KİŞİSEL VERİLER PLATFORMU ÇALIŞMA NOTLARI

AMAÇ
TARTIŞILAN KONULAR
TOPLANTI NOTLARI,
TESPİT VE ÖNERİLER

Ocak – Haziran 2018

İçindekiler Tablosu

I. AMAÇ

Hukuksal gelişme ve uygulamaları tartışmayı önemseyen İstanbul merkezli beş değerli hukuk bürosunun girişimiyle oluşturulan ve ilk olarak 2018 yılı Ocak ayında bir araya gelen Kişisel Veriler Platformunun amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") kapsamında tespit ettiği konuları farklı disiplinlerden (bilişim, ceza, idare, medeni, borçlar, iş hukuku gibi) gelen akademisyen ve uygulamacı hukukçular ile veri güvenliği, siber güvenlik, bilişim ve yönetişim alanındaki akademisyen ve uygulamacı kişilerle derinlemesine tartışmak ve ortak bir akıl ile kişisel verilerin korunması alanındaki uygulamaların birlik ve doğruluğuna katkı sağlamaktır.

Bu amaçlarla, 2018 yılı Ocak ila Haziran ayları arasında sekiz kez toplanan Platform toplantılarını, Boğaziçi Üniversitesi Bilgi Sistemleri Uygulama ve Araştırma Merkezi ("ISRC") altındaki Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi'nde ("BUSİBER"), ISRC'nin çok değerli hocaları Prof. Dr. Meltem Özturan, Doç. Dr. Ceylan Onay Şahin ve Doç. Dr. Bilgin Metin'in de destekleriyle gerçekleştirmiştir.

Platformun ilk toplantısında KVKK kapsamında akıllara takılan hususlar ile ileride uygulamada doğabileceği düşünülen soru ve sorunlar belirlenmiştir. Devamında her ay düzenli olarak gerçekleştirilen platform toplantılarında farklı disiplinlerden gelen uygulamacı akademisyen ve hukukçular ile veri güvenliği alanındaki uygulamacı ve teknik kişiler bir araya gelerek, tespit edilen konular üzerinde detaylı tartışmalar yapmışlardır.

Kişisel Verilerin Korunması Platformu, KVKK'nın doğru ve yeknesak olarak uygulanmasına hizmet etmeyi arzulamakta, özellikle uygulamada birliğin sağlanmasını, bu nedenle de şeffaflığı önemsemektedir. Platform, bu amaçla çalışma ve faaliyetleri ile bunların sonuçlarını Kişisel Verilerin Korunması Kurulu ("Kurul") ile de paylaşmak ve Kurul'un vereceği kararların da kapsamlı olarak kamuya duyurulmasını talep etmek niyetindedir.

Platform, KVKK'nın uygulamasına öncülük edebilecek katılımcı bir çalışma ortamı yanında gerek yerel gerekse uluslararası gelişmeler hakkında toplum ve teşebbüsler nezdinde

farkındalık yaratmayı da önemsemektedir. Bu amaçla özellikle Kurum'la birlikte çalışmalar yürütmeye hazırdır.

Platformun bir amacı da KVKK uygulamalarını veri sorumluları ve veri işleyenler açısından işlevsel kılmaktır. Bu bağlamda tespit ettiği konu ve sorunları zaman zaman "sektörel" bazda ayırımlar yaparak tartışmaktadır.

II. TARTIŞILAN KONULAR

Platformun ilk toplantısının öncesinde birçok uygulamacı hukukçu ve teknik kişilere, toplantılarda gündeme getirmek istedikleri ve tartışmakta fayda gördükleri konular sorulmuş ve öne çıkanlar içinden yaklaşık 60 (altmış) adet soru belirlenmiştir. Bu sorulardan aşağıda listelenmiş olanlar, Ocak – Haziran 2018 döneminde gerçekleştirilen platform toplantılarında Kişisel Verilerin Korunması Kurumu ("Kurum") tarafından çıkarılan ikincil mevzuat ve kılavuzlar ile Kurul Kararları da dikkate alınarak, detaylı olarak tartışılmıştır. Aşağıda yer alan bilgiler, toplantılarda yapılan konuşmaları ve tartışmaları özetlemektedir. Toplantıların amaçlarından birisi kişisel veriler ile ilgili konulara farklı açılardan bakabilmek, bu konuda çalışan hukukçulardan değişik fikirler de alabilmek olduğundan, tartışma zenginliğini gösterebilmesi açısından üzerinde hemfikir olunmayan ancak tartışılmasında fayda görülen noktalara da aşağıda yer verilmiştir. Konuların hangi tarihte tartışıldığına da özellikle yer verilmiştir. İlgili tartışmaların tarihinden sonra Kurum ve Kurul'un açıklama yaptığı konular da mevcuttur.

