KİŞİSEL VERİLER PLATFORMU ÇALIŞMA NOTLARI - 2

TARTIŞILAN KONULAR, TOPLANTI NOTLARI, TESPİT VE ÖNERİLER

Ocak – Haziran 2019

İçindekiler Tablosu

I. GİRİŞ

Kişisel verilerin korunması alanında multidisipliner fikri ve mesleki tartışma ortamı sağlamak, uygulamanın birlik ve doğruluk içinde gelişmesine katkıda bulunmak gibi amaçlarla kurulan ve Ocak 2018'den bu yana toplanan Kişisel Veriler Platformu, ikinci dönem çalışmalarını da Boğaziçi Üniversitesi Bilgi Sistemleri Uygulama ve Araştırma Merkezi ("ISRC") ve Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi'nin ("BUSİBER") destek ve katkılarıyla gerçekleştirmiştir.

Ocak – Haziran 2019 döneminde beş defa toplanan Platformda tutulan tutanaklardan derlenen Çalışma Notları – 2, toplantılarda yapılan tartışmaların özeti mahiyetindedir. Bu toplantıların amaçlarından birisi de kişisel veriler ile ilgili konulara farklı açılardan bakabilmek ve alanda çalışan hukukçulardan değişik fikirler alabilmek olduğundan, tartışma zenginliğini gösterebilmesi açısından üzerinde hemfikir olunmayan, ancak tartışılmasında fayda görülen konulara da notlarda yer verilmiştir. Konuların hangi tarihlerde tartışıldığına da yer verilmiştir. Zira ilgili tartışmaların tarihinden sonraki tarihlerde Kurum ve Kurul'un açıklama yaptığı konular mevcuttur.

II. TARTIŞILAN KONULAR

Ocak – Haziran 2019 döneminde gerçekleştirilen Platform toplantılarında aşağıdaki konular, KVKK, ikincil mevzuat, Kişisel Verilerin Korunması Kurumu ("Kurum") Kılavuzları ile Kişisel Verilerin Korunması Kurulu ("Kurul") Kararları ekseninde, yeri geldikçe Avrupa Genel Veri Koruma Tüzüğü ve uygulaması da dikkate alınarak tartışılmıştır.

1. **KVKK ve GDPR kapsamında "Unutulma Hakkı" / "Rigth to be Forgotten"**
2. Veri Kayıt Sistemi (cep telefonları ve bilgisayarların veri kayıt sistemi olma noktasında değerlendirilmesi ve sahipleri açısından veri sorumlusu olma durumunun tartışılması)
3. **Veri Sorumlulukları Sicili'ne ("VERBİS") kayıtta muafiyet şartları ve uygulamaya dair tespitler**

4. **"**Mülkilik İlkesi", KVKK'nın uygulama alanı ve GDPR ile karşılaştırılması
5. **KVKK karşısında grup şirketlerinin ve merkezi yurtdışında olup da Türkiye'de sadece şubesi veya irtibat bürosu olan şirketlerin durumu; *Veri Sorumlusunun kim olacağı meselesi***
6. KVKK'da değişiklik önerileri; *mevcut maddelere değişiklikler ile yeni madde önerileri*
7. **Saklama sürelerinin tespiti meselesi, uygulamaya yönelik öneriler**
8. Kurul Kararı ışığında veri ihlal bildirimleri
9. **Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ ve Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi ışığında uygulama ve güncel tespitler**
10. Yabancı veri sorumluları (özellikle GDPR'a tabi olanlar) açısından aydınlatma yükümlülüğü; *kanunlar ihtilafı sorunu olup olmadığı*
11. **Grup şirkleti açısından aydınlatma yükümlülüğü ve uygulamadaki tespitler**
12. Saklama süreleri ve kişisel veri işleme envanterinin düzenlenmesi
13. **Kurul Kararlarına dair değerlendirmeler; *Facebook kararı, yeterli koruma bulunan ülkelerin tayini, vb.***

III. TARTIŞILAN KONULARA DAİR NOTLAR, TESPİT VE ÖNERİLER

1. KVKK ve GDPR Kapsamında "Unutulma Hakkı" / "Rigth To Be Forgotten"

Konu 18 Ocak 2019 tarihli Platform toplantısında ele alınmıştır.

Platformda konu hakkındaki tartışmalara *unutulma hakkının* öneminden bahsedilerek ve unutulma hakkı ile silme yükümlülüğü kavramlarına özellikle Avrupa Genel Veri Koruma Tüzüğü ("GDPR") çerçevesinden yaklaşmanın yerinde olacağı belirtilerek başlanmıştır.

Kişilerin, kendilerine ait/dair verilerin toplum hafızasından kaldırılmasını talep etmesi demek olan unutulma hakkının bir kişilik hakkı olarak yorumlandığında kapsamının genişlediği ifade edilmiştir. Bu durumda, talebe cevap verildiğinde, silmenin yalnızca dijital ortamlardan

silmekten mi ibaret olacağı, yoksa **Yargıtay HGK 2015/1679 karar sayılı kararındaki** gibi fiziksel imhanın da gerekip gerekmeyeceği tartışılmış, bu bağlamda ikincil mevzuata duyulan ihtiyaçtan bahsedilmiştir. Unutulma hakkının tanımı, kapsamı, söz konusu talebe karşı yükümlülüklerin sınırı, silme yükümlülüğü ile olan ilişkisi ve fiiliyatta talebin nasıl karşılanacağının ikincil mevzuat ile düzenlenmesine ihtiyaç bulunmaktadır.

Unutulma hakkı kavramının, özellikle Avrupa Birliği Adalet Divanının ("ABAD") "Google" kararından sonra gündeme geldiği belirtilmiştir. ABAD'ın ilgili kararının da hukuki gerekçelendirme bakımından çok tartışıldığı, kararda esasen unutulma hakkından değil silme yükümlülüğünden bahsedildiği ve 2014'te bu karar verildiği zaman GDPR'ın yürürlükte olmadığından söz edilmiştir. ABAD'ın bu önemli kararı aslında arama motorlarına yönelmiş bir karardır ve sektör açısından da bir dönüm noktasıdır. Konu bu bağlamda tartışılırken Platformda ilgili kararın bugün gördüğümüz veri koruma dalgasının kırılma noktası olduğundan bahsedilmiştir.

Türkiye açısından, Avrupa Birliğine benzer bir sistemin uygulanma olasılığının yüksek olduğu, erişimin engellenmesinin bir taraftan temel haklar açısından sıkıntılı bir konu olduğu ve erişimin engellenmesi ile arama sonuçlarından çıkarmanın tam olarak aynı şey olmadığı, dolayısıyla, GDPR'a paralel bir düzenleme ile uygulamanın şekillenebileceği belirtilmiştir.

Konu kapsamında "*right to delisting"* tartışması da yapılmıştır. Bazı akademisyenlerin görüşüne göre, bu aslında unutulma değil, listeden çıkartılmadır. Örneğin, Google arama motoru üzerinden yapılan aramalarda ilk sayfa çıkan sonuçlardan sonrasına neredeyse kimsenin bakmadığı, ancak kapsamlı araştırma yapmak isteyen bir kişinin, örneğin bir gazeteci, bunu o arama motorundan değil de başka yerden araştırdığında bilgiye ulaşabildiği söylenmiştir. Dolayısıyla, *right to delisting* ile bilgi edinme hakkı kullanmaya devam edilirken, ilgili kişiyi karalama tehlikesinin de bir parça engellediği belirtilmiştir.

Unutulma hakkı başlığı altında tartışılan birtakım kavramların esasen birbirlerinden farklı kavramlar olduğunun, unutulma hakkı ile kastedilenin netleştirilmesinin ayrı bir sorun olduğunun altı çizilmiştir. Bu doğrultuda medeni hukuk alanından bir değerlendirme yapılmış ve unutulma hakkının aslında kişinin kendi geleceğini (self-determinasyon hakkı) belirleme hakkına dayandığı vurgulanmıştır. Silmede ise, hukuka aykırı olarak işlenmiş bir veri varsa, bunun zaten hukuka aykırı olduğu için silinebileceği, ama unutulma hakkında kişinin

kendisinin paylaşmış olduğu bir verinin de kişinin talebi üzerine silinmesi gerekeceği söylenmiştir. Kavrama, Medeni Kanunda yeri olan iyi niyetin korunması üzerinden de yaklaşılabileceği, dolayısıyla, zamana bağlı olarak verinin yıllanması, işleme amacının ortadan kalkması, o insanın artık farklı bir kişi olması gibi durumların da önemli olacağı belirtilmiştir.

Anayada Mahkemesinin suçlara ilişkin haberlerin silinmesine dair bireysel başvurular aldığı ve konu hakkında yaklaşık altı kararının bulunduğu söylenmiştir.

Bunlarla birlikte, unutulma hakkının, arşivi değiştirerek, tarihi tekrar yazma gibi bir olumsuzluğa hizmet edip etmeyeceği tartışmalarının da var olduğundan bahsedilmiştir. Hakkın kullanım alanının sadece arama motorlarından ibaret olmadığı, Youtube, Facebook, Twitter gibi sosyal medyayı da kapsayacağı ifade edilmiştir.

Hukuka aykırı olarak işlenen verilerin silinmesinin zaten bir hak olduğu belirtilmiş, bu bağlamda Avrupa Birliği'nde de kavram karmaşası olduğundan bahsedilmiştir. Örnek olarak, GDPR madde 17'de hukuka aykırı verilerin silinmesinden bahsedildiği ama parantez içinde *right to be forgotten* yazıldığı, ancak kişiye ait verinin en baştan işlenmemesi gerekiyorsa zaten silmeye gidileceği, oysa ki unutulma hakkının kapsamında, başta meşru amaçlarla işlenen verilerin de olduğu belirtilmiştir.

Unutulma hakkının, çoğu kez kişinin özel hayatı ile ilgili olduğu ve kişinin hayatını kaygısız bir biçimde devam ettirebilmesi için ne gerekliyse onun yapılması anlamına geldiği ifade edilmiştir. Tabii bu durumda birtakım temel haklar arasıda menfaat çatışmasının doğması kaçınılmaz olabilecektir. Nitekim söz konusu kişilik hakkının karşısına fikir hürriyeti, basın hürriyeti gibi haklar çıkabilecektir. Bu durumda yapılması gerekenin vaka bazında makul bir denge sağlamak olduğu söylenmiş ve tartışma kapsamında Yargıtay GK 2015/1679 sayılı kararından tekrar bahsedilmiştir. Zira bu karar ile dijital hafızayı silmenin ötesine geçilerek, söz konusu kitabın fiziken de imha edilmesine karar verilmek suretiyle kişilik hakkının, bilim özgürlüğünün üstünde tutulduğu belirtilmiştir.

Fransız veri otoritesi CNIL'in unutulma hakkına dair güzel kararları olduğundan bahsedilmiştir. İlgili kişinin başvurusu üzerine, kişinin bilgilerini tüm dünyadan silmek yerine, Google'ın taraftarı olduğu gibi geo-blocking yani siteye hangi coğrafyadan ulaşılıyorsa, ona engel olmak yeterli olacaktır. Son olarak 10 Ocak 2019 tarihinde son

savunmalar alındığında General Attorney'nin de, dünya çapında verilerin silinmesinin talep edilemeyeceği, nitekim 3. ülkelerde bir menfaat testi yapılamayacağı ve AB dışındaki kişilerin bu verilere ulaşım hakkının ellerinden alınamayacağı görüşünde olduğu söylenmiş, silme ile unutulmanın ayrı işlevleri olduğu belirtilmiştir.

Konu hakında, Ditto M. Schoreneberger; "the virtue of forgetting in the digital age" isimli kitabı önerilmiştir.

Öte yandan tartışmalar arasında, konuya dair yaptırımların uygulanması üzerine değerlendirmeler de yapılmıştır. Mahkemelerin erişime engelleme kararına rağmen, ilgili medya kuruluşunun kararı uygulamadığı, içeriği kaldırmadığı vakalar olduğu, bunun devamında tazminat davasına gidilebileceği söylenmiştir. Son zamanlarda sulh ceza hakimliklerinde basın özgürlüğüne daha fazla önem verilmeye başlandığı belirtilmiştir. Yaptırımlarla ilgili olarak, içeriğin kaldırılması veya erişimin engellenmesi yerine, Anayasa Mahkemesinin kararında (2013/5653) bahsedildiği gibi *anonimleştirmenin* aslında basın özgürlüğünün de zedelenmemesi için daha iyi bir çözüm olabileceği görüşü verenler olmuştur.

Tartışmalar boyunca, unutulma hakkının küresel düzeyde düzenlenmesinin, bir başka deyişle ülkelerin ve bölgelerin aynı veya benzer usul ve esaslarla düzenlemeler yapmasının varılmak istenen sonuç ve amaç için gerekli olacağı birkaç kez vurgulanmıştır.

Silme talebinin muhatabının veri sorumlusu olduğu, unutulma hakkını kullanmanın şartlar ve koşullar itibariyle silmeden daha zor olması gerektiğini ileri süren katılımcılar olmuştur. Yürürlükte olan KVKK'da unutulma hakkına dair bir düzenleme olmaması nedeniyle yoruma dayalı işlem yapılmasının ve yaptırım uygulanmasının doğru olmayacağının, dolayısıyla bu konuda ikincil mevzuata duyulan ihtiyacın altı bir kez daha çizilmiştir.

Veri işleme faaliyetinin 28. Maddedeki istisnalara girdiği hallerde, kanunun kapsamı dışına çıkacağı ve bu durumda Kurum'un yaptırım yetkisinin de olmayacağı görüşleri paylaşılmıştır. Ayrıca, KVKK madde 28/2'deki istisnalar nedeniyle, ilgili kişinin 11. maddedeki haklarını kullanamama riski yönünden de değerlendirme yapılmıştır. Alenileştirmenin hangi durumlarda bu istisnaya girdiğinin belirlenmesinin gerektiği ve alenileştirme istisnalarının sadece alenileştirme amacı ile bağdaştırılması gerektiği belirtilmiştir. Alenileştirme ile ilgili

amaca bağlılık sınırlamasının yıllardır tartışıldığı, aslında bunun alenileştirmenin amacı dışında başkaca kriterler ile de desteklenmesi gerektiği (işleme türü, verinin niteliği gibi) ifade edilmiştir.

ABAD'ın, silme hakkına dair hükme dayanarak unutulma hakkı kararı verdiği hatırlatsa da, bu durumun unutulma hakkı üzerine ayrı bir düzenleme yapılması gerekliliğini ortadan kaldırmadığının altı çizilmiştir.

Platform, silme ve unutulma haklarına dair Kurum'un BTK ile nasıl bir işbirliği içinde olduğunu ve konuya dair birlikte ne tür çalışmalar yaptıklarının veya yapabileceklerinin kendilerine sorulabileceğini düşünmüştür. Diğer taraftan, uluslararası ilişkiler açısından da bu konunun önemli olduğu belirtilmiş, örneğin dışarıda host edilen bir verinin silinmesi talep edildiğinde, Kurul kararıyla bir yurtdışı otoriteye gidilmesi gerekeceği, dolayısıyla Kurul'un, belirli alanlarda yurt dışındaki otoriteler ile ortaklıklar geliştirmesinin gerekli ve faydalı olacağı belirtilmiştir.

