa Birliği'nde yüksek veri koruma sistemini standartlaştırmak üzere yeknesak bir uygulamaya geçilmek üzere olduğunun altını çizdi.

AVRUPA BİRLİĞİ DÜZENLEMELERİ DAHİLİNDE ÖZEL NİTELİKLİ VERİLER, VAKIF VE DERNEK ÜYELİĞİ

Kural, bireylerin bilgilerinin kişisel veriler ve özel nitelikli (hassas) kişisel veriler olarak ikiye ayrıldığını, özel nitelikli verilerin sadece veri sahibinin açık rızası ile işlenebileceğini ve kurallar gereği bu nitelikteki verilerin daha sıkı güvenlik tedbirlerine tabi tutulduğunu belirtti. AB yasalarında, özel nitelikli kişisel verilerin; ırk, etnik köken, siyasi görüş, dini veya felsefi inanç, sağlık, cinsel yaşam, genetik, biyometrik veriler ve sendika üyeliği olarak tanındığını aktaran Kural, bahsi geçen konularda hassasiyet gösterilmesinin nedenini ayrımcılığın engellenmesi olarak açıkladı. Bu bilgilerin öğrenilmesinin bilgi sahibi kişinin mağduriyetine sebep olabileceğini ve bu nedenle, bu bilgilerin daha özenle korunmasının kanunlarca sağlandığını aktardı. Kural, Türkiye'de vakıf ve dernek üyeliğinin özel nitelikli veri olarak kabul edilirken, AB'de bu durumun söz konusu olmadığını, kanunların sadece sendika üyeliğini hassas veri olarak saydığını söyledi.

Kural, AB yasalarına göre özel nitelikli verinin işlenmesinin ancak veri sahibinin rızası, hayati çıkarlarının korunması, iş hukukundan kaynaklanan yükümlülüklerin yerine getirilmesi ve düzenlemede yer alan diğer spesifik durumlarda mümkün olduğuna değindi ve AB yasalarında sivil topluma tanınan bir istisnadan bahsetti. Bu istisnaya göre, STK'ların kendi üyelerinin veya STK'nın kuruluş amaçları ile ilgili olarak kendileriyle düzenli iletişime geçen kişilerin verilerini veri sahibinin açık rızası olmadan işleyebildiklerini aktardı.

Türkiye'de ise Kişisel Verilerin Korunması Kanununun Ocak 2016'daki yasa taslağında yer alan bir maddenin, siyasi parti, vakıf, dernek veya sendika gibi kâr amacı gütmeyen kuruluşların kuruluş amaçlarına ve tabi oldukları mevzuata uygun ve faaliyet alanlarıyla sınırlı bir şekilde, üçüncü kişilere açıklamamak kaydıyla, topladıkları kişisel verileri işleyebilmelerini mümkün kıldığını, ancak bilinmeyen bir nedenden dolayı bu maddenin devre dışı bırakıldığını anlatan Kural, AB entegrasyon süreçleri kapsamında bu düzenlemenin kanuna aktarılması konusunun sivil toplum kuruluşları tarafından gündeme getirilebileceğini belirtti.

KİŞİSEL VERİLERİN KORUNMASI KANUNU

Avukat Gözde Aracı sunumunda 6698 sayılı Kanunun amacı ve düzenlemeleri ile ilgili kapsamlı bilgi verdi. Kanunla, kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucunda kişisel hakların ihlal edilmesinin önüne geçilmesinin amaçlandığını belirten Aracı, Kanunun kişisel verilerin işlenmesine ilişkin kurallar ve bu kuralların uygulanmasını denetleyecek mekanizmalar getirdiğini belirtti. Kanunun yürürlüğe girmesiyle özel hayatın gizliliği hakkının, kişisel veri güvenliği hakkının ve kişisel verilerin işlenmesinde kişilik haklarının korunmasının amaçlandığını söyledi.

KANUNDA GEÇEN TEMEL KAVRAMLAR

Aracı, sunumunda Kanunda yer alan bazı temel kavramlara da yer verdi. ***Kişisel veri***yi 'Kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi' olarak açıklayan Aracı, kişinin kimlik bilgisi, sağlık ve eğitim durumu, başkaları ile yaptığı haberleşmeler, ikamet adresi, alışveriş alışkanlıkları; IP adresi gibi bilgilerin bir kişiyi diğer kişilerden ayırabilir nitelikte olduğunu, bu nedenle yasal çerçevede kişisel veri olarak kabul edilebileceğini anlattı. Bununla birlikte, özel nitelikli kişisel verilere de değinen Aracı, bu verilere siyasi düşünce, ırk, etnik köken, din, mezhep, dernek/vakıf/sendika üyeliği, ceza mahkumiyeti, biyometrik ve genetik bilgiler, kılık/kıyafet ve felsefi inanç gibi verilerin girdiğini aktardı. Aracı, Kanunun ***veri sahibi*** (ilgili kişi) terimini kişisel verisi işlenen gerçek kişi olarak tanımladığını, ***veri sorumlusu*** terimini ise verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak kabul ettiğini belirtti. Bununla birlikte, Kanunun ***veri işleyen*** terimini, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi tanımlamak amacıyla kullandığını anlattı.