1. **Açık rıza kapsamında değerlendirmeler; Avrupa Birliği uygulamalarıyla karşılaştırmalı olarak "rızanın geri çekilmesi", "rıza kirliliği".**
2. Kişisel verilerin yurtdışına aktarılması ve uygulamadaki sorunlar.
3. Kişisel Veri Güvenliği Rehberi ve Özel Nitelikli Verilerin İşlenmesinde alınması gereken yeterli önlemlere dair 30.01.2018 tarih ve 2018/10 sayılı Karar ışığında veri güvenliğine dair teknik değerlendirmeler, uygulama ve sorunlar.
4. **Silme, yok etme ve anonimleştirme başlıkları altında çeşitli konular.**
5. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar hakkında Tebliğ Madde 5/1 (c) hükmü kapsamında aydınlatma yükümlülüğünün farklı birimler nezdinde yerine getirilmesi meselesi.

6. **Aydınlatmanın geçerliliği sorunu ile eksik ya da hatalı aydınlatmanın sonuçlarının değerlendirilmesi dahil aydınlatma yükümlülüğünün yerine getirilmesine dair çeşitli meseleler.**
7. Veri Sorumlusuna Başvuru Tebliği kapsamında pratikte karşılaşılması olası sorunlar.
8. **KVKK madde 5/2 kapsamında kişisel veri işleme şartlarının 95/46 sayılı Direktif ve General Data Protection Regulation ("GDPR") ile birlikte değerlendirilmesi, açık rıza dışındaki hukuka uygunluk sebepleri, özel nitelikli kişisel veriler yönünden değerlendirme.**
9. **Veri saklama ve imha sürelerine dair genel prensiplerin neler olması gerektiği.**
10. Anayasa Mahkemesinin 2016/125 Esas 2017/143 Karar sayılı ve 28.09.2017 tarihli Kararı ile Kurul'un Uygulama Rehberi çerçevesinde "açık rıza" meselesinin detaylı olarak ele alınması. Bu bağlamda; "battaniye rıza", "rıza kirliliği", "yanıltıcı rıza", "geçersiz rıza" ve "gereksiz rıza" kavramlarının tanımlanması ve genel yaklaşımın nasıl olması gerekeceği.
11. **Açık rızanın hizmetin ön şartı olması halinin Kurum'un yayınladığı özet kararlar ışığında değerlendirilmesi; *e-ticaret uygulamaları açısından tespit ve değerlendirmeler.***
12. GDPR'ın Türkiye'ye etkileri üzerine ve uygulamada ortaya çıkan sorunlara dair KVKK ve GDPR karşılaştırmalı değerlendirme.

III. TARTIŞILAN KONULARA DAİR TOPLANTI NOTLARI, TESPİT VE ÖNERİLER

1. Açık Rıza Kapsamında Değerlendirmeler; Avrupa Birliği uygulamalarıyla karşılaştırmalı olarak "geçersiz rıza", "rızanın geri çekilmesi", "rıza kirliliği"

ÖZET: Konu 23 Şubat 2018 tarihli Platform toplantısında ele alınmıştır. Açık rıza ve KVKK'da sayılan diğer kişisel verilerin işlenme şartlarının, hiyerarşik olarak birbirlerine karşı üstün olmadıklarının kabulü ile KVKK madde 5/2'ye göre hukuka uygun bir işleme nedeni varken, KVKK kapsamında doğru yapılmış bir aydınlatma ardından açık rıza da alınmışsa, alınan rızanın "geçersiz" sayılmayabileceği ve rızanın geri çekilmesi halinde ise,

veri işlemenin dayandığı diğer hukuka uygunluk sebebi uyarınca veri işlemenin devam edebileceği olasılıkları tartışılmıştır.

Kişisel verilerin KVKK madde 5/2'de yer alan bir nedene dayalı olarak işlendiği hallerde, veri sahibinden verisini işlemek için açık rıza da alınmışsa, alınan rızanın geçerli olup olmayacağı ve rızanın geri çekilmesi halinde, veri işlemeye devam edilip edilemeyeceği pratikte sıkça tartışılmaktadır. KVKK madde 5/2'de yer alan bir kişisel veri işleme nedeninin varlığı halinde, madde 5/1'e göre rıza alınmamalı mıdır?