2. Veri Kayıt Sistemi (Cep Telefonları ve Bilgisayarların Veri Kayıt Sistemi Olma Noktasında Değerlendirilmesi ve Sahipleri Açısından Veri Sorumlusu Olma Durumunun Tartışılması)

Konu 18 Ocak 2019 tarihli Platform toplantısında ele alınmıştır.

Platformda konu hakkındaki tartışmalara, veri kayıt sisteminin tanımı ile başlanmıştır. Kişisel veri olarak nitelendirilen verilerin esasen veri sorumlusu ile paylaşıldığı, veri sorumlusunun kendi bünyesinde istihdam ettiği veya farklı sıfatlarla çalıştırdığı kişilerin bu verilere erişiminden ve verileri işlemesinden de sorumlu oldukları, dolayısıyla hepsinin veri kayıt sisteminin parçası olduğu ifade edilmiştir.

Bu bağlamda, veri sorumlusu olan tüzel kişi ile iş ilişkisi içinde olan çalışanların GDPR uyarınca ayrıca "veri işleyen" olarak değerlendirilmedikleri, veri işleme amaçlarını bizzat kendileri belirlemedikçe ve dolayısıyla çalışanların şahsi kullanımında olan cep telefonlarının da veri kayıt sisteminin birer parçası olarak kabul edilemeleri gerektiği belirtilmiştir. Konunun tartışmalı alanlardan biri olduğunun da altı çizilmiştir.

Gerek kişisel bilgisayarlar gerekse cep telefonları kendi işletim sistemlerine sahip olan ve veri girişi yapılabilen cihazlardır, bu meyanda bir uyum sürecinde bu cihazlarda kayıtlı olan kişisel verilerin de tespit edilmesi sağlıklı olacaktır.

Aslında hem KVKK hem de diğer mevzuatın, kişisel verilerin korunması kapsamına sadece dijital ortamdaki kayıtlar değil fiziksel ortamda tutulan kayıtları da dahil ettiği belirtilerek, şahsi alanlarda örneğin evdeki fiziki dolaplarda tutulan kayıtların veri kayıt sisteminin bir parçası olup olmadığı değerlendirmesi yapılırken, bunların ABC gibi bir algoritmaya bağlanıp bağlanmadığına bakılması gerekeceği söylenmiştir. Yasa hükmüde "otomatik" şeklinde kullanılan ifadenin, 1981 sayılı Sözleşmede yer alan "automated" kelimesinden kaynaklandığı da ve "Atomated decision making" kavramı ile pek bir alakası olmadığı da eklenmiştir.

Eski teknolojilerin de, yeni teknolojilerin de birer veri kayıt sistemi olduğu, nitekim veri kayıt sistemi ifadesinin nedeninin, teknolojik gelişmeler karşısında kapsayıcı bir terminoloji getirmek olduğu, dolayısıyla belirli bir sistematik dahilinde verilerin tutulduğu her yerin, veri kayıt sistemi olarak kabul edilmesi gerekeceği ifade edilmiştir.

Bu başlık altındaki tartışmalar esnasında ileri tarihli bir Platform toplantısında, yapay zekanın büyük veriyi kullanmasının ve büyük veri analizlerinin taşıdığı risklerin tartışılmasının da faydalı olacağına dair fikir bildirilmiştir.

Elimizde bir veri kayıt sistemi varsa bunun sorumlusunun kim olduğu veya olması gerektiği hususu tartışılmıştır. Örneğin, şirketlerdeki "bring your own device" politikalarında bu tartışma kaçınılmaz olacaktır. Öte yandan, cep telefonlarının çoğunun artık akıllı telefon olduğu ve eski yazılımlar gibi çalışmadıkları, sıklıkla bulut bilişim ile depolama yaptıkları, kullanıcıların ise bu sistemleri kontrol edebilecek düzeyde sofistike bilgi sahibi olmadıkları, konuya bu açıdan bakıldığında örneğin Apple'ın veri sorumlusu olup olmayacağı da sorgulanmıştır.

İşleme yöntem ve amacını belirleyen kişinin veri sorumlusu olduğu, dolayısıyla bir şahsın telefon numarasının çalışanın kullandığı telefona kaydedilmesinin neden ve amacını kimin belirlediğinden yola çıkarak değerlendirme yapılmasının doğru olacağı, bu durumda cep telefonlarının veri kayıt sisteminin bir parçası olarak kabul edilebilecekleri görüşleri iletilmiştir.

Çalışanların kullanımında olan bilgisayarların çoğunlukla veri sorumlusu şirkete ait olduğu belirtilmiştir. Bu nedenle, gelen bir elektronik postanın bilgisayara indirilip, daha sonra farklı bir noktada saklanabileceği, dolayısıyla ilgili kişiden gelecek bir silme talebi karşısında veri sorumlusunun bu tür kayıtlardan da haberdar olması gerekeceği söylenmiştir. Bu durumda veri sorumlusu şirketlerin, çalışanların bilgisayarları üzerinde denetim yaptırmalarında haklı ve meşru menfaatleri olduğu söylenebilecektir.

Benzer bağlamlardan büyük veri sorumlularının, tahsis ettikleri cihazlar üzerinden çalışanlarının Whatsapp ve Snapchat gibi uygulamaları kullanmalarını yasaklamaya başladıkları iletilmiştir.

Bu konuda "amaç" unsuru çerçevesinde bir değerlendirme yapılmasının gerekli ve faydalı olacağı, ancak salt yasanın lafzından yola çıkılacak olursa, çalışanların dahi veri sorumlusu olarak niteledirilmesinin söz konusu olabileceği belirtilmiştir. Netleştirilmesi gereken başlıklardan biri olarak kayda alınmıştır.

3. Veri Sorumluluları Sicili'ne ("Verbis") Kayıtta Muafiyet Şartları ve Uygulamaya Dair Tespitler

Konu 18 Ocak 2019 tarihli Platform toplantısında ele alınmıştır.

VERBİS'e kayıt muafiyetleri hakkında yabancı veri sorumluları yönünden bir değerlendirme ile tartışmalar başlamış, yabancı veri sorumlularının muafiyetler kapsamında belirtilen kriterlerden ari tutulduğu ve VERBİS'e kayıt olmaları gerektiği sonucuna varıldığı söylenmiştir. Ayrıca, bilanço büyüklüğü konusunda tartışılması gereken noktalar olduğu, dernek ve vakıfların istisnaları açısından ise uygulamanın tam olarak nasıl işleyeceğinin düşünülmesinde fayda olacağı ve avukatlara getirilen istisna hakkında da farklı yorumlar olduğu belirtilmiştir.

Şirketler hakkında getirilen, "çalışan sayısı 50'den az ve mali bilanço toplamı 25 milyon TL'den az olanlar" istisnasında, bilanço büyüklüğünden, aktif pasif büyüklüğünün toplamı anlaşılmaktadır. Bu doğrultuda, özellikle grup şirketlerinde bazı şirketlerin sadece belirli

malvarlıklarına sahip oldukları ve aktif ticaret ve/veya çalışanları olmadığı halde, bilanço büyüklüğü nedeniyle muafiyet kapsamına girmeyecekleri söylenmiştir. Bu durumdan hareketle şu soruyu sormak gerektiği ifade edilmiştir; veri işleme ile mali bilançonun arasındaki ilişki nedir?

Derneklerin VERBİS'e kayıt istisnası kapsamında oldukları, fakat bir yandan iktisadi işletmeleri olan ve ciddi paralar kazanan derneklerin olduğu gündeme getirildiğinde, iktisadi işletmelerin VERBİS'e kayıt yükümlülüğüne tabi olacağına dair Kurumun bir değerlendirmesinin olduğu söylenmiştir. Ayrıca DERBIS'ten (Dernekler Bilgi Sistemi) bahsedilerek, sisteme her üyenin verisinin girildiği, verilerin arasında özel nitelikli kişisel verilerin de bulunduğu, bu sebeple konunun tartışılmasında fayda olacağı belirtilmiştir.

VERBİS'e kaydın amacı özellikle yoğun veri işleme faaliyetlerini gözden kaçırmayıp, aydınlatma metinlerinden, politiklara kadar kayıtların birbirleri ile uyumlu olup olmadığının kontrolü ise, belirlenen kriterlerin bu amaca tam olarak hizmet etmeyeceği, zira örneğin çoğu start-up'ın kapsam dışanda kalacağı vurgulanmıştır.

Öte yandan, zaman içinde işlemeyen veya ihtiyaç duyulan alanları fark etmesi ile birlikte Kurul'un istisna kriterlerini değiştirmesinin mümkün olabileceği ifade edilirken, kriterler yönünden olması gerekenin veri işleme yoğunluğuna dair kriterlerin belirlenmesi olduğu şeklinde fikirler de verilmiştir.

VERBİS'e kayıt istisnalarının geç yayımlandığı, esasen birçok şirketin, istisna kapsamında olup olmadığını bilmeden uyum çalışmaları yaptıkları söylenirken, istisnaların Kanun'un kapsamına girip girmemeye ilişkin olmaması nedeniyle, yapılan uyum çalışmalarının birçoğunun VERBİS'e kayıt istisnasında bağımsız olarak gerekli ve faydalı çalışmalar oldukları belirtilmiştir.

Saklama ve imhaya dair yönetmelikten de bahsedilerek, kişisel veri işleme envateri çıkartmanın veri sorumluları için VERBİS'e kayıt yükümlülüğünden bağımsız olarak gerekli olduğu, saklama ortam ve süreleri ile imha yöntemlerinin herhalde belirlenmesi için envantere ihtiyaç olduğu ve Kurum'un katıldığı birçok ortamda bu hususu anlattığı söylenmiştir.

Avukatlara ilişkin istisnadan da bahsedilmiştir. Avukatların istisna kriterlerden bağımsız olarak, VERBİS'e kayıttan istisna tutuldukları hatırlatılmıştır. Buna göre avukatın sadece kendi adına faaliyette bulunması durumunda bu istisnanın geçerli olacağı, ortaklık olarak faaliyet gösterilmesi durumunda ise veri sorumlusunun avukatlık ortaklığının kendisinin olacağı, bu durumda avukatlardan bağımsız olarak avukat ortaklığının veri sorumlusu sıfatı olacağı ve bu noktada çalışan sayısı kriterine bakılması gerekeceği iletilmiştir. Ancak, istisnanın kanundan kaynaklanan bir istisna olduğu ve dolayısıyla VERBİS'e kayıt yükümlülüğü kapsamında yapılacak bildirimlerde çalışanları açısından mı, yoksa tüm faaliyetleri açısından mı bildirim yapılacağında dair soru işaretlerinin doğduğu eklenmiştir. Söz alanların çoğu avukatlık faaliyeti dışında kalan hususlar için bir sorumluluk olduğunu beyan etmişlerdir.

Tartışmalar yoğunlukla yabancı veri sorumlularına ilişkin olarak devam etmiş, uç bir örnek olarak, ABD'de bir uygulama geliştiren şirketin uygulamasının Türkiye'de indirilip kullanıldığı noktada, Kurum'un bu durumda dahi ilgili ABD şirketini veri sorumlusu olarak gördüğü ve VERBİS'e kayıt olmasını beklediği yönünde bir bakış açısına sahip olabileceği paylaşılmıştır. Öte yandan istisnalar ise yabancı veri sorumlularına uygulanabilir değildir. Bu bakış açısından, Türkiye ile ilgili / Türkiye'den veri işleyen kişinin, veri sorumlusu olacağı ve bu bağlamda veriyi işlemeden önce VERBİS'e kayıt ile yükümlü olacağı yönünde bir sonucun kaçınılmaz olacağı, ancak bunun fiiliyatta yönetilmesinin zor bir durum olduğu tartışılmıştır. Diğer taraftan, konunun daha dar yorumlanmaya ihtiyacı olduğu ve Kurum ile görüşülmesi ve Kurum'dan yazılı görüş alınmasında fayda olduğu kanaati ön plana çıkmıştır. Zira bu bağlamda "mülkilik" gündeme gelmektedir. Öte yandan dijital işleme faaliyetlerinde verinin tam olarak nerede işlendiğinin tespitinin neredeyse imkânsızlığından da hareketle, mülkilik prensibi çerçevesinde GDPR düzenlemesine benzer bir yorumun yapılıp yapılamayacağı ve bunun Kurum ile görüşülmesi önerilmiştir.

Türkiye Cumhuriyeti sınırları içerisinde kalan herhangi bir veri işleme faaliyeti için mülkilik prensibi çerçevesinde TC kanunlarının zaten uygulanacağı, Türk Ceza Kanunu'nun (TCK) buradaki olası senaryoları düzenlediği, fakat diğerleri açısından MÖHUK'a gidilmesi gerekeceği, bu doğrultuda esas sorunun, Kişisel Verilerin Korunması Kanunun bir özel hukuk düzenlemesi olup olmadığı olduğu belirtilmiştir. Bu eksende yürütülecek tartışmalar yönünden Kanun'un esasen çok sınırlı kaldığı ve bazı hükümlerinin daha açık şekilde düzenlenmesine ihtiyaç olduğu ifade edilmiştir.

4. "Mülkilik İlkesi", KVKK'nın Uygulama Alanı ve GDPR ile Karşılaştırılması

Konu 15 Şubat 2019 tarihli Platform toplantısında ele alınmıştır.

Tartışmaların başında mülkiliğin tanımı ve KVKK'da coğrafi kapsama dair bir maddenin olmadığı maddesi hatırlatılmıştır.

Devamında Veri Sorumluları Sicili Hakkında Yönetmelik madde 5/1-b'den bahsedilmiştir. Bu madde uyarınca: *"Türkiye'de yerleşik olmayan veri sorumluları, veri işlemeye başlamadan önce veri sorumlusu temsilcisi marifetiyle Sicile kaydolmak zorundadır*." Bu madde her ne kadar kapsamı net olarak belirtmese de, konuya dair yorum yaparken yardımcı olacaktır, ancak herhalde konuya dair en faydalı çözüm KVKK'da bir kapsam maddesinin olmasıdır, zira Kanun'da bu hususa dair herhangi bir düzenleme yoktur.

GDPR'da ise konu hakkında açık bir düzenleme olarak "madde 3" vardır. Maddenin başlığı *"territorial scope"*. İlgili maddeye göre Avrupa Birliğine mal ve hizmet sağlamayı hedefleme, hedefleme yoksa bile cookieler veya çerezlere monitoring halinde bu faaliyetler ve dolayısıyla bu faaliyetlerin sahibi olan veri sorumlusu GDPR'a tabi olacaktır.