Kişisel veri işleme kavramını da açıklayan Aracı, veri işlemenin, verilerin elde edilmesi, kaydedilmesi, muhafaza edilmesi, değiştirilmesi, düzenlenmesi, aktarılması, devralınması, sınıflandırması, silinmesi, yok edilmesi gibi veriler üzerinde gerçekleştirilen her tür eylem olarak kabul edildiğini söyledi.

Aracı, Kanunun tamamen veya kısmen otomatik yöntemlerle, hatta bir veri kayıt sistemi içerisinde olmak kaydıyla otomatik olmayan yöntemlerle işlenen kişisel verileri kapsadığını belirtti. Tüzel kişilere ait bilgilerin, örneğin; vakıfların veya derneklerin unvanlarının, vergi numaralarının, adreslerinin işlenmesinin Kanun'un kapsamına girmediğinin altını çizdi. Vakıfların ne tür verileri ne amaçla işlediği konusunu açan Aracı, örnek olarak vakıfların mevzuat gereği çalışan verilerini, gönüllülerin özgeçmişleri gibi kayıtlarını, bağışçı ve bursiyer bilgilerini, varsa ticari işletmelerden yapılan satışların kayıtlarını ve raporlarda yayımlanan kişisel bilgileri işliyor olabileceğini belirtti.

KANUN NELERİ DÜZENLİYOR?

Etkinlikte, kişisel verilerin hukuka uygun olarak işlenmesinin ve paylaşılmasının, gerekli süre boyunca veya mevzuatta belirtilen süre kadar güvenli bir şekilde saklanmasının ve sonrasında silinmesinin, veri sorumlularının Veri Sorumluları Siciline (VERBİS) kaydolmasının, veri sahiplerinin verileri ile ilgili taleplerinin cevaplanmasının, Kurul kararlarının yerine getirilmesinin ve ihlal halinde kurumların karşılaşacağı yaptırımların, Kanun kapsamında yapılan düzenlemeler arasında olduğu belirtildi.

Aracı, kişisel verilerin Kanun'da belirtilen genel ilkelere uygun olarak işlenmesi gerektiğini belirtti ve bunun için işlemenin dürüstlük kurallarına uygun olması, kişisel verilerin doğru ve güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendiği amaçla bağlantılı ve sınırlı olması ve ilgili mevzuatta öngörülen veya işlendiği amaç için gerekli olan süre kadar muhafaza edilmesi gerektiğinin altını çizdi. İleride ihtiyaç duyulacak amaçlar için veri toplanamayacağını söyleyen Aracı,

kişisel verilerin belirli bir amaç çerçevesinde gerekli ölçüde işlenip, işleme amacı son verildiğinde silinmesinin Kanunda temel olduğunu belirtti.

İŞLEME ŞARTLARI- AÇIK RIZA

Aracı, veri işleme şartlarında açık rızanın esas olduğunu belirtti. Veri sorumlularının alacakları açık rızaya ilişkin olarak, açık rızanın belirli bir konuya ilişkin olması, veri sahibinin işleme konusunda bilgilendirilmiş olması, akabinde veri sahibinin özgür iradesiyle rızasını açıklaması gerektiğini söyledi. Aracı 'özgür iradeyle açıklama' kavramının tartışmalara neden olduğunu, veri sahibi ile veri sorumlusu arasında hiyerarşik bir ilişki olması durumunda, veri sahibinin iradesinin özgürlüğünün tartışılabilir olduğunu belirtti.