Öncelikle söz konusu tartışmanın, Article 29 Data Protection Working Party tarafından rızaya ilişkin olarak verilmiş 2011 tarihli bir kararından ve bu karardan doğan "rıza kirliliği" kavramından kaynaklandığı düşünülmektedir. Anılan kararda, rıza haricindeki diğer hukuka uygun işleme nedenlerinden birine dayanılarak veri işlendiği, ancak yine de açık rızanın alındığı bir durumda, söz konusu rızanın geçerliliğinin tartışılabilir hale geleceği ifade edilmektedir. Kararda böyle bir durumda alınan rızanın ilgili kişiyi yanıltıcı bir niteliğe sahip olacağı ifade edilmektedir.

Nitekim Kurum'un, "Kişisel Verilerin Korunması Kanunu'nun Uygulanmasına Yönelik Soru ve Cevaplar" kılavuzunun, "açık rıza geri alınabilir mi?" biçimindeki 11 numaralı soruya cevabında, "veri işleme faaliyeti diğer kişisel veri işleme şartlarına dayanıyorsa bu faaliyet için açık rızaya gidilmemelidir. Eğer faaliyetin gerçekleştirilme amacı Kanun'daki açık rıza dışındaki diğer kişisel veri işleme şartlarını karşılamıyorsa, bu faaliyet özelinde ve o faaliyetle sınırlı olarak açık rıza alınmalıdır" ifadesine yer verilmektedir. Dolayısıyla Kurum'un, diğer işleme nedenleri varsa, açık rızaya gidilmemesi gerektiği görüşünü benimsediği anlaşılmaktadır. Kurum'un bu görüşü, Kurum yetkililerince, katıldıkları etkinliklerde de vurgulanmakta ve bu durumda "rıza kirliliği" yaratılmış olunacağı belirtilmektedir.

Öte yandan, veri sorumlusunun veri envanterini oluştururken, hangi veriyi hangi amaçla ve hangi işleme şartına dayanarak işlediğini bilmesi ve yansıtması, veri işlemenin salt genel nitelikli bir rızaya dayandırılmaması beklenmektedir.

Ancak, KVKK'nın lafzına, başka bir deyişle yazım tekniğine bakıldığında, gerek Kurum'un yukarıda belirtilen yaklaşımından gerekse mehaz 95/46 sayılı AB Direktifi'nin 7. Maddesi'nden farklı olarak - Direktif'te rıza diğer tüm işleme nedenleri ile aynı seviyede

tutulmuştur - KVKK'nın 5. Maddesi'nin yazılımından açık rıza almanın asıl kural, diğer kişisel veri işleme şartlarının açık rıza almanın istisnası olarak yazıldığı sonucuna varmak da mümkündür. Zira Anayasa Mahkemesi'nin 2016/125 Esas, 2017/143 Karar sayılı ve 28.09.2017 tarihli Kararında değerlendirmenin bu yönde yapıldığı görülmektedir.

Bu bağlamda, Kurum'un rehberlerinde ve farklı etkinliklerde açıklamış olduğu *"veri işleme faaliyeti diğer kişisel veri işleme şartlarına dayanıyorsa bu faaliyet için açık rızaya gidilmemelidir*" görüşü çerçevesinde gündemde olan "rıza kirliliği", "yanıltıcı rıza" ve "rızanın geçersizliği" yönündeki tartışmaları, Anayasa'nın 20. Maddesi ve KVKK'nın lafzını da dikkate alarak değerlendirmenin daha sağlıklı olacağı konuşulmuştur.. Zira yukarıda da atfedilen Anayasa Mahkemesi Kararı'nda (kararın 42. Paragrafı) *"...açık rızaya getirilen istisnaların, esas kural haline getirildiği veya açık rızaya ihtiyaç duyulmasını imkansız hale getirdiği söylenemez"* ve *"...bir başka deyişle, dava konusu kurallar, maddede belirtilen konularda gereklilik veya zorunluluk halinde ortaya çıkabilecek bir ihtiyacın karşılanmasına yönelik olup, hakkın özüne dokunmamaktadır"* denmiştir.

Ceza hukuku ilkeleri uyarınca da, KVKK'da sayılan veri işleme şartlarının arasında bir hiyerarşi olmaması gerektiği savunulmakta ve diğer hukuka uygunluk sebeplerinin varlığı halinde alınan rızanın "geçersiz" değil, yalnızca "gereksiz" olabileceği ifade edilmektedir. Bu bağlamda, veri işlerken bir hukuka uygunluk sebebinin varlığı yanında rıza da alınmış ise, o rıza geri çekilse dahi ilgili hukuka uygunluk sebebi kapsamında kişisel verilerin işlenmeye devam edilebileceği belirtilmektedir.