KVKK'nın mevcut halinde herhangi bir düzenleme olmaması, sadece dolaylı olarak bir coğrafi alan belirten yönetmelik maddesinin bulunması nedeniyle konunun genel kanunlardan yola çıkılarak yorumlanmasına geçilmiştir. Bu bağlamda, Kabahatler Kanununda yer bakımından TCK'nın 8. Maddesinin dikkate alındığı belirtilmiştir. TCK madde 8'e göre; *"Türkiye Cumhuriyeti içinde işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde ise suç, Türkiye'de işlenmiş sayılır."* Hareketin mi, neticenin mi, TC sınırları içinde gerçekleşmiş olması gerektiği konusunun tartışılmalı olduğu belirtilmiştir. Neticeye gitmeye gerek olmaksızın Türkiye'de veri toplanıyorsa, hareketin Türkiye'de gerçekleştiği kanısına varılacağı ifade edilmiştir. Şayet hareket Türkiye'de gerçekleşiyorsa, KVKK'nın uygulanacağı, daha önce bazı ortamlarda Kurum'un da bu konuyu bu şekilde yorumlama eğiliminde olduğu, belirtilmiştir.

Akabinde, Workin Party 29'un çıkardığı kılavuzdan bahsedilmiştir. Buna göre;

"A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market. The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR."

Bu örnekte hedefleme kriterinden yola çıkıldığı, hedefleme kriteri ile GDPR'ın uygulama alanının daraltılmış olduğu, bizde ise esasen tespit edilmiş bir kriter olmadığı için uygulama alanının daha geniş olduğuna dair bir sonucun çıktığının altı çizilmiştir. Plaform katılımcılarına konu hakkında görüşleri ve TCK hareket noktası olarak alındığında kural olarak bir zararın meydana gelmesi gerektiği, peki zarar ortaya çıkmadan Kurumun yetki alanının tanımının nasıl yapılacağı sorulmuştur. Bu noktada MÖHUK (Milletlerarası Özel Hukuk) madde 35'e atıf yapılmış ve orada da zarar koşulunun mevcut olduğuna değinilmiştir.

1. *"Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlâlinden doğan taleplere, zarar görenin seçimine göre;*

    a. *Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zarar görenin mutad meskeni hukuku,*
    b. *Zarar verenin işyeri veya mutad meskeninin bulunduğu ülke hukuku veya*
    c. *Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zararın meydana geldiği ülke hukuku, uygulanır.*

2. *Kişilik haklarının ihlâlinde cevap hakkı, süreli yayınlarda, münhasıran baskının yapıldığı ya da programın yayınlandığı ülke hukukuna tâbidir.*

3. *Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere de uygulanır."*

KVKK'da ihlalin dışında önleyici denetimlerin de düzenlendiği belirtilmiştir. Kurul'un herhangi bir zarar doğmamış olsa dahi, Türkiye'de veri işleme faaliyeti olan yabancı

şirketlerle ilgili denetleme, soru sorma yetkisi olup olmadığı ya da idari tedbir noksanlığı nedeniyle aksiyon alıp alamayacağı gündeme getirilerek, Facebook örneği verilmiştir. Facebook'taki veri sızmasından bahsedilmiş, Kurum'a Facebook tarafından henüz bir ihlal bildiriminin yapılmadığının altı çizilip, Kurum'un bir aksiyon alıp almayacağı sorulmuştur.

TCK'daki mülkilik prensibinin KVKK'ya kıyasen uygulanabilirliğinin tartışmalı olacağı, TCK'da kapsamın çok geniş tutulduğu, zira devletlerin temel mantığının bu yönde olduğu söylenmiştir. TCK'daki mülkiliğe dayanılırsa, Türkiye'de herhangi bir şekilde veri işlenmişse Kanun'un uygulanacağı ifade edilmiştir. Amerikalı bir turistin sadece Amerika için geçerli olan bir uygulamayı Antalya'da indirdiği zaman bu Türkiye'de meydana gelmiş bir netice olarak mı kabul edilecek, tartışılabileceği belirtilmiştir. Bu durumun tersinin de mümkün olacağı, örneğin bir TC vatandaşının yurtdışında bir uygulama indirme hali tartışılmıştır. Uygulamanın TC uygulamasıysa konunun tartışmalı olmayacağı, zira veri sorumlusunun TC kanunlarına göre kurulmuş ve Türkiye'de faaliyet gösteren bir kişi olması nedeniyle KVKK'nın uygulanacağı belirtilmiştir. TC vatandaşının bir yabancı uygulamayı Türkiye'de indirmesi halinde ne olacağı, yurtdışında indirmesi halinde ne olacağı üzerinden tartışılmış, veri sorumlusunun kim olduğundan bağımsız olarak kişinin temel hak ve özgürlüklerinin korunması bağlamında KVKK'nın uygulama alanı yurtdışını da kapsar mı konusunun önemli olabileceğinin altı çizilmiştir.

Öte yandan, kişisel verilere karşı işlenen suç ve kabahatlerde TCK veya Kabahatler Kanununun zarar şartını aramadığı, çünkü bu kapsamdaki suçların soyut tehlike suçu olduğu ifade edilmiştir.

Ceza Hukuku bakımından mülkiliğin mağdura göre esas alındığı, teorik olarak TCK özelinde düşünülecek olursa, yurtdışında indirilen uygulamaya da KVKK'nın uygulanmasının mümkün olacağı belirtilmiştir.

Tartışmalar kapsamında, kişisel verinin yurtdışına transferi, tazminat ve ceza gibi sonuçları hakkındaki bir görüş paylaşılmıştır. Bu görüşe göre kişisel veriler alanında ceza hukukunun mülkilik ilkesinin uygulanmasının doğru olmayacağı, zira verinin küresel dolaşımında bu sınırların uygulanabilir olmayacağı söylenmiştir. Öncelikle "erişimin" kontrol edilmesi gerektiği ifade edilmiştir. Teknik önlemelerle erişim sınırlandırılabililirse, ihlal riski azalacaktır.

Bazı katılımcılar tarafından KVKK'da "işleme" tanımının çok geniş olduğu ve bu tanımın daraltılmasına ihtiyaç olduğu belirtilmiştir.

Bu başlık altındaki tartışmalarda bulut depolama konusu da gündeme gelmiş ve veri sorumlusudan veri işleyene yapılan aktarımın aslında aktarım değil paylaşım olduğu, Kurum'un rehberinde de bulut depolama hizmeti veren şirketlerin veri işleyen olarak göz önünde bulundurulduğu halde, serverın yurtdışında olduğu durumlarda bu işlemin yurtdışına aktarım olarak kabul edildiği, halbuki bulut depolama şirketlerinin sadece server tuttuğu tekrar dile getirilmiştir. Kurum'un, veri işleyen yurtdışındaysa herhalde madde 9'u uygulamak istediği, zira verinin Türkiye'nin hakimiyetinden çıktığı düşüncesi ile hareket ediyor olabileceği söylenmiştir. Veriyi doğrudan/sadece yurtdışında tutmak yerine bir kopyasının Türkiye'de tutulmaya devam edilebileceği ifade edilmiştir.

Mülkilik ilkesi başlığında tekrar söz alan bir katılımcı, gerek KVKK gerekse diğer ülke mevzuatlarında da uygulama alanının dar tanımlanmasının daha doğru olacağı, zira her ülkenin farklı kuralları olabileceği için bir veri sorumlusunun her ülkenin kişisel verilerin korunmasına ilişkin kuralarını bilmesinin beklenemeyeceğini belirtmiştir.

KVKK'nın 5. ve 9. Maddeleriyle ilgili olarak, şayet son kullanıcı verisi işleniyorsa 5. Maddenin, başka bir veri sorumlusunun müşterinin verisi işleniyorsa 9. Maddenin dikkate alınacağı görüşü paylaşılmıştır.

Bu başlık altındaki tartışmaların genelinde, KVKK'da da "hedefleme" gibi bir kriterin benimsenebileceği ve kanuna bu yönde bir tanımın eklenebileceği, GDPR madde 3'ün örnek alınabileceği, esasen Kurum'un da GDPR'ı örnek alma eğiliminde olduğunun düşünüldüğü dile getirilmiştir. Ancak bu hususun bir mahkemenin önüne geldiğimde, savcı ve hakimlerin kanunun lafzından yola çıkarak, hedefleme kriterini dikkate almayabilecekleri, bu nedenle hedeflemeye yönelik bir değişikliğin kanuna işlenmesi gerektiği, Kurum'a da bu yönde görüş iletilmesi üzerinde durulmuştur.

Veri sorumlusundan veri işleyene olan veri transferinin bir aktarım değil paylaşım olarak kabul edilmekle birlikte, veri işleyen yurtdışındaysa eğer bu ayrıma gidilmeksizin veri aktarımı olarak ve KVKK madde 9 içinde değerlendirildiği, Kurum'un eğiliminin bu yönde

olduğu tekrar edilmiştir. Yurtdışındaki veri sorumlusu veriyi direkt ilgili kişiden alıyorsa, bir aktarım olup, olmadığı konusuna tekrar değinilmiş, Kurum'un bu işleme faaliyetinin bir aktarım olmadığı ve ilgili veri sorumlusunun VERBİS'e kaydının gerekli olduğunu düşündüğü dile getirilmiştir.

Türkiye'deki bir veri sorumlusunun yurtdışında bir sunucunun maliki olduğu örneğinde ise, aynı tüzel kişilik olduğu için bunun bir aktarım faaliyeti olarak değerlendirilmemesi yönünde görüşler bildirilmiştir.

Bu konu başlığı altındaki tartışmaların sonunda, KVKK'ya bir coğrafi alan tanımının eklenmesine ve GDPR'da olduğu gibi hedefleme gibi bir kriterle daraltmaya gidilmesine duyulan ihtiyaç Platformun ortak bakış olarak not alınmıştır.

5. KVKK Karşısında Grup Şirketlerinin ve Merkezi Yurtdışında olup da Türkiye'de Sadece Şubesi veya İrtibat Bürosu olan Şirketlerin Durumu; *Veri Sorumlusunun Kim Olacağı Meselesi*

Konu 15 Şubat 2019 tarihli Platform toplantısında ele alınmıştır.

Platformda konu hakkında tartışmalara mevzuatta *"Türkiye'de yerleşik olmayan veri sorumlusu"* kavramı hatırlatılarak başlanmıştır. Bu doğrultuda;

- Türkiye'de anonim veya limited şirket türünde iştiraki olan ve bu iştiraklerde hakim veya tam hakim durumda bulunan yabancı şirketlerin,
- Türkiye'de sadece şubesi veya irtibat bürosu olan yabancı şirketlerin,
- Türkiye'de herhangi bir kuruluşu olmaksızın Türkiye'den veri toplayan şirketlerin ayrı ayrı değerlendirilmesinin faydalı olacağının altı çizilmiştir.

Buna bağlı olarak, Türkiye sınırları içerisinde kişisel veri işleme faaliyetinin olması mı, yoksa Türk vatandaşlarının kişisel verilerinin işlenmesinin mi esas alındığı tartışması da gündeme getirilmiştir.

Türkiye'de anonim veya limited şirket türünden iştiraki olan bir yabancı şirketin, iştirakinin üzerindeki hakimiyet durumunun tam hakimiyet olup olmadığının, şube ve irtibat bürolarının ise iç ilişkideki bağımlılığı ve yasal zeminde tüzel kişi olarak kabul edilmemelerinin, konunun doğru tahlili açısından önemli hususlar oldukları belirtilmiştir. Her birinin ayrı ayrı ele alınması da gerekebilecektir. Bu noktada, 95/46 sayılı Direktif zamanında Hollanda veri koruma otoritesinin görüşünün sadece holdingin / hakim şirketin veri sorumlusu olması gerektiği yönünde olduğu, ancak bu görüşün kabul görmediği dile getirilmiştir.

Grup şirketlere dair bir değerlendirmede, mevzuattaki tanımlara bakıldığında her birinin ayrı ayrı veri sorumlusu olacakları söylenmiştir. İrtibat bürosu ve şubelerin durumundan bahsedildiğinde ise, mevzuatta gerçek veya "tüzel kişi" dendiği, oysaki şubelerin veya irtibat bürolarının tüzel kişiliği olmadığı belirtilmiştir. Diğer taraftan şube ve irtibat bürolarının tüzel kişiliği olmamasında hareketle, ana şirkete gidildiğinde, yükümlülüğün çok genişletilmiş olacağına değinilmiştir. Makul olan uygulamanın, kişilik tanımına bakılmaksızın, iş hukukunda davaya taraf olma ehliyetine benzer bir şekilde, Türkiye'deki şubenin veri sorumlusu olarak kabul edilmesinin olacağı görüşü paylaşılmıştır. Ancak irtibat bürosu yönünden konuya daha farklı yaklaşılabileceği, oradaki ilişkinin daha bağımlı bir ilişki olduğu, bu nedenle, yurt dışındaki şirketin her koşulda veri sorumlusu olarak kabul edilebileceği belirtilmiştir.

ABAD'ın unutulma hakkına ilişkin Google İspanya kararından bahsedilmiştir. Başvuru ve şikayetin Google İspanya'nın irtibat bürosu gibi bir biriminin üzerinden ilerlediği, usulen oraya başvurulduğu, ABAD'ın incelemesinde ise yaptırımı İspanya'daki birime değil Amerika'ya uyguladığı anlatılmıştır. Nedeninin İspanya'da yürütülen operasyonun Amerika tarafından kontrol edilen bir operasyon olduğu söylenmiştir.

Tartışmalarda, grup şirketlerle (hakim ve bağlı şirketlerin ilişkileri bakımından) şube ve irtibat bürolarının durumlarının birbirlerinden ayrı değerlendirilmesinin gerektiği sıklıkla belirtilmiştir. Türkiye'deki şubede çalışanların kişisel verilerini yurtdışındaki ana şirket işliyorsa ve yurtdışındaki ana şirket veri sorumlusu ise, bu bağlamda çalışan verilerinin aktarımının KVKK madde 9 kapsamında olup, olmayacağının da sorulması gerekeceğinden bahsedilmiştir.

Mevzuatta yapılacak tek bir değişikliğin bu konuyu çözemeyeceği; grup şirketlerin, şubelerin ve irtibat bürolarının ayrı düzenlemelere tabi olması gerektiği vurgulanmıştır. İrtibat büroları içinse yurtdışındaki şirketin şu anki düzenlemeler uyarınca veri sorumlusu olmasının kaçınılmaz gibi gözüktüğü belirtilmiştir. Böyle bir durumda, Türkiye'de şubesi olan yurtdışındaki neredeyse tüm şirketlerin VERBİS'e kayıt zorunluluğunun doğacağından bahsedildi.

Bu konu kapsamında VERBİS'e kayıt yükümlülüğü de tartışılmış, şube ve irtibat bürolarının sahibi olan şirketlerin VERBİS'e kaydolmaları gerektiği, ancak bu durumda muafiyet kriterlerinin şube ve irtibat bürosu üzerinden mi değerlendirilmesi gerekeceği sorgulanmış, yurtdışındaki veri sorumlusunun sicile kaydının zorunlu olduğu halde ciro ve çalışan sayısına bakılmayacağına dair görüşler bildirilmiştir.