AÇIK RIZA ALINMADAN KİŞİSEL VERİ İŞLENEBİLECEK ŞARTLAR

Kanun'da esas olarak, kişisel verinin sadece veri sahibinin açık rızası ile işlenebileceği düzenlenmiş olsa da, Kanun'da belirtilen veri işleme şartlarının olması halinde kişisel verilerin açık rıza alınmadan da işlenebileceği aktarıldı. Aracı: kanun hükmü gereği kişisel veri işlenmesinin zorunlu olduğu hallerde(ör. Çalışan özlük dosyaları), bir sözleşmenin kurulması/ifası dahilinde kişisel veri işlemenin zorunlu olduğu hallerde(bir ticari işlemde satın alınan ürünün teslimi için), fiili imkansızlık durumunda (ör. Bilinci kapalı bir kişinin, hayatını kurtarmak amacıyla), veri sorumlusunun hukuki sorumluluğunu yerine getirmesi durumunda (ör. Yönetim Kurulu üyelerinin Vakıflar Genel Müdürlüğüne bildirilmesi), kişisel verilerin aleni olması durumunda (verilerin sosyal medyadan kamuya açık bir şekilde yayımlaması halinde), bir hakkın tesisi, korunması ve kullanılması için veri işlemenin zorunlu olması durumunda (ör. Burs verilmesi) ve veri sahiplerinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaati söz konusu olduğunda (bir şirketin meşru menfaati için performans verilerini işlemesi) açık rıza alınmadan kişisel veri işlenebileceğini açıkladı.

ÖZEL NİTELİKLİ VERİLER

Her çeşit özel nitelikli verinin kural olarak sadece veri sahibinden açık rıza alınarak işlenebileceğini vurgulayan Aracı, sağlık ve cinsel hayat dışındaki özel nitelikli verilerin kanunlarda öngörülen hallerde açık rıza aranmaksızın işlenebileceğini; bir bireyin sağlık ve cinsel hayata ilişkin verilerinin ise kamu sağlığının korunması, tıbbi teşhis/tedavi, hizmet finansmanı amaçları ile sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar (hastane, sosyal sigorta gibi sağlık kuruluşları gibi) tarafından açık rıza aranmaksızın işlenebileceğine değindi.

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN YETERLİ ÖNLEMLER ALINARAK İŞLENMESİ

Kanun'da özel nitelikli kişisel verilerin işlenmesine oldukça hassas yaklaşıldığını aktaran Aracı, 31.01.18 tarihli *Özel Nitelikli Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemlere İlişkin Karar*'dan da bahsetti. Karar kapsamında her kuruluşun özel nitelikli verilerin işlenmesine ve güvenliğine yönelik politikalarını belirlemesinin gerekliliğini vurgulayan Aracı, karar kapsamında çalışanların bilgilendirilmesi, erişim yetkilerinin tanımlanması ve gizlilik sözleşmesi imzalanması, görevden ayrılan çalışanların bilgiye erişiminin kesilmesi, hassas verilerin şifrelenerek saklanması, verilerin ayrı depolarda tutulup güvenliğinin düzenli olarak test edilmesi, özel veriler

üzerinde yapılan işlemlerin kayıt altında tutulması ve özel nitelikli kişisel verilerin yer aldığı sistemlere erişimde en az iki kademeli kimlik doğrulama sistemlerinin geliştirilmesi vb. önlemlerin yer aldığını aktardı.

KİŞİSEL VERİLERİN ÜÇÜNCÜ KİŞİLERE AKTARILMASI

Aracı, kişisel verilerin veri sahiplerinin açık rızaları veya varsa Kanun'da yer alan veri işleme şartları dahilinde, özel nitelikli kişisel veriler için ise ayrıca yeterli önlemlerin alınması kaydıyla yurtiçinde üçüncü kişilere aktarılmasının mümkün olduğunu söyledi.

Aracı kişisel verilerin, veri sahibinin açık rızası olması veya varsa Kanun'da yer alan veri işleme şartları dahilinde yurt dışına aktarılabileceğini belirtti. Veri sahibinin açık rızası bulunuyorsa, kişisel verilerin herhangi bir ülkede yerleşik olan veri sorumlusu ile paylaşılabileceğini aktaran Aracı; veri sahibi açık rızasını beyan etmemişse, Kanunun 5/2 ve 6/3 maddelerindeki şartlar sağlanıyorsa veri aktarılacak ülkenin Kurul tarafından kabul edilen güvenli ülke listesine dahil olup olmadığının kontrol edilmesi gerektiğini anlattı. Eğer veri aktarılacak ülke Kurul tarafından ilan edilen güvenli ülkeler arasında ise verinin yurt dışına aktarılmasının uygun olduğunu ifade etti. İlgili ülke güvenli ülkeler listesinde yer almıyorsa, (Türkiye'deki) kişisel verileri aktaracak veri sorumlusunun ve verilerin aktarılacağı veri sorumlusunun yeterli korumayı sağlayacaklarına dair yazılı taahhüt vermesi gerektiğini ve bunun Kurul'un onayına sunulması gerektiğini söyledi. Kurul izni alındıktan sonra verinin yurt dışına aktarılabileceğini ifade etti. Ancak tüm şartlar sağlansa dahi (uluslararası sözleşme hükümleri saklı kalmak üzere) Kurul'un Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceğine kanaat getirdiği durumlarda, ilgili kamu kurum veya kuruluşunun görüşünü alarak yurt dışına veri aktarımını yasaklama yetkisinin de olduğunun altını çizdi.