Sonuç olarak, hukuka uygunluk nedenleri arasında bir hiyerarşi bulunmaması gerektiği ve başka bir hukuka uygunluk nedeninin yanında alınan açık rızanın geri çekilmesi halinde veri işlemenin, asıl olarak dayandığı hukuka uygunluk sebebi uyarınca devam edebileceği ve böyle bir durumda alınan açık rızanın "geçersiz" olarak nitelendirilmemesi gerektiği gerektiğinin savunulabileceği konuşulmuştur. Geçersizliğin ciddi sonuçları olan bir durum olduğu, rıza ile başka bir hukuka uygunluk sebebinin birlikte yer aldığı her durumda rızaya geçersiz denmemesi gerektiği ve her olayın kendi içerisinde ayrı ayrı incelenmesi gerektiği konusunda görüşler iletilmiştir. Veri sahibinin baştan tam ve doğru bir şekilde aydınlatılmış olması ve verisinin hangi amaçlarla ve hangi veri işleme şartlarına dayanılarak işleneceğini biliyor olması ise tabii ki şarttır.

Bunun yanında, Anayasa Mahkemesinin kararı ve KVKK'nın yazım tekniği de dikkate alındığında, Türk mahkemeleri, savcılar veya denetim görevini üstlenecek olan kişilerin de bu hususta nasıl bir yaklaşım içinde olacakları önemlidir, zira KVKK'nın uygulaması tüm paydaşlarla birlikte gelişecektir.

2. Kişisel Verilerin Yurtdışına Aktarılması ve Uygulamadaki Sorular / Sorunlar

ÖZET: Konu 23 Şubat 2018 tarihli Platform toplantısında ele alınmıştır. Kişisel verilerin yurtdışına aktarılması hususunda en önemli sorunlardan biri yeterli korumanın bulunduğu ülkelerin henüz ilan edilmemiş olmasıdır. Bu listenin ne zaman açıklanacağının hâlihazırda varsayılabilir olmadığından hareketle, listenin ilanına kadar yurtdışına aktarım için uygulamada rıza alınması yoluna başvurulmaktadır. Doğru uygulamaların gelişmesi açısından yeterli korumanın bulunduğu ülkelerin ilan edilmesi, bunun yanı sıra Kurum'un bulut hizmet sunucularında tutulan kişisel veriler yönünden görüşlerini bildirmesi önemlidir.

Kişisel verilerin yurtdışına aktarılması başlığı altında, yeterli korumanın bulunduğu ülkeler henüz ilan edilmemekle birlikte, Kurum'un bu konuda sözlü olarak karşılıklılık ilkesini uygulayacağına dair açıklamaları bulunmaktadır. Bununla birlikte, Platformdaki tartışmalarda, listenin ne zaman açıklanacağının hâlihazırda varsayılabilir olmadığı ve bu nedenle listenin ilanına kadar, yurtdışına aktarım için rıza yoluna başvurulması gerektiği konularında hemfikir olunmuştur.

Bu kapsamda, hangi işlemlerin yurtdışına veri aktarımı olarak kabul edileceği / edilmesi gerekeceği de önemli bir konudur. Örneğin, uluslararası şirketlerin çeşitli birimlerinin yurtdışından yönetildiği ve ilgili birimlere ilişkin tüm verilerin yurtdışında tutulduğu veya şirket serverlarının yurtdışında bulunduğu uygulamalar günümüzde oldukça fazladır. halihazırda, uygulamada şirketlere yurt dışına aktardıkları tüm veriler için rıza almaları veya serverlarını yurt içinde tutmalarını önermek tercih edilse de, bu tür önerilerin uygulamada pratik, hızlı ve tam olarak gerçekleştirilebilir olmayacağı veya rızanın geri çekilmesi halinde sorunlara yol açabileceği de açıktır. Uygulamada karşılaşılacak zorlukları düşünerek,

uluslararası şirketlerin burada belirtilen şekildeki veri aktarımları için farklı bir yaklaşım getirmek faydalı olacaktır.

Öte yandan, yeterli korumanın bulunduğu ülkeler listesi yayımlansa dahi, bulut hizmet sunucularının genellikle verileri birden çok ülkede tuttukları ve verilerinin yedeklemesini çeşitli ülkelerde yaptıkları göz önünde bulundurulursa, yayımlanan listenin bu noktada yetersiz kalma ihtimali bulunmaktadır. Buna karşılık olarak, sorunun, şirketlerin hizmet sunucularıyla yapacakları sözleşmelere koyacakları hükümler aracılığıyla, verilerin yedekleneceği ülkeleri kısıtlamaları yoluyla çözebilecekleri düşünülebilir. Ancak bu şekilde bir çözüm veri sorumluları açısından ciddi maliyetler doğurabilecektir. Kaldı ki bulut hizmet sunucularının çoğu kendi standartları ile hareket etmektedir ve bunlardan bazılarının sözleşmeleri müzakere etmeye kapalı olması da uygulamada sorunlara yol açabilecektir.