Grup şirketlerinin Türkiye'deki iştiraklerinin kendilerinin birer veri sorumlusu olarak VERBİS'e kayıt olacakları, tam hakimiyet durumu için aktarımla ilgili istisnalar getirilebileceği, bunun pratik ve işleyiş yönünden faydalı olacağı ifade edilmiştir. Bununla birlikte, yurt dışına aktarılan kişisel verinin işleme amacı orada değiştiğinde, bir başka deyişle aktarılan veri başka bir amaçla işlenmeye başladığında, yurtdışı şirketinin de veri sorumlusu olarak kabul edileceği belirtilmiştir.

Öte yandan ana şirketi, veri sorumlusu olarak her bir ülkenin farklı kanununa tabi tutmanın ağır bir yükümlülük olacağı, menfaati sağlayan şirketin tespit edilip, onun veri sorumlusu addedilmesinin daha doğru olabileceğine de yer verilmiştir. Bugünün dünyasında, global grup şirketlerinin özelinde merkezi departmanlaşmanın engellenemeyen bir durum olduğu, bu nedenle her birine veri sorumlusu demenin pratiği zorlaştıracağı ve yükümlülüğü arttıracağı ifade edilmiştir.

Kurum nazarında hangi verinin VERBİS'te bulunmasının değerli olacağının tespit edilmesinin de önemli olacağı, zira global şirketlerin Türkiye'deki iştiraklerinde örneğin çalışanlarının verileri bakımından birincil veri sorumlusunun zaten o iştirakin kendisi olduğu, bu sebeple iştirakin VERBİS'e kaydından sonra ana şirketin de aynı kişisel veriler ve faaliyet amaçları üzerinden kaydedilmesinde herhangi bir menfaatin olmayacağı söylenmiştir.

Yabancı veri sorumlularının, veri sorumlusu olarak addedildiklerinde yükümlülüklerinin neler olacağı, tüm veri sorumlularının sicile kaydının zorunlu olup olmayacağı, örneğin aydınlatma yükümlülüğünün kimin tarafından yerine getirilmesi gerekeceği gibi konularda açık düzenlemelere ihtiyaç olduğu vurgulanmıştır.

6. KVKK'da Değişiklik Önerileri; *Mevcut Maddelere Değişiklikler ile Yeni Madde Önerileri*

Konu 15 Şubat 2019 tarihli Platform toplantısında ele alınmıştır.

Mevcut Maddelerde Değişiklik Önerileri	Yeni Madde Önerileri	Ceza Hukuku Açısından öneriler
Madde 3 (Tanımlar)	Çocukların Kişisel Verileri	Davranış normlarının alanının daraltılması
Madde 5 (Verilerin işlenmesi şartları) Madde 6 (Özel nitelikli kişisel verilerin işlenme şartları)	Müşterek veri sorumlusu kavramı	Özel nitelikli kişisel veriler açısından TCK ile uyum sağlanması
Madde 7 (Silme, yok etme veya anonim hale getirme)	Veri sorumlusu ile veri işleyen arasındaki sorumluluk rejimi	TCK m. 135, 136 ve 138'nın da şikâyete bağlı olacak şekilde yeniden düzenlenmesi
Madde 9 (Kişisel verilerin yurt dışına aktarılması)	Pseudonymisation (Takma Ad Kullanımı - Bulanıklaştırma)	KVKK-TCK arasından terminolojinin yeknesaklaştırılması
Madde 10 (Aydınlatma Yükümlülüğü)	Gizlilik ve mahremiyete saygılı olarak tasarım	KVKK Madde 28 (1) (ç) ile ilgili, kamunun kişisel verilerin korunmasına ilişkin hangi usul ve esaslara uyacağına ilişkin ayrı bir çerçeve yasa yapılması
Madde 11 (Otomatik sistemlerle analiz ile sonuçlar elde edilmesi ve profil çıkarma)	Veri Koruma Etki Değerlendirmesi	KVKK m. 17/2'deki düzenlemenin suçta ve cezada kanunilik ilkesine uygun hale getirilmesi

Madde 28 (İstisnalar)	Veri Koruma Görevlisi Zorunluluğu	
	Yargı Yolu	

Mevcut Maddeler Kapsamında Değişiklik Önerileri:

Madde 3 - Tanımlar:

Açık rıza tanımında değişikliğin şart olduğu vurgulanmıştır. TC Anayasası'nda *açık rıza* yazdığı, fakat rıza olarak ve GDPR'la uyumlu şekilde düzenlenmesine ihtiyaç olduğu belirtilmiştir. Kurum'un uygulamalarını GDPR ile benzer yürüterek, olası şikayetleri değerlendirirken bunu göz önünde bulundurma ihtimali olsa bile, konunun bir yargı boyutunun olduğu da unutulmamalıdır, olası bir yargılamada mahkeme mutlaka açık rıza arayacaktır.

Alenileştirmeyle ilgili olarak, veri işlemenin kişinin rızasına dayanmayan hallerde verinin alenileştirmesi vs. gibi detaylarının belirginleştirilmesine ihtiyaç olduğu, kanunda olmasa bile ikincil mevzuat ile hatta kılavuzlarla bu açıklamaların yapılabileceği belirtilmiştir.

KVKK'da *sağlık verisi* tanımının gerekliliği vurgulanmıştır. Bu noktada konu tekrar açık rıza meselesine gelmiştir. Kurum'un rehberlerinde olumlu irade beyanından bahsedildiği söylenmiş, bu bağlamda, *onaylayıcı eylemin* (affirmative action) kabul görüp, görmeyeceği sorulmuştur. Özellikle, örneğin sağlık verisi toplayan bir uygulamada, kişinin kendi isteğiyle ilettiği fotoğrafının onaylayıcı eylem olarak kabul edilip edilmeyeceği, gündeme getirilmiştir. Medeni hukuk perspektifinden onaylayıcı eylemin rıza olacağı, ancak açık rıza olarak kabul edilemeyeceği, KVKK'nın mevcut lafzında ve Anayasa'da açık rıza şeklinde yazılı olduğu için rıza olarak geniş bir tanımlama yapmanın bu halde mümkün olmayacağı ifade edilmiştir.

Maddeler 5 ve 6:

5/1 ve 5/2'nin ayrı ayrı yazılmayıp, madde 5'in GDPR'daki gibi tek bir madde olarak düzenlenmesi gerektiği belirtilmiştir. Zira bu haliyle açık rıza ile diğer hukuka uygunluk sebepleri arasında bir hiyerarşi varmış gibi okunduğu, oysaki fiili durumda hiyerarşi olmadığı, hatta Kurum'un kılavuzlarında da ve birçok yerde de madde 5/2'de sayılan hukuka uygunluk sebepleri varken, açık rıza alınmaması gerektiğini vurguladığı dile getirilmiştir. Aynı bakış açısıyla madde 6/2 ve 6/3'te tek bir madde olarak düzenlenebilecektir.

Madde 6 kapsamında, *çalışanların sağlık verisi* konusu gündeme gelmiştir. Madde 6/3'ten, mesleki sır saklama yükümlülüğü altında olma şartından bahsedilmiştir: *"Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir."* İnsan kaynakları birim çalışanlarına kısıtlı sayı ve erişim ile bu hususta bir esneklik tanımlanmasına ihtiyaç olduğu vurgulanmıştır. Örneğin, mesleki sır saklama yükümlülüğü olan kişinin talimatı ile insan kaynakları birim çalışanlarının kişisel verileri işleyebileceği şeklinde bir istisna yaratılabileceği yönündeki fikirler paylaşılmıştır.

Pratikte madde 6 kapsamında, özellikle sağlık verileri yönünden yaşanan zorlukların giderilebilmesi amacıyla, GDPR'daki sağlık verilerinin işlenmesiyle ilgili istisnaların ve ilave hukuka uygunluk sebeplerinin benimsenmesinin gerekli olduğu belirtilmiştir.

Sır saklama yükümlülüğü, sigortacılık sektörü açısından değerlendirilmiş, bu konuda neden Sigortacılık Kanunu madde 31/a'daki sır saklama yükümlülüğünden faydalanılamadığı sorulmuş, bu kapsamda öncelikle madde 6/3'te sayılan amaçlara takıldığının düşünüldüğü ifade edilmiştir. 6. Maddede sayılı olan dört faaliyet amacından en az birine girdikten sonra devamındaki kriter olarak, sır saklama yükümlülüğüne sahip kişi olmanın aranacağı belirtilmiştir. Bu esnada, sigortacılığın *sağlık hizmetleri ile finansmanının planlanması ve yönetimi* amacına dahil edilebileceği, Türkiye Sigortacılar Birliği'nin bu konuda Kurum'a görüş sunduklarının bilgisi de paylaşılmış, ancak Kurum'un benzer görüşte olmadığı söylenmiştir.

Madde 5/2'de sayılmış istisnaların birçoğunda *zorunluluk* dendiği, oysa ki bunun GDPR ile de uyumlu bir şekilde *gereklilik* olarak değiştirilmesine ihtiyaç olduğu vurgulanmıştır.

Madde 6 kapsamında özellikle sağlık verileri yönünden istihdam ilişkisi amacıyla işlenmesi gibi bir amacın da maddeye eklenmesi önerilmiştir.

Pratikte, sabıka kaydı ve adli güvenlik kayıtlarında yer alan özel nitelikli kişisel verilerin işlenmesine dair de zorluklarla karşılaşıldığı, bu verileri işlemek için ilgili kişiden açık rıza alınması şartı olduğu halde, hemen hemen her yerde paylaşmanın zorunlu tutulduğu, bunun çelişkili bir durum yarattığı belirtilmiştir. Kanunda bir değişiklikle olmasa bile, Kurum'un bu konuda bir kılavaz ile en azından sektörel bazda görüş ve tavsiyelerini iletebileceği söylenmiştir.

Analık izni, iş göremezlik gibi hallerde sadece sır saklama yükümlülüğü altında olan kişinin değil, personel ve özlük birimi çalışanlarının da bu bilgilere erişime ihtiyaç duydukları vurgulamıştır.

Madde 7:

Silme, yok etme, anonimleştirme ve unutulma hakkının düzenlenmesinde değişikliğe, özellikle unutulma hakkına dair kapsamlı düzenlemeye gerek olduğu paylaşılmıştır.

Madde 9 – Yurtdışına Aktarım:

Güvenli ülkelerin henüz açıklanmaması bir sorun olarak belirtilmiştir. Burada grup içi aktarım muafiyetleri gibi düzenlemelerin söz konusu olabileceği ifade edilmiş, yine GDPR'a paralelliğin öneminin altı çizilmiştir.

Madde 10 – Aydınlatma Yükümlülüğü:

Aydınlatma Yükümlülüğü Tebliğ'indeki *"Her bir birim nezdinde"* ifadesi eleştirilmiş, ancak, Kurum'un da benzer bir bakış açısında olduğu, her bir birim nezdinde yürütülen işleme faaliyetlerinin tek bir metinde yazılabileceğini söyledikleri belirtilmiştir. Ancak Tebliğ'in lafzında da bu doğrultuda bir değişikliğe ihtiyaç olduğu söylenmiştir.

GDPR'a paralel olarak, 3. kişiyi aydınlatma yükümlülüğünün doğması hususunun makul çerçevede eklenebileceği önerilmiştir.

Yeni Madde Önerileri:

- Çocukların kişisel verilerinin işlenmesi ilgili bir madde ve devamında detaylı bir tebliğinin gerektiği vurgulanmıştır. Bu konuda GDPR'daki düzenlemeyle aynı veya benzer bir düzenlemenin yapılabileceği ve devamında Kurum'un bir kılavuz çıkartmasanın istenebileceği söylenmiştir.

- Saklama süreleriyle ilgili ICO'nun yaptığı gibi bir kılavuza ihtiyaç olduğu belirtilmiştir. Özel sektör firmalarının kurumsal hafıza yaşatma talebinden bahsedilmiş, belirli konularda dava zamanaşımı sürelerine gidildiği ifade edilmiş, ancak kurumsal hafıza ve arşiv amaçlı saklama ihtiyacının daha uzun süreler veri saklamayı gerektireceği söylenmiştir. Bu talebe, meşru menfaatinin olması perspektifinden bakılıp bakılmayacağı sorulmuştur. Kurumun bu konuda şu ana kadar açık bir yorum yapmadığına değinilmiştir.

  Global şirketlerde ise fiiliyatta dönemsel silme faaliyetlerinin yapıldığı, ancak bunların genellikle globalden bildirilen süreler olduğu, farklı süreler belirlemek içinse alt yapı ihtiyaçları ve dolayısıyla ilave maliyetlerin doğabileceğinden bahsedilmiştir.

  Sektörel birliklerin ve derneklerin süreleri belirleme konusunda önem taşıdıklarının altı çizilmiştir. Saklama sürelerine dair yurtdışı örneklerine de bakılmasının gerektiği söylenmiştir. Sektörel anlamda da yurtdışı örneklerine bakılabileceği ifade edilmiştir. Diğer taraftan, saklama süreleri için sadece kanuni zamanaşımı sürelerinin dikkate alınmaması, zamanaşımı definin ileri sürülebilmesi için veriyi bir süre daha saklamaya ihtiyaç olabileceği şeklinde görüş iletilmiştir.

  Çalışan verileri, sözleşme taraflarının verilerinin saklanması konusunda, silme-yok etme-anonimleştirme tebliğinde silme tanımı olduğu ama bu işlemin sadece bilişimsel anlamda bir silme olduğu, çünkü fiiliyatta erişimin kısıtlanması şeklinde yapıldığı ifade edilmiştir. Kanundaki yükümlülüğün ise silme, yok etme, anonimleştirmeden

biri olduğu söylenmiştir. Fiziki kayıtlarda ise, erişimi kısıtlamanın silme olarak kabul edilmediği belirtilmiştir. Tüm bu hususlar bir arada gözetilerek silme tanımının yeniden düzenlenmesinin gerektiğinin altı çizilmiştir.

Kişinin unutulma hakkının olduğu, veri saklamanın süresiz olmasının bu bağlamda kişinin temel hak ve özgürlükle çakışacağı hatırlatarak, kurumsal hafıza veya arşiv gibi amaçlarla dahi süresiz bir saklamanın yapılamayacağı belirtilmiş, bir sonraki Platform toplantısında bu konunun ayrı bir gündem maddesi olarak tartışılması önerilmiştir.

- Veri sorumlusu ve veri işleyen arasındaki rejim ve veri işleyenin yükümlülükleri konularında da ilave düzenlemelere ihtiyaç olduğu söylenmiştir.

Ceza hukuku açısından Öneriler:

- Davranış normlarının alanının daraltılması,
- Hassas veriler için TCK'ya uyumluluk,
- Madde 135, 137, 138 şikayete bağlı olacak şekilde yeniden düzenlenmesi,
- KVKK ve TCK arasındaki terminolojik olarak yeknesaklık şeklinde öneriler anlatılmıştır.