Aracı, Kurul tarafından henüz bir güvenli ülkeler listesi yayımlanmadığını belirtti ve Avrupa Komisyonu tarafından güvenli olarak kabul edilen ülkelerin, Kurul tarafından da güvenli kabul edilebileceğini aktardı. Avrupa Komisyonu'nun veri paylaşımını güvenli gördüğü ülkeler listesinde Andora, Arjantin, Kanada, Faroe Adaları, Guernsey, İsrail, Man Adası, Jersey Adası, Yeni Zelanda, İsviçre, Uruguay ve ABD (Privacy Shield framework ile limitli) olduğu belirtildi.

VERİ SORUMLULARININ YÜKÜMLÜKÜKLERİ

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğe değinen Aracı, Kanun kapsamında veri sahibinin kişisel verilerin elde edilmesi sırasında: veri sorumlusu ve varsa veri temsilcisinin kimliği, verilerinin hangi amaçla işleneceği, bu verilerin kimlere aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve veri sahibinin hakları konularında bilgilendirilmesi gerektiğini belirtti. Bu yükümlülüğe uymama halinde uygulanabilecek idari para cezasının 5.000 TL ila 100.000 TL arasında olduğunu söyledi.

Veri sorumlusunun bir başka görevinin ise kişisel verilerin güvenliğini sağlamak olduğundan bahseden Aracı, Kanunun her veri sorumlusuna standart tedbirler dayatmadığını, veri sorumlusunun işlediği verileri ve herhangi bir güvenlik ihlali olması halinde doğabilecek riskleri değerlendirerek, kendi veri güvenliğini sağlamak için alınabilecek tedbirleri belirlemesi ve yürürlüğe

koyması gerektiğini belirtti. Bu süreçte, veri sorumlularının Kişisel Veri Güvenliği Rehberini baz alarak uygulayabileceği birçok idari ve teknik tedbir olduğunu açıkladı.

Aracı alınabilecek bazı idari tedbirlere, erişim, güvenlik, kullanım, saklama ve imha politikalarının belirlenmesi, çalışanların eğitilmesi, kurum içi denetimler gibi örneklerin girdiğini, teknik tedbirlere ise, siber güvenlik için belirli güvenlik yazılımları (şifreleme, sızma testi, saldırı önleme sistemleri) çalışanların gerekli olmayan verilere erişiminin kısıtlanması gibi örneklerin girdiğini belirtti (Detaylı bilgi için aşağıdaki tabloyu inceleyebilirsiniz).

İdari Tedbirler
Kişisel Veri İşleme Envanteri Hazırlanması
Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında)
Gizlilik Taahhütnameleri
Kurum İçi Periyodik ve/veya Rastgele Denetimler
Risk Analizleri
İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi)
Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.)
Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Tablo 4.2. İdari tedbirler

Teknik Tedbirler
Yetki Matrisi
Yetki Kontrol
Erişim Logları
Kullanıcı Hesap Yönetimi
Ağ Güvenliği
Uygulama Güvenliği
Şifreleme
Sızma Testi
Saldırı Tespit ve Önleme Sistemleri
Log Kayıtları
Veri Maskeleme
Veri Kaybı Önleme Yazılımları
Yedekleme
Güvenlik Duvarları
Güncel Anti-Virüs Sistemleri
Silme, Yok Etme veya Anonim Hale Getirme
Anahtar Yönetimi

Tablo 4.1. Teknik tedbirler

Aracı, bütün veri sorumlularının; gerekli güvenlik düzeyini temin etmek ve denetim yapmak, sır saklamak ve kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi durumunda hem veri sahibini hem de Kurul'u veri sızıntısıyla ilgili bilgilendirmekle yükümlü olduğunu, aykırı davranışlara15.000 ila 1.000.000 TL arasında idari para cezası verilebileceğini aktardı. Aynı zamanda, veri sorumlularının, veri işleyen tarafından gerekli güvenlik önlemlerinin alınması hususunda, veri işleyen ile birlikte müştereken sorumlu olduğu belirtildi.