Kurum'un bulut çözümlerine ilişkin yaklaşımı henüz belirli değildir. Ancak, şu ana kadar çeşitli konularda uygulamaya vermiş olduğu yön dikkate alınacak olursa, Kurum'un, büyük olasılıkla bulut hizmet sağlayıcıları aracılığıyla işlenen verileri, yurtdışına aktarım kapsamında değerlendireceğini düşünüyoruz.

Bunların yanı sıra Platformdaki tartışmalarda, bir verinin bulutta tutuluyor olmasının oldukça güvenli bir yöntem olduğuna, bu konuda yapılacak düzenlemelerin uygulamaya olan etkisine dikkat edilmesi gerektiğine, aksi halde Türkiye'nin dijital gelişimine ve ticaretine engel olunacağına da değinilmiştir.

Ceza hukuku açısından konuya bakıldığında, buluta aktarılan bir verinin yurtdışında kabul edildiği bir halde, herhangi bir suç soruşturmasında, ilgili veriye erişerek soruşturma yürütülmesi için bulut sunucularının bulunduğu ülkeden adli yardımlaşma talebinde de bulunulması gerekebileceği hakkında görüşler ileri sürülmüştür. Verinin yurtdışındaki sunucuda da olsa Türkiye'deki bir bilgisayardan verilecek bir komutla saniyeler içerisinde çekilebilecek olması halinde de verinin yurtdışında olduğunun kabul edilmesi halinde, ilgili verinin soruşturma kapsamında elde edilebilmesi için ciddi bir maliyet ve zaman kaybı riski doğacağı konusuna da değinilmiştir.

Yabancı bir denetim makamının (Avrupa ülkeleri veya Amerikan makamları incelenebilir) bugüne kadar herhangi bir hizmet sunucusunun server veya kullandığı yöntemi için "güvenli"

olduğuna ilişkin bir kararının var olup olmadığının araştırılmasının faydalı olabileceği düşünülmüştür. Nitekim böyle bir tespit Kurum için de yararlı olabilir, benzer bir yaklaşım Kurum'a da önerilebilir.

3. Kişisel Veri Güvenliği Rehberi ve Özel Nitelikli Verilerin İşlenmesinde Alınması Gereken Yeterli Önlemlere Dair 30.01.2018 tarih ve 2018/10 sayılı Karar Işığında Veri Güvenliğine Dair Teknik Değerlendirmeler, Uygulama ve Sorunlar

ÖZET: Konu 16 Mart 2018 tarihli Platform toplantısında ele alınmıştır. Kişisel verilerin işlenmesi süreklilik arz eden bir "süreç yönetimidir" ve konunun "veri güvenliğine dair teknik boyutu" en az KVKK'ya hukuki belgeler ve altyapı bazında uyum sağlamış olmak kadar önemlidir. Bu bağlamda, veri güvenliğinin temini için veri sorumlularının "standart politikalar" oluşturmaları ve bu politikalar aracılığıyla gerekli planlamaları yapıp, önlemler almaları gereklidir.

KVKK'nın, siber güvenlik önlemlerinin kullanılmasını zorunlu hale getirdiği ve "kriptoloji" kavramının ön plana çıktığı görülmektedir. KVKK'nın, verilerin şifrelenerek saklanması gerektiğine ilişkin atfı ve verilerin silinmesi noktasında kriptolojinin işlevsel bir yöntem olarak kabul edildiğine dikkat edilmelidir.

Veri sorumluları, "güvenli ağlar" temin etmelidir. Güvenli ağ için teknik ve idari tedbirler bir arada düşülmelidir, teknik tedbirlerden en önemlisi, ağlara erişimin güvenlik duvarları ile engellenmesi olacaktır.

Veri güvenliğinin sürekli temini için belli bir güvenlik tedbiri yönteminin kullanılması da yeterli olmayacak, mutlaka güncel tutulması gerekecektir. Bunun yanı sıra, veri sorumlularının, dönem dönem sızma testleri ve her ay bir kere yedekleme testi yaptırmaları tavsiye edilmektedir.

BÜSİBER'den Doç. Dr. Bilgin Metin tarafından konuya dair teknik açıklama ve değerlendirmeler ile BÜSİBER'in KVKK'ya uyum çerçevesinde yürütmekte olduğu projelere ve kişisel verilerin güvenliğine ilişkin teknik bilgilere yer verilen Platform toplantısında,

kişisel veri işlemenin süreklilik arz eden bir "süreç yönetimi" olduğu ve konunun "veri güvenliğine dair teknik boyutunun" en az KVKK'ya hukuki belge ve altyapı bazında uyum kadar önem taşıdığının altı çizilmiştir. Bu kapsamda BÜSİBER'de veri güvenliğine ilişkin eğitim kampları düzenlemekte ve kamuya yönelik adli bilişim ve siber güvenlik eğitimleri verilmekte, siber güvenlikte yerli çözümler desteklenmektedir.