Ayrıca; kamunun kişisel verilerin korunmasına ilişkin hangi esaslara uyacağının ayrı bir çerçeve yasayla belirlenmesi gerekliliğinden bahsedilmiştir.

7. Saklama Sürelerinin Tespiti Meselesi, Uygulamaya Yönelik Öneriler

Konu 15 Mart 2019 tarihli Platform toplantısında ele alınmıştır.

Platformda tartışmalara kişisel verinin değeri ve tüm veri sorumlularının kişisel veriyi azami ölçüde saklamak için gerek ihtiyaç gerekse meşru menfaatlerinin olduğunun belirtilmesi ile başlanmıştır. Zira telekomünikasyon, elektronik ticaret veya herhangi bir sektör fark etmeksizin kişisel verilerin, veri sorumluları için adeta bir hazine niteliğinde olduğu ve bu

verilerin veri sorumluları için müşteri memnuniyetini sağlamak gibi pek çok hususta temel oluşturduğuna dikkat çekilmiştir. Nitekim sigorta sektöründe de ne kadar çok delil toplanırsa riske ilişkin karar verebilme yetisinin o denli keskin olacağı ifade edilerek, kişisel verilerin silinmemesinde ve kullanılmasında veri sorumlularının bu tür haklı gerekçelerinin de olabileceği ifade edilmiştir. Bu doğrultuda, önemli olan noktanın, saklama sürelerinin efektif bir şekilde belirlenmesi olduğu belirtilerek, bu konuya ilişkin olarak yurtdışındaki iyi uygulama örneklerinin baz alınması önerilmiştir.

Saklama sürelerinin belirlenmesine ilişkin olarak, kişisel veri işleme envanterlerinde veri kategorisi bazında en uzun saklama süresinin belirlenmesi gerektiği ve aydınlatma metinlerinde saklama sürelerine ilişkin bir belirleme yapma yükümlülüğü olmasa dahi, fiiliyatta bu tür bir gerekliliğin de doğmaya başladığı belirtilmiştir.

Saklama sürelerinin tespiti açısından en çok zorluk teşkil eden hususların neler olduğuna ilişkin sorunun ardından; saklama süreleri belirlenirken mümkün olduğunca kanuni zamanaşımı sürelerine ve mevzuatın beklentisine uyulmaya çalışıldığı, ancak çağrı merkezi gibi örneklerde sorunlar yaşandığı ifade edilmiştir. Nitekim çağrı merkezindeki kayıtların uzun süreler saklanmasının müşteri memnuniyeti bağlamında önemli olduğu ve bu verilerin kanuni zamanaşımı sürelerinden daha uzun sürelerle saklanabilmesi için veri sorumlusunun meşru menfaati olduğu gerekçesine dayanılabileceği, ancak bu konuda mevcut halde ciddi bir belirsizlik olduğu belirtilmiştir.

Saklama sürelerine ilişkin bir diğer sorunun ise, belirlenen saklama süresinin bitişi ile birlikte kişisel verilerin hangi noktada ve nasıl imha edileceğine ilişkin bir tetikleme mekanizmasının var olmaması olduğu ifade edilmiştir. Zira kişisel verilerin yer aldığı belgelerin tamamen imha edilmesinin de her zaman mümkün olmadığı; çünkü belge içerisinde yer alan diğer verilerin de kanuni yükümlülükler dolayısıyla saklanması gerekebildiğine dikkat çekilmiştir. Bu kapsamda, belge bazlı silme yaklaşımının doğru bulunmadığı, bunun yerine spesifik olarak veri bazlı bir yaklaşımın benimsenmesi gerektiği ifade edilmiştir.

KKVK madde 28'in dolaylı uygulaması nedeniyle bu dokümanlar içerisinde yer alan bazı verilerin de çok daha uzun süreler ile saklanabileceği, örneğin, pek çok Telekom şirketinde trafik bilgilerinin potansiyel bir suç kaygısından dolayı 10-20 yıl gibi süreler ile saklandığı belirtilmiştir.

Bunlarla birlikte, yurtdışında yer alan iyi uygulama örneklerinde dahi saklama süreleri konusunda bir uyumluluğun söz konusu olmadığı söylenmiş, ABD'de üst düzey pozisyonlara ilişkin CV'lerin 6 ay ve diğer CV'lerin ise 3 ay saklanmasına ilişkin teamül olduğu, uygulamada ise hiçbir şirketin bu kısa sürelere bağlı kalmak istemediği örnek olarak verilmiştir.

Saklama sürelerine ilişkin bir diğer sorunun ise, global şirketlerin durumundan kaynaklandığına dikkat çekilerek; bu tür GDPR uyumlu merkezlere sahip şirketlerde birden çok veri sorumlusu olduğu, şirket merkezinin kendi veri koruma politikasının global ölçekte uygulanmasını istediği, ancak Türkiye şirketinin KVKK dolayısıyla farklı saklama süreleri öngörebileceği ifade edilmiş ve bu durumun ortaya bir "compliance" uyuşmazlığı çıkardığı belirtilmiştir. Bu tür durumların önüne geçilmesi adına olabildiğince yeknesak uygulamaların benimsenmesinin önemli olacağı vurgulanmıştır.

Bunun yanında, aslında verilerin gerçek anlamda "silinmesi" kavramının dijital dünya açısından da oldukça zor olduğu, silinen verilerin teknin olarak her zaman geri getirilmesinin mümkün görüldüğü belirtilmiştir. Bununla birlikte, Kurum'dan alınan bir görüş kapsamında saklama süresinin dolması ardından silinen bir verinin, bir uyuşmazlık konusu olması halinde dahi geri getirilerek kullanılmaması gerektiği ifade edilmiştir.

Silme ve yok etme kavramlarının arasındaki farka dikkat çekilmiş, Kurum'un görşünde bahsettiği hususun bir ihtimal "yok etme" kapsamında olabileceği ifade edilmiştir. Nitekim verilerin silinmesinin aslında veri sorumluları için bir çıkış yolu olduğu ve iyi yazılmış ve uygulana bir silme politikasının, hem amaca hizmet ederken hem de verilere daha sonra ihtiyaç duyulması halinde geri getirilmesi yolunda oldukça yararlı bir araç olabileceği belirtilmiştir. Ek olarak, yok edilen bir verinin ileride kamu kurumları tarafından talep edilmesi halinde veri sorumlusunun, KVKK kapsamındaki imha yükümlülüklerini bir savunma karinesi olarak da kullanabileceği ifade edilmiştir.

Bu düşünceye destek olarak, verilerin imhasının veri sorumlularına verilen bir yükümlülük olmasının yanında, aynı zamanda bir hak olduğu dile getirilmiştir. Ancak bununla birlikte, oldukça yeni bir yasal düzenlemeye dayanan bu tür bir savunmanın yargıda nasıl algılanacağının bu safhada oldukça belirsiz olduğuna dikkat çekilerek, hakim ve savcıların

böyle bir durumu “delillerin yok edilmesi” veya “karartılması” olarak algılama ihtimallerinden çekinilmesi gerekeceği belirtilmiştir. Karşılaşılan bir olayda, kamera kayıtlarını 2 hafta saklayan bir şirkette yaşanan bir hırsızlık olayında savcının kamera kayıtlarını talebi üzerine verilerin silinmiş olduğunun aktarıldığı ve savcının takipsizlik kararı verdiği söylenmiştir. Bu noktada verilerin imhasının bir delil karartma değil ancak bir yükümlülüğün yerine getirilmesi olduğu yönündeki algının yerleştirilmesinin oldukça önemli olduğu ifade edilmiştir.

Bu doğrultuda, işin TCK boyutuna da dikkat çekilerek, savcıların şu an için uygulamada nasıl bir bakış açısına eğimli oldukları sorulmuştur. Bu noktada, öncelikle ceza hukuku boyutunda şüpheli veya sanığın kendi elindeki delilleri yok etmesinin aslında bir suç teşkil etmediğine dikkat çekilerek, günün sonunda saklama sürelerinin ister ceza, ister hukuk olsun mahkemeleri uzmanlık isteyen bir noktaya götüreceği belirtilmiştir. Hakim ve Savcıların güncel durumuna ilişkin olarak ise, ilk derece ve istinaf mahkemelerinin henüz KVKK’ya hakim olmadıkları, TCK kapsamında kişisel veri işleme ihlallerine karşı verilecek bir cezanın 5 yılın altında olacağı, bu nedenle temyiz incelemesine tabi olmayıp, istinaf kanun yoluyla kesinleşeceği, dolayısıyla Bölge Adliye Mahkemelerinin konuya hakimiyetinin oldukça önemli olacağı belirtilmiştir.

Ayrıca, TCK madde 138’de yer alan “belirlediği süreler” ifadesine dikkat çekilerek, KVKK madde 7’nin de veri sorumlularını yönetmeliğe yönlendirdiği ve yönetmeliğe göre kanunda belirli bir süre olmadığı durumlarda saklama sürelerinin, veri sorumlularının kendilerinin belirlemesi gerektiği ifade edilmiştir. Ancak bu düzenlemenin hem eşitlik hem de kanunilik ilkeleri kapsamında tartışılır olduğu, bu nedenle de Kurum tarafından sektörel birliklerin de görüşleri alınarak yapılacak açık düzenlemelere ihtiyaç olduğu belirtilmiştir.

Kişisel verilerin saklama sürelerinin sonunda imha edilmelerine ilişkin olarak, tartışılması gereken bir diğer konunun ise zamanaşımı defi olduğuna dikkat çekilerek, veri sorumlularının zamanaşımı defini, zamanaşımı geçtikten sonra ileri süreceğine, ancak zamanaşımının geçmiş olduğunu ispatlamak için ise delil sunması gerektiğine ve verilerin silinmesi durumunda bu delilin sunulamayacağına dikkat çekilmiştir.

Veri sorumlularının verilerin silinmesi durumunda savunma haklarını kullanamayacaklarına dair kaygı taşıyan bu görüşe karşılık olarak ise, bu durumun hukuka aykırılık olacağı ve

herhangi bir muhakemede dikkate alınmayacağı görüşü iletilmiştir. Ancak, düzenlemenin mevcut haliyle saklama süresini belirleme yetkisini veri sorumlusuna bırakmış olduğu hatırlatılmıştır. Ek olarak, verilerin ileride doğabilecek ihtiyaçlar nedeniyle saklanması durumunda aslında zaten KVKK madde 5 kapsamında işleme şartının var olduğu ve silme halinde verilerin zaten teknik olarak geri getirilebileceği de ifade edilerek, sorunun bu gerekçelerle aşılabileceği de dile getirilmiştir.

Sonuç olarak tüzel kişi veri sorumlularının verilerin silinmemesi halinde taşıyacakları riski bilerek hareket etmeleri ve kanunun kendilerine bıraktığı takdir yetkilerini ölçülülük ilkesi çerçevesinde kullanılmaları gerektiği belirtilmiştir.

Bu kapsamda, veri sorumlusunun takdir yetkisini kullanarak belirlediği sürelere ilişin bir şikayet geldiği takdirde ise, Kurul'un bu sürelerin doğruluk ve uygunluğunu değerlendirebileceğine dikkat çekilmiştir.

Bazı katılımcılar, saklama süreleri belirlenirken zamanaşımı sürelerini dikkate almak gerektiği, zamanaşımının dolduğu noktada verinin daha fazla tutulmasının istenmediği ve ancak verinin işlenmeye devam edilebilmesi için somut bir neden olması gerektiği, bunun tartışmalara neden olacağı, dolayısıyla saklama sürelerine sınırlar ve/veya somut kriterler getirilmesinin gerekli olduğunu ifade etmişlerdir. Bu görüşe karşılık olarak, gerek KVKK gerekse Kurum'un somut ve keskin süreler belirlemesinin riskli olacağı, bu nedenle veri sorumlularının her bir işleme faaliyeti için amaç ve verilerin niteliğini birlikte düşünerek farklı süreler belirlenmesinin yerinde olacağı ileri sürülmüştür.

Silme faaliyeti kapsamında tartışılan bu konuya dair yapılan bir öneride; kişisel verinin silinmesinin ardından açılabilecek bir davada, veri sorumlusunun şirket içerisinde oluşturacağı bir kurul tarafından alınacak bir karar ile ilgili verinin geri çağırılması, bu işlemin yeni bir amaç taşıyacağı ve verinin artık bu işleme amacı kapsamında işlenebileceği söylenmiştir. Veri sorumlularının kendi bünyelerinde yürütecekleri samimi ve titiz çalışmalar ile çıkartacakları prosedürlerin faydalı olacağı, hatta bu hallerde Kurul'un da cezalandırıcı bir yöntem izlemesinin beklenmeyeceği görüşü paylaşılmıştır.

Kurum'un önceki haftalarda yayımlanan veri imha politikası ve tablosuna ilişkin olarak ise, 3 farklı tablonun söz konusu olduğu; verinin mi, kategorinin mi, yoksa sürecin mi imha edilmesinin net olarak anlaşılmadığı ifade edilmiştir.

Kurum'un yayımlamış olduğu tabloya ilişkin olarak ilaveten, sektörlerin tablolarını daha önceden kategori bazında oluşturdukları ve Kurum'un yeni yayımlanan tablosuna göre yeni düzenlemeler yapmalarnın ciddi bir efor gerektireceği söylenmiştir. Bunun yanında pratikte silme faaliyeti için kullanılan çok farklı cihazlar ve yazılımlar olduğu, ancak Kurum'un hangi tekniğin kullanılmasına ilişkin açık bir yönlendirme yapmadığı da belirtilmiştir.

Kurum'un yayımladığı politika üzerine çalışarak, Kurum'a bir görüş verilebileceği ve sektör spesifik ihtiyaçlar farklı olabileceği için kesin süreler belirlemek yerine, sürelerin nasıl belirleneceğine dair açık ve spesifik kriterler üzerine bir doküman hazırlanmasının daha yararlı olabileceğine dair fikir birliği oluşmuştur.

8. Kurul Kararı Işığında Veri İhlal Bildirimleri

Konu 15 Mart 2019 tarihli Platform toplantısında ele alınmıştır.

Kurul'un veri ihlallerine ilişkin bildirim formunu yayımlamış ve bu konuda bir ilke kararı almış olduğu, GDPR altında belirlenen 72 saatlik ihlal bildirimi süresini bir zorunluluk olarak kabul ettiği belirtilerek, katılımcıların bu konudaki tespitleri sorulmuştur.

Öncelikle böyle bir karara uzun zamandır ihtiyaç duyulduğu belirtilmiş, zira KVKK'da ihlalin kısıtlı bir şekilde düzenlendiği, formda ihlalin kaynağına ilişkin örnekler de bulunmasının oldukça olumlu olduğu, ancak bildirimin kapsamının çok geniş olmasının sorunlar yaratabileceği söylenmiştir. Bununla birlikte, formun ICO formuna oldukça benzer olduğuna dikkat çekilmiştir. Formda yer alan "siber saldırı" kavramının ise açık olmadığına işaret edilmiştir.