Veri sorumlularının yerine getirmek zorunda olduğu bir başka görevin, kişisel verinin işlenmesini gerektiren sebeplerin ortadan kalkması halinde imha edilmesi olduğunu aktaran Aracı, bunun için Kanun tarafından tanınan üç yol olduğunu söyleyerek bunların, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi olduğunu aktardı. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi'nde de belirtildiği üzere, silme işlemini verilerin kayıtlı olduğu mecralardan ilgili kişiler tarafından geri getirilemeyecek şekilde silinmesi, yok etme işlemini verilerin kaydedildiği mecralardan kimse tarafından geri getirilemeyecek ve kullanılamayacak şekilde imha edilmesi olarak tanımlayan Aracı, verilerin anonim hale getirilmesini ise verilerin gerçek bir kişi ile ilişkilendirilemeyecek hale getirilmesi olduğunu aktardı.

Aracı, Kanunun veri sorumlularının Veri Sorumluları Siciline (VERBİS) kaydolması yükümlülüğünü getirdiğini, ancak bu sistemin henüz oluşturulmadığını belirtti. Bir veri sorumlusunun VERBİS' e kaydolmak için, önce kendi veri envanterini oluşturması gerektiğini, anlatan Aracı, veri saklama ve imha politikasının da belirlenmesi ve gerekli bilgilerin VERBİS'e kayıt olarak bildirilmesi gerektiğini

aktardı. VERBİS'e bildirim yapma yükümlülüğünden müstesna olacak veri sorumlularının da olacağını ancak bunun için kriterlerin henüz belirlenmediğini söyleyen Aracı, VERBİS' e kaydolma yükümlülüğünün ihlali halinde verilebilecek idari para cezasının 20.000 ila 1.000.000 TL arasında olduğunu belirtti.

Aracı, Kanunla veri sahiplerine çeşitli haklar tanındığını, bunların kişisel verilerin işlenmesi süreci ile ilgili bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, kişisel verilerde eksik veya yanlışlık olması durumunda düzeltilmesini talep etme, kişisel verilerinin paylaşıldığı kişiler hakkında bilgi edinme, verilerinin veri sorumlusu tarafından silinmesini isteme, düzeltme ve silme işlemlerinin verilerinin aktarıldığı üçüncü kişilere bildirilmesini talep etme, veri sahibinin kişisel verilerinin Kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme ve işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme olduğunu aktardı. Aracı, veri sorumlusunun yukarıda belirtilen hakların kullanımına ilişkin başvurulara cevap vermekle yükümlü olduğunun altını çizdi.

Kişinin başvurusunu önce veri sorumlusuna bildirmesi gerektiğini ve veri sorumlusunun başvuruyu cevaplandırmak için en fazla otuz günü olduğunu belirten Aracı, veri sorumlusunun gerekli açıklamayı yaparak talebi reddedebileceğini söyledi. Cevabın veri sahibini tatmin etmemesi, başvurunun reddedilmesi veya başvuruya süresi içerisinde cevap verilmemesi durumunda, veri sahibinin Kurul'a şikâyette bulunabileceğini, Kurul'dan altmış gün içerisinde cevap gelmezse başvurunun reddedilmiş sayılması gerektiğini anlattı. Herhangi bir ihlalin varlığının saptanması durumunda, Kurul'un kararı ilgililere tebliğ edeceğini ve veri sorumlusunun gereğini otuz gün içerinde yapması gerekeceğini aktardı. Aracı, Kurul'un şikâyet üzerine veya resen verebileceği kararları yerine getirmeyenler hakkında 25.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası öngörüldüğünü belirtti.

SUÇLAR

Sunumunda suçlara da değinen Aracı, kişisel verilerin hukuka aykırı kaydedilmesi durumunda kaydeden kişiye bir yıldan üç yıla kadar hapis cezası verilebileceğini, kişisel verileri paylaşma şartlarına aykırı olarak paylaşan veya ele geçiren kişiye ise iki yıldan dört yıla kadar hapis cezası verilebileceğini belirtti. Verileri sistem içerisinde Kanun gereği silmek veya yok etmekle yükümlü olan kişilerin, bu işlemi gerçekleştirmezlerse bir yıldan iki yıla kadar hapis cezası alabileceğini söyledi.

Aracı, Kanunun yayımlanmasından önce hukuka uygun olarak alınan veri sahibi rızalarının, bir yıl içinde aksine bir beyanda bulunulmaması halinde, 6698 no'lu Kanuna uygun kabul edileceğini bildirdi. 7 Nisan 2018 tarihi itibariyle geçmiş verilerin hukuka uygun hale getirilmesi için tanınan sürenin sona erdiğini belirtti.