Veri güvenliğinin teknik açıdan da sağlanmasının önemine dikkat çekebilmek adına, Platform toplantısı sırasında yapılan demonstrasyonda, Android telefonlara Google Play Store dışından indirilerek kurulan uygulamaların, içerdikleri zararlı yazılımlar aracılığıyla ilgili kişiden habersiz olarak kamera görüntüsü, ekran görüntüsü ve ses kaydı alabildiği gösterilmiş ve veri güvenliğinin sağlanması için temel anti-virüs programları kullanmanın önemi vurgulanmıştır. Bu bağlamda, özellikle keylogger durduran anti-virüs programlarının seçilmesinin gerektiği belirtilmiştir. Veri güvenliğinin sürekli temini için belli bir güvenlik tedbiri yönteminin kullanılmasının yeterli olmayacağı, mutlaka güncel tutulması gerektiği ifade edilerek, VPN kullanılması gerekliliğinin de altı çizilmiştir.

Veri güvenliği için önemli bir husus da veri sorumlularının "standart politikalar" oluşturmaları ve bu politikalar aracılığıyla gerekli planlamaları yapıp, önlemleri almalarıdır. Bu noktadan hareketle, KVKK'nın siber güvenlik önlemlerinin kullanılmasını zorunlu hale getirdiği ve bu önlemlerden bir tanesinin de "kriptoloji" olduğu görülmektedir. Bu bağlamda, KVKK'nın, verilerin şifrelenerek saklanması gerektiğine ilişkin atfına ve verilerin silinmesi noktasında kriptolojinin işlevsel bir yöntem olarak kabul edildiğine dikkat edilmelidir. Kriptoloji veri güvenliği için önemli bir kavramdır. Veri sorumluları nezdinde özellikle veri güvenliğinden sorumlu olacak kişilerin, kriptolojiye hakim olmaları gerekecektir.

Öte yandan veri sorumluları, politikalarında "güvenli ağlar"ın sağlanmasını temin etmelidir. Güvenli ağ için teknik ve idari tedbirler bir arada düşünülmelidir, teknik tedbirlerden en önemlisinin, ağlara erişimin güvenlik duvarları ile engellenmesi olduğu belirtilmiştir.

Veri güvenliği için veriye fiziksel erişim de göz ardı edilememeli ve üzerinde azami kontrol sağlanmalıdır. Bu bağlamda, fiziksel erişim kontrolü, iki yollu kimlik doğrulama sistemlerinde olduğu gibi çift aşamalı olarak sağlanabilecektir.

Güvenlik cihazlarının kullanımının da verilerin korunması için bir diğer önemli adım olduğu açıktır ve bu doğrultuda "Unified Threat Management (UTM)" olarak adlandırılan firewall cihazlarının etkin bir koruma sağlayacağı belirtilmiştir. Bu cihazların maliyet açısından da birbirinden farklı seçeneklerinin olduğu ve böylece çok güçlü güvenlik önlemleri almasına gerek olmayan bir KOBİ'nin de kendine uygun ve daha az maliyetli bir UTM cihazı ile gerekli tedbiri alması mümkündür.

Veri güvenliğine dair önlemlerden bir diğeri de verilerin tutulmakta olduğu cihazların düzenli olarak güncellenmesidir. Bunun yanı sıra, uygulama güvenliğinin sağlanması sistem güvenliğinin sağlanması kadar önemlidir ve veri sorumlularının kurulu olan uygulamalarını da düzenli olarak güncellemesi gerekmektedir. Bu bağlamda, Windows kullanan bilgisayarlara ücretsiz kurulabilecek Microsoft WSUS yazılımıyla bilgisayarlardaki güncellemelerin rahatlıkla sağlanabileceği belirtilmiştir.

Bunlarla birlikte, olası tehditler karşısında riski azaltmak için belirtilen tedbirleri almanın yanı sıra, dönem dönem sızma testleri ve her ay bir kere de yedekleme testi yapılması tavsiyeler arasında sayılmıştır.

Özellikle bankacılık sektöründe kullanılan çift taraflı kimlik doğrulama sisteminin, Türk mevzuatında yeterli bir tedbir olarak kabul edilse de, yurtdışında yeterli görülmediği belirtilmiştir. Google Authenticator kimlik doğrulama için uygun bir sistem olabilir.