Öte yandan, Kurum'un bildirim formunun kendilerine e-posta yoluyla iletilmesi yönündeki önerisinin şaşırtıcı olduğu, çünkü bu tür bir iletişimin daha fazla sızıntıya yol açma riski barındırabileceği ifade edilmiş, bu konuda Kurum'a bir görüş verilebileceği önerilmiştir.

GDPR'ın her türlü ihlali bildirim yükümlülüğü getirmediği, önemli risk potansiyeli taşıyan ihlallerin bildirilmesini istediği, Kurum'un da benzer bir yol izlemesinin hem kendilerinin iş yükü hem de veri sorumlularına getirilen yükümlülükler karşısında daha yerinde olacağı da ifade edilmiştir.

Bununla birlikte, bu defa veri sorulularının ihlali bildirip bildirmemek yönünde bir test yapması gerekebileceği ve bildirmeme kararının cezai sorumluluk açısından riskli olabileceğine dikkat çekilmiştir.

Veri sorumlusunun formu doldurmak için Alo 198'i araması, ancak daha sonra bildirimde bulunmaktan vazgeçmesi halinde ise, kamu görevlisine ihlalin bildirilmemesinin ayrı bir suç teşkil edeceği, bu nedenle böyle bir bilgilendirme yaptıktan sonra ihbarın artık zorunlu olacağının düşünüldüğü ifade edilmiştir.

Bu hususlardan hareketle, hangi hallerde bildirimin yapılması gerekeceğinin daha net olarak belirlenmesinin yerinde olacağı, zira şirketlerin itibar zedelenmesi kaygısıyla küçük ihlalleri bildirmek istemeyeceği belirtilmiştir. Ayrıca, ilgili formda ihlalin boyutuna ilişkin yorum da istendiği, ancak bunun DPIA yapılmasını gerektirecek bir istek olduğu ve Türkiye'de henüz böyle bir uygulamanın söz konusu olmadığı belirtilmiştir.

"72 saat" sınırına ilişkin olarak ise, aslında bunun çok mutlak bir sınırlama olmadığı, nitekim Kurum'un aşamalı bildirime de izin verdiği ve ayrıca bildirim formunda "gecikmenin nedenleri" başlığının da yer aldığına dikkat çekilmiştir. Bunun yanında olası bir saldırıda kişisel verilerin etkilenip etkilenmediğinin öncelikli olarak araştırılması gerektiği ve 72 saatin de "kişisel verilerin" saldırıdan etkilendiğinin öğrenilmesi anında başlayacağı belirtilmiştir.

Ek olarak, formda yer alan "gerekli görülen" teknik ve idari tedbirlerin çok geniş bir spektrum olduğu belirtilerek, bunun bir şekilde daraltılması ve sektöre özgü önlemlerin belirlenmesinin faydalı olacağı ifade edilmiştir.

9. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ ile Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi Işığında Uygulama ve Güncel Tespitler

Konu 19 Nisan 2019 tarihli Platform toplantısında ele alınmıştır.

Daha önceki Platform toplantılarda Aydınlatma Tebliğine ilişkin tartışmalara yer verildiği hatırlatılarak, katılımcıların Aydınlatma Rehberine ilişkin görüşleri ve uygulamada ortaya çıkan sorunlar sorulmuştur.

Bazı global şirketlerin GDPR metinlerini kullanmakta olduğuna dikkat çekilerek; GDPR uyumlu global şirketlerde kullanılan aydınlatma metinlerinin, KVKK rehberlerine göre revize edildiği, işleme amaçlarının tek tek yazıldığı ve bu amaçların da departman bazlı olarak yazıldığı ifade edilmiştir. Bunun yanında, metnin uzamasının önüne geçmek adına, Kurul'un uygulamasında olduğu gibi ilgili kişinin haklarını tek tek saymak yerine KVKK'nın 11. Maddesine atıf yapılarak geçildiği belirtilmiştir.

Bu kapsamda, Tebliğ'de geçen "farklı birimler nezdinde aydınlatma" ifadesine ilişkin olarak özellikle Platformun yeni katılımcılarının yorumları sorulmuştur. Soruya cevaben, işleme amaçlarının birim bazlı olarak yazılmasının gerekli görülmemesine rağmen, risk almamak adına metinlerin bu şekilde hazırlandığı hallerin olduğu söylenmiştir.

Rehbere ilişkin tespit edilen sorunlardan ilkinin "katmanlı aydınlatma" olduğu belirtilerek; Rehber uyarınca ilk katmanda tam olarak hangi unsurlara yer verilmesi gerektiğinin belirtilmemiş olduğuna, ancak bunun yapılmasının uygulamadaki birlik ve veri sorumlusunun aydınlatma yükümlülüğünü doğru bir şekilde yerine getirmesi gibi amaçlar yönünden önemli olduğuna dikkat çekilmiştir.

İkinci olarak, Rehberin veri kategorilerinin yazımına ilişkin örnekler dışında bir açıklama içermiyor olması eleştirilmiş ve mevzuatta aslında "veri kategorisi" kavramının yer almadığı belirtilmiştir. Aydınlatma metinlerinde kullanılan "gibi" tarzı ifadelerin uygun bulunmaması

da sert bir bakış açısı olarak nitelendirilmiş, bu tür kelime ve edatların kullanıldığı yere göre değerlendirilmelerinin daha doğru olabileceği üzerinde durulmuştur.

Buna karşın, özellikle dijital sektörlerde iş akışının çok hızlı bir şekilde değiştiğine işaret edilerek, doküman bazlı veri yazımının aydınlatma metinlerini anlamsızlaştırabileceği, bu doğrultuda metinlere verileri tek tek yazmak yerine veri kategorilerinin belirtilmesinin yeterli olması gerektiği ifade edilmiştir.

Bu doğrultuda, veri sorumlusunun aydınlatma yükümlülüğünün esas amacının verinin elde edilmesi sırasında ilgili kişiyi aydınlatmak olduğu hatırlatılarak, veri sorumlusunun detaylı ve genel bir veri politikasını web sitesine koymuş olması ve bu politikada işlenen verilerin yazılmış olması durumunda, aydınlatma metinlerinde kategori bazlı veri belirtmenin yeterli olabileceği, ancak bilgilendirmenin kişisel verilerin elde edilmesi sırasında yapılması gerekliliği doğrultusunda veri bazında aydınlatma yapmanın daha sağlam bir yöntem olduğu yorumları da yapılmıştır.

Ek olarak, aydınlatma yükümlülüğünün yerine getirilmesi sırasında veri sahibinin hangi verisinin ne şekilde ve hangi amaçla işlendiğinin oldukça şeffaf ve net bir şekilde ortaya konması gerektiği ve katmanlı aydınlatmaların yalnızca detaylı bir aydınlatma yapmanın yer ve zaman gibi nedenlerle mümkün olmadığı durumlar için tercih edilmesinin daha doğru olacağı belirtilmiştir.

Uygulamadaki bazı aydınlatma metinlerinin verinin hangi amaçla işlendiğini açıkça belirtmeyen genel ifadelerle yazılmış olması eleştirilmiş; buna karşılık olarak fazla spesifik aydınlatma metinlerinin ise, veri sorumlusu tarafından örneğin yalnızca tek bir etkinlik için kullanılabilmesi nedeniyle zorluk ve belge kalabalığı yaratabildiğine dikkat çekilmiştir. Bu soruna karşı bir çözüm olarak; veri sorumlularının web-sitelerinde temel ve genel bir aydınlatma yaparken, içeriğin ilgili kısımlarına yerleştirecekleri linkler vasıtasıyla spesifik kişi grupları veya veri işleme faaliyetlerine ilişkin detaylı aydınlatma metinlerine bu suretle yönlendirme yapabilecekleri önerilmiştir.

Uygulamadaki bir diğer sorunun ise, şirketlerin bazı veriler açısından veri işleyen, bazıları açısından ise veri sorumlusu olması durumunda aydınlatma metinlerinin içeriğinin nasıl olacakları ve aydınlatma bildiriminin ne suretle yapılması gerekeceğinin olduğu söylenmiştir.

Bu tür durumlarda aydınlatma metinlerinin oldukça karmaşık ve uzun hale gelmesinin önüne geçmek için yurtdışında kullanılan bir yöntemin ise, aydınlatma metinlerinin içerisine çeşitli semboller, linkler, renkler eklemek ve ilgili kişileri bu şekilde yönlendirmek olduğuna dikkat çekilmiştir. Nitekim bu tür sembollerin Kurum tarafından da benimsenmesi ve yeknesaklaşması durumunda metinlerin çok daha yalın, anlaşılır ve kısa olabileceği belirtilmiştir. Bu öneriye bir eleştiri getirilmiş, aydınlatma yükümlülüğünün asıl amacının ilgili kişinin açık bir şekilde aydınlatılması olduğu, sembol kullanımının ise veri sorumlusunun pratiği kolaylaştırmak adına bir alternatif olduğu ve aydınlatma yapmanın ruhu ile bağdaşmayacağı söylenmiştir. Bu görüş çerçeveside, uygulamanın işlenen verinin yoğunluğu ve kişi grubuna göre de değişiklik gösterebileceği, örneğin çalışanlara yönelik aydınlatma metinlerinin detaylı olarak yazılmasına devam edilirken, bir outdoor aktiviteye ilişkin aydınlatma metninde sembollere başvurulabileceği, ilgili kişinin odağına göre çeşitli / farklı yöntemlerin benimsenebileceği ifade edilmiştir.

Uygulamada, bazı metinlerde standart bir şekilde "Kanun'un 5. ve 6. Maddesinde sayılan sebeplere dayanarak" gibi genel bir ifadenin kullanılmakta olduğuna dikkat çekilerek; bu noktada da işleme amaçlarının açıkça sayılmasının önemine işaret edilmiştir. İlgili kişinin haklarına ilişkin 11. Maddenin aydınlatma metninde Kurum'un uygulaması doğrultusunda yalnızca atıfla geçilebileceği, ancak ilgili kişinin haklarını düzenleyen bu maddenin aydınlatmanın ruhu ile de uyumlu olarak, korunabildiği hallerde açık olarak yazılmasının daha doğru olacağına dair görüşler de iletilmiştir.

Özellikle dijital sektörlerdeki iş akışının çok hızlı bir şekilde değiştiği yorumu tekrar edilmiş, bu yoruma katılanlar, birbirine atıf yapan kısa aydınlatma metinleri sunmak gibi esnek yöntemlerin de benimsenebileceğini, nitekim Google'ın aydınlatmalarını da bu şekilde yaptığını ifade etmişlerdir.

Kurum'un aydınlatma rehberinde dikkat çekilmesi gereken bir hususun da kamera kaydı alınan yerlere konulan katmanlı aydınlatma metinleri olduğu söylenmiştir. Güvenlik gerekçeleriyle bir veri sorumlusunun işyerindeki tüm kameraların yerini ifşa etmek istemeyebileceği, bunun yerine işyerine girişte ve/veya genel bir alanda işyerinde kamera ile fiziksel mekan güvenliği takibinin yapldığının açıklanmasının, yeterli bir aydınlatma seviyesi olarak kabul edilmesinin yerinde olacağı belirtilmiştir.

Aydınlatma metninin katmanlı, sembollü ve benzeri yöntemlerle olmasına ilişkin tartışmalara karşın, asıl önemli olanın söz konusu metnin gerekli mesajı açık bir şekilde verip veremediği olduğu hatırlatılmış ve metin anlaşılabilir ve açık olduğu sürece, bu tür detayların fazla önem taşımayacağı dile getirilmiştir.

Uygulamada karşılaşılan bir diğer sorunun, iki veri sorumlusu olduğu hallerde yasaşandığı, kanunda ortak veri sorumlusu kavramının yer almadığı, ancak ticaret hayatının gereklilikleri doğrultusunda, adi ortaklık gibi durumlarda iki veri sorumlusunun da belirtilmesinin mecburi olduğu ifade edilmiştir.

Rehberin 10. sayfasında, "*veri sorumlusunca aydınlatma yükümlülüğü yerine getirilirken kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları da açıkça belirtilmelidir*." ifadesinin yer aldığı; ancak 16. sayfada yer alan "*Yurt içi ve yurt dışına aktarım yapılacaksa, aktarımın amacının aydınlatma metninde belirtilmesi gerekmektedir. Ayrıca bu aktarımın yapılacağı gerçek veya tüzel kişilerin kimler olacağı da belirtilmelidir"* ifadesi ile çeliştiklerine dair bir yorum iletilmiştir. Bu tür durumlar karşısında Kurul'un yaklaşımları üzerinden de okuma yapılabileceği, amacın verilerin aktarılacağı kişilerin veya kişi kategorilerinin belirtilmesi şeklinde yorumlanabileceği, tek tek kimler olduğunun yazılmasının beklenmediği söylenmiştir. Aydınlatma metnine konu her bir faaliyet yönünden spesifik tahliller yapılabileceği, kaldı ki önemli olanın ilgili kişilerin aydınlatılmasında samimi ve açık bir çaba içinde olmak olduğu ve Kurul uygulamalarını sert kurallar olarak yorumlamamak gerektiği de iletilen yorumlar arasında yer almıştır.

Değinilmesi gereken bir diğer sorunun ise belgeyi imzalatmak olduğu belirtilmiştir. Tebliğ uyarınca veri sorumlusunun aydınlatma yükümlülüğünün yerine getirildiğini ispat yükümlülüğü olduğundan, pratikte metinlerin altına imza alma uygulamasının arttığı söylenmiştir. Avrupa'dan örnek verilmiş, bu ispat yükümlülüğünün, belirli bir sürecin uygulanmakta olduğunun ortaya konulması ile yerine getirilmiş kabul edildiği, bizde de benzer bir yaklaşım ile hareket etmekte fayda olacağı, zira her bir aydınlatma metnine imza almanın fiiliyatta süreçleri zorladığı ifade edilmiştir.

Aydınlatma yükümlülüğünün, "ilgili kişinin anlayabileceği şekilde" yapılması gerektiği hususuna ilişkin olarak, 18 yaşından küçük bir çocuğun aydınlatılmasının nasıl yapılması gerektiği sorulmuş ve bu noktada ayırt etme gücünün devreye girdiğine işaret edilerek, rızayı

da yasal temsilcinin vereceği göz önünde bulundurularak, aydınlatmanın yasal temsilciye hitaben yazılmasının doğru olacağı belirtilmiştir.

Aydınlatma yükümlülüğünde yer alan asgari şekil şartlarının yerine getirilmemesi durumunda hangi sonuçlar ile karşılaşılabileceği sorulduğunda ise bu noktada "geçerlilik" tartışmasının değil, ancak "yükümlülüğün gereği gibi yerine getirilmemiş olması" tartışması yapılabileceği söylenmiştir. Devamında işleme şartı açık rıza ise, bu noktada aydınlatmnına usulüne aykırı olması halinde, verilen rızanın da sakat olacağı ifade edilmiştir. Bu kapsamda işin ceza hukuku boyutuna bakıldığında alınan rızanın sakat olmasının, cezai yaptırıma giden sonuçları olabileceği belirtilmiş olmakla birlikte, aydınlatma metninde nitelikli hatalar veya hukuka uygunluk sebeplerinde yanılmaya sebep olacak türden ifadeler yok ise, metne dair belirli düzeltici faaliyetlerin yerine getirilmesi ile ilerlenebileceği görüşler arasında yer almıştır.

Aydınlatma yükümlülüğüne ilişkin bir diğer sorunun ise, aydınlatma yükümlülüğünün veri sorumlusunun "yetkilendirdiği kişi" tarafından yerine getirilmesi durumunda bu yetkilendirmenin prosedürünün belirli olmadığı ve ikinci bir problemin ise ilgili kişilerin aydınlatmaya ulaşması boyutunun hiç tartışılmadığı, nitekim AB'de online olarak sunulan aydınlatmaların tek tıklama ile ve mobilde de iki tıklama ile ulaşıma açık olması gibi kuralların varlığı dile getirilmiştir.

Aydınlatma yükümlülüğünün yerine getirilmesinde, kişisel verinin başka bir veri sorumlusuna aktarıldığı esnada aydınlatmayı kimin yapacağı / yapması gerektiği de sorulmuştur. Soruya, kişisel verinin ilk toplama noktasında zaten bir aydınlatma yapıldığı ve orada aktarıma ilişkin hususlara da yer verildiği, alıcının veriyi aynı amaçla işleyeceği noktada ayrıca bir aydınlatma yapmasına gerek bulunmadığı, fakat alıcının verileri farklı / yeni bir amaçla işleyeceği durumlarda ayrı bir aydınlatma yapması gerekeceği şeklinde cevap verilmiştir. Öte yanda, veri sorumlularının, alt işveren, tedarikçi çalışanı gibi kişi gruplarına karşı ilgili alt işveren ve tedarikçi firmalar eliyle aydınlatma yükümlülükklerini yerine getirebilecekleri ve gereken haller için açık rızalarına başvurabilecekleri söylenmiştir.

10. Yabancı Veri Sorumluları (Özellikle GDPR'a Tabi Olanlar) Açısından Aydınlatma Yükümlülüğü*; Kanunlar İhtilafı Sorunu Olup Olmadığı*

Konu 19 Nisan 2019 tarihli Platform toplantısında ele alınmıştır.

Öncelikle, yabancı veri sorumlularının aydınlatma yükümlülüğünü yerine getirmesi noktasında uygulamada karşılaşılan bir sorunun, bu veri sorumlularının kendilerini veri sorumlusu olarak addetme veya addetmeme konusundaki sübjektif kararları olduğu ifade edilmiştir. Zira bu veri sorumlularının takdir yetkilerini kullandığı ve bazılarının merkezlerini veri sorumlusu olarak gördüğü, bazılarının ise Türkiye'deki iştiraklerini veri sorumlusu olarak gördükleri belirtilmiştir.

Bu tür belirlemelerin yapılmasında yardımcı olacak bir ölçütün, server paylaşımı olduğu ifade edilerek, yurtdışındaki ana şirketin yalnızca kendi sistemini kullanıma sunması durumunda veri işleyen olacağı, ancak örneğin terfilerin belirlenmesi gibi süreçlere dair bir işleme faaliyeti içinde olduklarında kendilerinin de ayrı birer veri sorumlusu olarak kabul edileceği gibi bir durumun var olduğunu altı çizilmiştir.

Yabancı veri sorumlularının aydınlatma yükümlülüğü sırasında hem GDPR hem de KVKK metinlerinin mi kullanılacağına ilişkin soruya ilişkin olarak, genel olarak GPDR metinlerinin, KVKK için gerekli olan minimum düzeyde revize edildiğine dair yorumlar paylaşılmıştır.

Bunun yanında, Türkiye'den gelen ziyaretçilere KVKK metni, AB ziyaretçilerine ise GDPR metni sunulabileceği, GDPR'da ilgili kişiye KVKK'da olmayan hakların da tanınmış olduğu ve bir şirketin hem GDPR hem de KVKK'ya tabi olması durumunda metinlerin özellikle sahip olunan haklar yönünden karıştırılmaması gerekeceği ifade edilmiştir.

11. Grup Şirketleri Açısından Aydınlatma Yükümlülüğü ve Uygulamadaki Tespitler

Konu 19 Nisan 2019 tarihli Platform toplantısında ele alınmıştır.

Uygulamadaki en sıkıntılı konulardan birinin, grup şirketleri açısından yurtdışına veri aktarımı olduğuna bir kez daha dikkat çekilerek, katılımcılara başvurdukları yöntemler sorulmuştur.

Yeterli koruma sahip ülkelerin açıklanmamış olmasındna dolayı, bu kapsamda, Kurum'un web sitesinde yer alan taahhütnamenin doldurulması yoluyla, yurdışına aktarım için izin alınması talebinde bulunulduğu, Kurum'un ilettiği cevabi yazıda ise sunulan talebin kabulü veya reddine ilişkin açık bir kararın bulunmadığı, Türkiye'de yerleşik global şirket iştiraklarini veya Türkiye merkezli global şirketlerin yurt dışı iştiraklarini düşünerek, bu konuda hızlı çözüme ihtiyaç duyulduğunun bir kez daha altı çizilmiştir.

Ek olarak, yabancı veri sorumlusunun doğrudan Türkiye'de veri toplaması durumunda ise bunun artık bir aktarım olarak değerlendirilemeyeceği, doğrudan bir veri işleme faaliyeti olduğu ve yabancı veri sorumlusunun birinci veri sorumlusu olarak KVKK'ya tabi olduğu hatırlatılmış, bu yorumun devamında yabancı veri sorumlularının VERBİS'e kaydedilmesi zorunluluğu kısaca yeniden tartışılmıştır.

12. Saklama Süreleri ve Kişisel Veri İşleme Envanterinin Düzenlenmesi

Konu 14 Haziran 2019 tarihli Platform toplantısında ele alınmıştır.

Kurumun hazırlayıp, internet sitesinde paylaştığı örnek kişisel veri işleme envanteri ile Kurumun bazı yorum ve cevapları arasında farklılar olduğuna dikkat çekilerek, konu tartışmaya açılmıştır. Örnek olarak, Kurumun yayınladığı envanterde banka hesap bilgisi, çalışana aitse özlük, müşteri verisiyse finans verisi olarak kategorize edildiği belirtilmiştir. VERBİS'e girişlerde ise "diğer" adlı kategorinin altında çok fazla alt grup oluştuğu vurgulanmıştır.

Pratikte veri sorumlularının esasen bir süredir kişisel veri işleme envanteri çıkarma çalışmaları içinde oldukları, bu bağlamda çok yüklü envanterlerin de oluştuğu, ancak VERBİS'e bu şekilde çıkartılan envanterlerin tamamının yüklenemeyeceği, bu nedenle

VERBİS'te bir takım kavram ve unsurların iç içe olduğu ifade edilirken, sonuç olarak VERBİS'teki bildirimlerde karışıklıklar çıkabileceği yönünde endişeler dile getirilmiştir.

Envanterler oluşturulduktan sonra VERBİS'e nasıl yükleneceği hususunda da kafa karışıklılıklarının olduğu iletilmiştir. Pratikte bazı çalışmalarda VERBİS'e kayıt olacak kısımların genel başlıklar altında toplanma eğiliminde olunduğundan da söz edilmiştir.

Kurumun, VERBİS'e yapılacak bildirimler suretiyle VERBİS'te tutulacak envanterlerle neleri amaçladığı konuşulmuştur. GDPR öncesi dönemde ICO'nun, veri işleme envanterlerini açık olarak kamuya arz ettiği, bu arz edilen envanterlerde yaklaşık 2 milyar satır olduğu, bu satırların bizdeki güncel uygulamanın aksine, birkaç kişi grubu ya da veri işleme amacı sayılıp, üst gruplar içermediği, tek tek detaylı düzenlemelerin yer aldığı belirtilmiştir. KVKK metni esasen eski 95/46 sayılı direktifin çevirisi olduğu için, kişisel verileri işlenenlere, aydınlatma metinleri ile yapılan açıklamaların yeterli gelmemesi halinde başvurabilecekleri bir kaynak olarak düşünülen kamuya açık envaterlerin, bizdeki fiili durumda bu amacı karşılayabilecek bir kapsayıcılıkta olmayacaklarının düşünüldüğü söylenmiştir.

Kişisel veri işleme envanteri hakkında, Direkt döneminde Almanya'da farklı bir algının oluştuğu, Almanya'nın Federal Veri Koruma Otoritesinin VERBİS envanteri benzeri envanterleri değiştirmenin çok yararlı olmadığı düşüncesiyle, DPO'ların ilk temelini attıkları belirtilmitir. Daha sonra GDPR'da *data mapping* denilen dökümlü kayıt tutma sisteminin oluştuğu söylenmiştir. Şu anda birçok şirketin GDPR'ın kapsamı yüzünden bünyelerinde DPO benzeri yapılanmalar oluşturdukları ifade edilirken, acaba KVKK kapsamında da böyle bir eğilim olup olmayacağı sorulmuştur. Kurumun daha önce de GDPR'a ait olan bazı düzenlemeleri adapte ettiği ve bu eğilimde olabileceğine dair kanaatler olduğu söylenmiştir.

İçerik yönetim sistemleri kullanan büyük holdinglerin *data mapping* için zaten bir altyapıya sahip oldukları, bu sebeple aksiyon almalarının diğer şirketler göre çok daha kolay olacağı söylenmiştir. Kullanmayan şirketlerde ise veri sınıflandırma derslerinin alınması önerilmiştir. Oto sınıflandırma programlarından bahsedilmiş, buna göre, "gizli", "az gizli" gibi sınıfların olduğu, halbuki daha fazla detaylandırılmaya ihtiyaç olduğu belirtilmiştir. Departman özeline göre sınıflandırma yapılacak olunursa, bu altyapı çalışmalarının ortalama bir yılı bulabileceği ifade edilmiştir.

Bu başlık altında, VERBİS envanterinin ne zaman DPO sistemine benzer bir sisteme dönüşeceğine dair haziruna görüşleri sorulmuştur. Hazirunun çoğunluğu tarafından bu aşamada olmaması gerektiği ifade edilmiştir. Zira İstanbul'daki veri sorumluları nezdinde bir farkındalık olduğu, ancak taşrada henüz çok düşük düzeyde farkındalık oluştuğu, yeni yeni oluşmaya başladığı söylenmiştir. Farkındalığa ulaşılana kadar VERBİS'in mevcut envanter bildirim sistemi ile devam edilmesi gerektiği vurgulanmıştır. Envanterde VERBİS amaçlarıyla, veri işleme amaçlarının mecburen paralel hale getirildiği, bu durumun aydınlatma metnine de VERBİS amaçları gösterilerek mi yansıtılmalı gerekeceği sorusu sorulmuştur.

VERBİS'ten önce ana amaç alt amaç gibi sınıflandırmalar yapılırken, Kurumun çıkardığı saklama politikasında süreçlerden bahsedildiği, ancak bu süreçlerin de Kurum'un yayınladığı envanterde olmadığı ifade edilmiştir. İlk başta mevzuatın envanteri düzenlemediği, daha sonra ikincil mevzuatların çıktığı, envanterin aslında uygulamanın bulduğu bir kelime olduğu belirtilmiştir. Normalde saklama politikasında envantere atıf yapılır, diye düşünülmüşken, şu an esasında her yere saklama sürelerinin yazılacak hale geldiği vurgulanmıştır.

Öte yadan kişisel veri işleme envanteri çıkartılmasının aslında faydalı ve doğru bir mantık olduğu da ifade edilmiştir. Veri sorumlusu olan bir şirkete inceleme amaçlı olarak gidildiğinde veya herhangi bir amaçla, iyi hazırlanmış bir kişisel veri işleme envanterinin kişisel veri işleme faaliyetleri yönünden bir bütünü gösterebileceği, diğer metin ve prosedürlerin de esasen bu envaterin çıktıları oldukları söylenmiştir.

Envanterdeki güncellemelerin aydınlatma metinleri ve açık rızaların da güncellenmesi anlamına geldiği, bazı süreçlerin yeniden kurgulanması ve envanterin sadeleştirilmesi de demek olduğu ifade edilmiştir. Aslında doğru olanın kişisel veri işleme envanterinin hukukçu veya danışmanlar tarafından değil, onlar tarafından yapılacak anlatımlardan sonra bizzat ilgili birimler tarafından doldurması gerekliliği ve faydasından söz edilmiştir. Envanterin yaşayan ve dinamik bir sistem olmasından dolayı birimler nezdinde bu bilinci geliştirmek gerektiği, henüz bu bilincin yayılmadığı, örneğin pazarlama biriminin envanter oluşturma sürecine girerken o envanteri anlayıp, amacını ve bu amaca göre neleri yazması gerektiğini bilmesinin öneminden bahsedilmiştir. Zaman içinde bu sisteme alışılacağı ve anlayışın artacağına dair inançlı ve umutlu olunduğunun da altı çizilmiştir.

Uygulamada kişisel verilerin korunması alanında yetkin kişi sayısının henüz az olduğundan da söz edilmiştir. Veri sorumlularının bünyelerinde kişisel verilerin korunması alanında genel takip ve koordinasyon için yetkin kişilerin yetiştirilmesinin yanı sıra, her bir birimin kendi süreçlerine hakim kişilerinin de bu alanda bilgilendirilmesinin, süreklilik ve sürecin sağlıklı yönetimi için çok önemli ve faydalı olacağı vurgulanmıştır.

KVKK düzenlemelerinin kurumsallaşmayı da teşvik edeceğinden söz edilmiştir.

Tartışmalar kapsamında VERBİS'e eleştiriler de getirilmiş, mevcut hali ile kanunun amacına hizmet etmeyen, aslında beklenen düzeyde şeffaflık sağlamayan, kayıt yükümlülüğü getiren bir sistem olarak anıldığı söylenmiştir. VERBİS ile veri sorumluları bünyesinde iki ayrı envater algısının yayıldığı, bunun bir ikilik oluşturma riski de barındırdığı, kişisel veri işleme envanteri ve VERBİS envanteri diye farklı kayıtlar oluşturulmak zorunda kalındığı, bunun bir yönüyle ekstra iş yükü de yarattığı gibi hususlar ifade edilmiştir.

Her ne kadar yaşayan, gerçek ve dinamik bir envanter çıkarılmasının öneminden bahsedilse de, VERBİS envanterinin sadece yapmış olmak için yapıldığı gibi bir algının var olduğu, halbuki amacının aydınlatma yükümlülüğüne uyulmadığı veya yeterli düzeyde yapılmadığı noktada ilgili kişinin müracaat edebileceği bir kayıt olarak, değerli bir kaynak yaratmak olduğunun / olması gerektiğinin altı çizilmiştir.