Kişisel verilerin korunması ve güvenliğine ilişkin uyum süreçlerinin, hukuki ve teknik tedbirlerin alınması ve gerekli teknik ürünlerin satın alınması gibi fazlara bölündüğü ve veri sorumlularının söz konusu hizmetleri bu alanlarda uzman profesyonel hizmet sağlayıcılardan satın aldığı bilinmektedir. Bazı veri sorumluları bu süreçte ISO 27001 gibi sertifikasyonlardan da geçmektedir. Bununla birlikte, Kurum'un bu tür hizmet sağlayıcıları tabii tuttuğu bir akreditasyon veya tavsiye listesi yoktur. Pratikte sıkça rastlanan bir soru olduğu için, Kurum'a ileriye yönelik olarak denetim konusunda yetkilendirilmiş kuruluşları belirlemeye yönelik bir eğiliminin olup olmayacağı sorulabilir. Ancak, bir yandan, veri sorumlularının veri güvenliğine ilişkin almış oldukları önlemlerin akredite edilmelerinin işlevsel olmayacağını düşünmek de gerekir, zira belirlenecek bir denetim kuruluşu tarafından akredite edilmiş olan bir veri sorumlusunun, bu noktadan sonra herhangi bir cezaya tabi kılınmasının önüne geçilmesi hukuki ve pratik açıdan gerçekçi değildir. Platformun bu bağlamdaki tartışmaları

esnasında, veri güvenliğinin denetimi açısından, yeminli mali müşavirlerin yaptığı "tam tasdik" işlemi gibi bir uygulamanın örneklenebileceği, bu suretle denetlenen veri sorumlularının Kurum'un kontrolünden muaf tutulmaksızın denetim firması ile beraber ortak bir sorumluluk taşıyabileceğine dair bazı görüşler bildirilmiştir.

4. Silme, Yok Etme ve Anonimleştirme Başlıkları Altında Çeşitli Konular

ÖZET: Konu 16 Mart 2018 tarihli Platform toplantısında ele alınmıştır. Veri sorumlusu olan kurumlar çoğunlukla "yedekleme" yapmakta ve bu işlem silinen veya yok edilen veriler yönünden geri döndürülme ihtimalini açık tutmaktadır. Diğer yandan bir veri setinin anonimleştirilmiş sayılabilmesi için her safhada anonimleşmiş olmasının gerektiği düşünülmekte, ancak herhangi bir kişiye işaret etmeyecek bir veri setinin, aktarıldığı kişinin elinde olan verilerle birleştiğinde kimliği belirli veya belirlenebilir bir kişiye işaret etme olasılığı varken, anonimleştirmenin tüm safhalarda temin edilmesi mümkün olmayacaktır. Bu noktalardan hareketle, kişisel verilerin korunması kapsamında veri sorumlusundan bu aşamada beklenen temel yükümlülük, riski en aza indirmesi ve bunun için iyi niyetli bir çaba içinde hareket ettiğini ispat etmesi olmalıdır.

Kişisel verinin saklaması, silinmesi ve yok edilmesi işlemleri ile sınırlı olmaksızın tüm veri işleme faaliyetleri yönünden veri sorumluları bünyesindeki "ilgili kullanıcılar" eğitilmeli, tüm çalışanlar nezdinde genel farkındalık yaratılmalıdır. Bu bağlamda ve sektörel ayırım gözetilmeksizin tüm veri sorumluları yönünden özellikle bilgi teknolojisi ve insan kaynakları birimlerinin çalışanlarının doğru yönlendirilmeleri önemlidir.

Veri imha süreleri ve gizlilik dereceleri veri kategorileri bazında ele alınmalıdır. Kurum'un saklama sürelerine ilişkin olarak, açıkça - rakamsal olarak - belirlenmiş süreler görmek isteyip istemeyeceğinin anlaşılması ve bununla birlikte pratikte ortaya çıkması muhtemel sorunları aşmak için, belirlenen sürelerin "aşırı" olmamasının yeterli olacağı düşüncesiyle hareket edilmesi faydalı olacağı değerlendirilmiştir.