Kurum ile bu konuların ve VERBİS envateri ile ilgili edinilen izlenminlerin görüşülebileceği bir platformun yarar sağlayacağı düşünülmüştür.

Bir görüşte, VERBİS sisteminin getirilmesinde aslında iki amacın güdüldüğü, ilk amacın aydınlatma olduğu, ikinci amacın ise veri sorumlusunun Kurum'a taahhüt vermesi olduğu dile getirilmiştir. Önceki görüşe katılarak, mevcut durumda maalef ilk amacın gerçekleşmesi yönünden VERBİS kayıtlarının yetersiz kalacağı vurgulanırken, buna karşın bir sistemin açılabileceği, herkesin kendi bünyesinde oluşturduğu kişisel veri işleme envanterini (çoğunlukla bir excel tablodur) bu sisteme yükleyebileceği, ancak bir format belirlemenin de çok zor olduğu belirtilmiştir.

Tüm bunlarla birlikte, VERBİS'e kayıt yükümlülüğünün olumlu bir yönü olarak, veri sorumluları nezdinde envanter çıkarmayı disipline etmesinin de öneminden bahsedilmiştir.

Kurumun kayıt altına alma ve genel farkındalık yaratma ihtiyaçlarını ön plana aldığı, esasen envanterin düzgün hazırlanmaması ihtimalinin bir yaptırıma bağlanmadığı şeklinde görüşler de paylaşılmıştır. Yaptırımın sadece envanter girişinin yapılıp yapılmadığına ilişkin olduğu söylenmiştir. Gerçeği yansıtıp yansıtmadığı, aydınlatmalarla paralel olup olmadığı hususlarının kontrole tabi olması gerekeceğine değinilmiştir.

VERBİS ve envater kapsamlı tartışmalarda saklama süreleri de gündeme gelmiştir. Bir görüşte ceza hukukundaki zamanaşımı sürelerinin çok uzun olduğu söylenmiştir. Örneğin TCK madde 182'de yer alan, suç delillerinin aklanması suçunda uzamış zamanaşımının 22 yıl 6 ay olduğundan bahsedilmiştir. Bu açıdan bakılacak olursa, kişisel verilerin 22 yıl 6 ay tutulması gerekeceği, fakat böyle bir süresinin kanunun amacına ve KVKK madde 4'teki temel ilkelere de uygun olmayacağının altı çizilmiştir. Bu yüzden, 5651 sayılı Kanunun dikkate alınıp, kişisel verilerin iki yıl boyunca tutulduktan sonra silinebileceği, ancak daha sonra adli makamların gelip silinen verileri talep etmesi olasılığının ise var olduğu belirtilmiştir.

Kanunda bir süre yoksa sürelerin sektörel yolla belirlenebileceği de önerilmiştir. Uygulamada ise hemen herkesin cezai sorumluluktan çekindiği söylenmiştir.

Kanunun silme, yok etme ve imha etmeye ilişkin maddesi uyarınca uygulamada silmenin tavsiye edildiği, bu sebeple o verilerin örneğin ziplenip, kriptolanıp saklanabileceği, ileride savcılık veya mahkeme istediğinde ise artık yeni bir geçerli işleme nedenine dayanarak, geri getirilebileceği belirtilmiştir.

Kriptolu back up'lara (yedeklemelere) imha etme veya silme süreçlerinde ne olduğu sorgulanmış, back up'ların arasından ilgili veriyi silmenin ya da imha etmenin pratik olarak çoğu zaman imkansızlığından da bahsedilmiştir.

Silmenin o verinin aslına erişmemek, üst anlamda imha etmek anlamına geldiği ifade edilmiştir. Şayet veri silinemeyecek kadar sistemlere bileşikse ve bu durum ilgili kişiye izah edilebiliyorsa, GDPR'a göre silme zorunluluğunun ortadan kalktığı da belirtilmiştir.

Farklı alanlardaki mevzuatlar arasında uyum olmadığı sürece KVKK hükümlerinin tam olarak uygulama alanı bulamayacağı da ifade edilmiştir. Örneğin en çok karşılaşılan veri öznelerinin

çalışanlar olduğu, bu sebeple iş mevzuatındaki hüküm ve koşulların gözetilmesinin kaçınılmaz olduğu, bu bağlamda iş mevzuatında yer alan maksimum sürelerde tutma yükümlülüğüne değinilirken, oluşan endişe yüzünden her ne kadar KVKK'ya göre silme yükümlülüğü olsa da silmenin gerçekleşmesinin mümkün olamayacağı söylenmiştir. Bu tür kaygıların kişisel verileri öngörülen sürelerden çok daha uzun tutmaya sevk ettiği, sektörel ve mevzuat bazında konunun kamu ve özel sektör ihtiyaçlarına göre düzenlenmesinin gerekli olduğu ifade edilmiştir.

Uygulamada ise veri sorumlularının özellikle danışmanlardan net azami süreler duymak istedikleri, konunun KVKK ile düzenlenmediği, Kurul'un da bu hususta bir karar vermediği söylenerek, diğer mevzuatta mevcut zamanaşımı sürelerinden yola çıkılması tavsiye edildiği, ancak pratikte herkesin endişe taşıdığı bir konu olduğuna dair yorumlar iletilmiştir.

Bu tartışmaların büyük çoğunluğunun aslında dijital ortamlardaki veriler için olduğunun, fiziksel verilerin silinmesi kapsamında Kurum rehberlerinde yok etmekten bahsedildiğinin altı çizilmiştir. Kurum'un, fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için, evrak arşivinden sorumlu ve imha edecek bir kişi haricinde kimse tarafından erişilemez hale getirilmesini tanımladığı belirtilmiştir.

Kurumun çeşitli politika ve rehberleri arasında imha yönetemlerine dair bir takım çelişkilerin de olduğu, saklama süreleri ve imha yöntemlerine dair tespit ve ihtiyaçların, önerilerle birlikte Kurum'a sunulmasının gerektiği, Platformda bir ön çalışma yapılabileceği söylenmiştir.

Avrupada belge bazında süre belirlemesi yapılırken, bizde veri bazında yapıldığının altı çizilmiştir. Kurulun yayınladığı saklama tablosunda; doküman, süreç, veri sahibi bazında birçok kategori öngördüğü söylenmiştir.

Anonimleştirme işleminde de bahsedilmiştir. Normalde bu işlem için dijital belgeler üzerinde redaksiyon yapıldığı belirtilmiştir. Orijinal versiyonun ise nerede tutulacağı veya tutulup tuutlmayacağı hakkında ise sorular barındırdığı ifade edilmiştir. Kurum'un yetkili kişinin talebinde orijinal versiyonuna ulaşması gerektiğini belirttiği, bu yaklaşımdan hareketle aslında öncesinde yapılan hiçbir işlemin tam olarak anonimleştirme anlamına gelmeyeceği gibi bir sonuç taşıdığı belirtilmiştir.

Kişisel veriyi imha etmekle ilgili bahsedilen birçok imkansızlığın esasen alt yapı ve maliyet kaynaklı olduğu, bu durumda KVKK'nın ilgili kişinin kişilik haklarının korunması amacı ile veri sorumlusunun meşru menfaatlerinin birbiriyle yarışan haklar olarak, karşımıza her zaman çıkacağının altı çizilmiştir.

13. Kurul Kararlarına Dair Değerlendirmeler; *Facebook Kararı, Yeterli Koruma Bulunan Ülkelerin Tayini, vb.*

Konu 14 Haziran 2019 tarihli Platform toplantısında ele alınmıştır.

Kriterlerin yayınlanmış olmasına rağmen, yurtdışı veri aktarımı yapmak istenildiğinde, fiiliyatta değişen bir durumun olmadığı, güvenli ülke listesi yayınlanmadıkça bu hususstaki fiili zorukların hiçbir zaman tam olarak aşılamayacağı ile ilgili kaygılar taşındığı ifade edilmiştir.

Kurulun bir rehberinde, alternatif bir seçenek olarak, şifreleme yöntemine gidilerek anahtarı TR'de kalmakla birlikte storage'ın yurt dışında olmasının sorun olmayacağını belirttiğini, bu çözümün veri işleyene transferdeki sorunu aşmakta da kullanılabileceği bir öneri olarak dile getirilmiştir.

Mütekabiliyet olmadığı için AB'nin kabul ettiği ülkelerin otomatik olarak kabul edilmediği belirtilmiştir.108 sayılı sözleşmenin, sözleşmeye taraf devletlerarasında veri paylaşımı için bir yol sağladığı, Kurum Rehberinin 1. ve 2. kısımlarında yazanların da 108 sayılı sözleşmeyle düzenlendiği, 55 ülkenin işbu sözleşmeye taraf olduğu söylenmiştir. Bu arada artık AB'nin 223'ü esas aldığı ifade edilmiş, bu kapsamdan hareket edersek, bizimle veri paylaşacak tek ülkenin Rusya olacağı, çünkü Rusya'nın veri paylaşımı için 108 taraf olmayı yeterli gördüğü belirtilmiştir. Mütekabiliyetin ise olmazsa olmaz mı şart olup, olmadığının Kurum'a sorulması gerekeceği ifade edilmiştir.

Türkiye'nin AB ilerleme raporunun yayınladığı ve Türkiye'de KVKK olsa da hala yeterli koruma olmadığının ifade edildiği söylenmiştir. Türkiye'nin 223 sayılı Sözleşmeyi onaylayıp GDPR benzeri bir sisteme geçiş yapması gerekeceği de belirtilmiştir.

Şirketler açısından; AB'den veri almak ile AB'ye veri yollamanın farklı işlemler olduğu, veri almakta AB'nin bir çekincesi olmadığı ifade edilmiştir.

27 Mayıs kararları

Migros loyalty kartlarına ilişkin karardan ve içindeki tespitlerden bahsedilmiştir. Buna göre, rıza metninin aydınlatma metni ile örtüşmediği ifade edimiş, loyalty card üyesi olmanın hizmetin ön şartı olmadığı söylenmiştir. Tüm bu hususlarla birlikte, ceza yerine talimatlandırma yöntemine başvurulduğu vurgulanmıştır.

Migros'un rıza metninde ise birçok konuya ilişkin rızanın tek seferde alındığı söylenmiştir. Migros kararında, 0,1 TL kesintinin iade edildiği, sistemsel bir hata olduğunun söylendiği, puan silme uyarıları içeren mesajlar hakkında da rızaya ilişkin kağıtların eksik olduğu ve tedbir amaçlı alındığı yönünde bir savunma yapıldığı belirtilmiştir.

Loyalty kartlarda işleme sebebi olarak açık rızanın tercih edildiği, bunun doğru bir yol olmadığı, sözleşmenin ifasına dayandırılan bir işleme sebebi olsaydı bu karardaki ihlallerden birinin olmayacağı da söylenmiştir. Sözleşmede verilerin kimlerle ne amaçla paylaşılacağı açıklandığı ve profilleme yapılmadığı sürece, verilerin toplanmasında bir uygunsuzluk olmayacağı belirtilmiştir.

Kurumun son kararlarında varsayımsal hareket edildiği, Facebook kararının da Migros kararının da bu paralelde olduğu, yaptırım uygulanmadığı ve talimatlandırmaya dair karar verildiği şeklimde değerledirmeler iletilmiştir.

Sözleşmenin aslında veri satışına ilişkin olduğu, indirim karşılığında veri alımının gerçekleştiği, bunun zaten yapılabilir bir şey olduğu, sözleşmeye yazılıp verinin alındığı, aydınlatmanın zaten yapıldığı, ancak indirim yapılması için veriye gerek olmadığı, bu noktada sözleşmenin ifa edilmesi nedenine dayanmayıp, rıza alınmasının daha doğru olduğuna dair görüşler de iletilmiştir.

Puan kazanılabilmesi için, alışveriş verilerinin tutulması gerektiği ve bunun sözleşmenin ifası hukuki sebebine dayandırılabileceği, bunu aşan yerde profilleme söz konusuysa, kişisel reklama gidiliyorsa, açık rızanın gerekebileceği söylenmiştir. Bu doğrultuda şu şekilde bir

kriter belirlenmesi önerilmiştir; *"Puan kazanma indirim yapma sözleşmenin ifasına dayanırken profillemeye gidiliyorsa açık rıza gerekecektir"*.

Sadakat kartların işletilmesi ve dayanacağı işleme şartları konusunda ayrı bir gündem ile toplantı yapılmasının çok faydalı olacağı önerilmiştir.

Açık rızaya dayanan işlemelerde, kişinin rızasını geri aldığında şirket sisteminden çıkacağı ifade edilmiştir. Ayrıca açık rıza vermeyenlere ise sadakat hizmeti verilmeyeceği gibi bir sonucun da çıktığı vurgulanmıştır. Öte yandan açık rızanın temin edildiği sırada sakatlanmadan alınması gerektiğinin de önemli olduğunun altı çizilmiştir. Örneğin, sunulacak indirim hizmetinin aşırılığının, kişiyi gereksiz/yersiz veri paylaşımına götürmesi halinde kişinin özgür iradenin sakatlanacağı ve bu işleme faaliyetinin KVKK madde 4'teki temel ilkeler de bağdaşmayacağı belirtilmiştir.

Ziraat Bankası'na ilişkin kararda da, ceza yöntemine değil talimatlandırma yöntemine başvurulduğu ifade edilmiş, Kurul'un başvurunun kapsamıyla bağlı olup olmadığı ve şirketlere karşı yapılan başvurularda Kurul'un 11.maddeyle sınırlı olup olmadığının da bir gündem olarak başka bir toplantıda ele alınmasının yararlı olacağına değinilmiştir.

**İşbu "Kişisel Verilerin Korunması Platformu Çalışma Notları - 2" dokümanında yer alan açıklama, tanım, beyan ve görüşler, Kişisel Veriler Platformunun toplantılarına katılanların, toplantılarda belirttikleri yorum ve görüşleri ile tartışılan konular kapsamında ileri sürülen fikir ve önerilerin özetidir. Dokümanda, Platformun amacına uygun olarak, kişisel veriler ile ilgili konulara farklı açılardan bakabilmek ve tartışma zenginliğini gösterebilmek için üzerinde hemfikir olunmayan ancak, tartışılmasında fayda görülen hususlara da yer verilmiştir. Her bir konunun ele alındığı toplantının tarihine de özellikle yer verilmiştir. Zira ilgili tartışmaların tarihlerinden sonra Kurum ve Kurul'un açıklama ve/veya düzenleme yaptığı konular da mevcuttur. Bu bağlamda, işbu "Kişisel Verilerin Korunması Platformu Çalışma Notları" dokümanı ve içeriğinde yer alan notlar hiçbir resmi, idari veya özel kişi, kurum ve kuruluş adına ve bağlayıcı değildir. Burada yer alan açıklamalar üzerinden yapılabilecek işlemler ve bunların sonuçlarıyla ilgili olarak Kişisel Veriler Platformu ve Veri Koruma Derneği sorumlu tutulamaz.*