İlk olarak kişisel verilerin yedeklenmesi işleminin silme ve yok etme kapsamındaki önemine dikkat çekilmiş ve kritik durumlarda yedekten geri dönme söz konusu olduğunda, silinmiş

olan bir kişisel verinin de veri sorumlusuna geri döneceği belirtilmiştir. Bu bağlamda, yedeklenen kişisel verilerin, yok etme işlemi ardından veri sorumlusuna geri dönmesinin önüne geçmek için düzenli test ve denetimler yapılması tavsiye edilmiştir. Ancak, düzenli denetimlerin maliyetleri küçük ve orta ölçekli işletmeleri olan veri sorumluları için ilave külfetler doğurabilecektir. Bu noktadan hareketle, kişisel verilerin korunması kapsamında veri sorumlusundan bu aşamada beklenen temel yükümlülüğün aslen riski en aza indirmesi ve bunun için iyi niyetli bir çaba içinde hareket ettiğini ispat etmesi olduğu vurgulanmıştır. Nitekim konunun teknik boyutuna bakıldığında, bir verinin tamamen silinmesi mümkün olmayacak, daha doğru bir deyişle silinen verilerin geri döndürülmesi riski her zaman bulunacaktır. Riskin azaltılabilmesi için iş sağlığı ve güvenliği uygulamasında olduğu gibi, veri sorumlularının işlemekte oldukları veri tabanlarının da kategorilere ayrılabileceği ve alınması gereken güvenlik önlemlerinin orantılı olarak farklı olabileceği yönünde bir öneri getirilmiştir. İlerleyen aşamalarda veri sorumlularından, işledikleri kişisel verilerin niteliği ve önemini göz önünde bulundurarak güvenlik tedbirleri almaları beklenebilecektir. Bu kapsamda Kurum'un ilerleyen aşamalarda sektörel fragmantasyona gitmesi de sözkonusu olabilir.

Silme işlemi kapsamında tartışılan bir diğer husus ise, KVKK madde 7'deki düzenleme ile Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") arasındaki ifade farkıdır. KVKK madde 7'de verilerin veri sorumlusu tarafından silineceğinden bahsedilirken, Yönetmelik'te "ilgili kullanıcı" tanımına yer verilmiş ve ilgili kullanıcıların veriye erişiminin engellenmesi ile silmenin gerçekleşeceği belirtilmiştir. Bu durumda, bir veri sorumlusunun depolamadan sorumlu olan teknik birimi haricindeki kişilerin veriye erişiminin engellenmesi ile veri silme gerçekleşmiş olacaktır. Ancak KVKK veya Türk Ceza Kanunu'nda bu şekilde bir ayırım yapılmadığından, Yönetmelik'te yazılı "ilgili kullanıcıların" ifadesinin tanımlanmış olan bir suçun daraltılması anlamına gelmekte olduğu da ifade edilmiştir. Fakat Türk Ceza Kanunu'nda belirlenen suçlar hakkında genişletme veya daraltma yapılması mümkün olmayacağından, söz konusu ifadenin hakime en fazla bir yorum aracı olarak tutulabileceği, bununla birlikte eylemin "suç" niteliğinde bir değişiklik olmayacağı belirtilmiştir.

Platformdaki tartışmalar esnasında şifreleme anahtarının saklanması veya elinde bulunduran kişilerin sınırlandırılması gibi uygulamaların pratikte ne kadar yapıldığı sorusu gündeme geldiğinde, bilgi teknoloji birimlerinin genellikle her türlü veriye erişiminin bulunduğu ve

şifreleme anahtarını elinde bulunduran kişi sınırlandırılmasının, hâlihazırda uygulama alanı bulmadığına dikkat çekilmiştir. Bunun yanında, bilgi teknoloji birimlerinin veriye ne ölçüde erişebileceğinin esasında yönetim tarafından belirlendiği de düşünülürse, görevler ayrılığı ilkesi uyarınca veri sorumlularının, sistemde kimin hangi veriye eriştiğine ilişkin loglama yapmasının gerekli olduğu ifade edilmiştir.

Kişisel verilerin güvenli bir şekilde işlenmesinin tesisi amacıyla veri sorumlularının, ilgili kullanıcıların yanı sıra tüm çalışanları nezdinde farkındalık yaratması yukarıda tartışılanlar kapsamında da önemlidir ve özellikle bilgi teknolojileri ile insan kaynakları birimlerine eğitimler verilmesi faydalı olacaktır. Yine uygulamada özel nitelikli kişisel veri veya hassas veri işleyen çalışanlara gizlilik taahhütleri imzalatmak, sisteme giriş çıkışların belirli saatler dışında yapılmasını engellemek, herkesin sisteme giriş yapamaması, gerekirse şifrelerin fiziksel olarak bir kasada saklanması gibi tedbirlere de başvurulduğu ve bunların da makul tedbirler olarak kabul edilmesi gerektiği belirtilmiştir.

Alınacak tedbirlerin maliyeti gündeme geldiğinde, risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatiflerinin maliyetlerine karşın faydalarını değerlendirirken, sadece veri sorumlusunun karşılaşacağı idari para cezalarının değil, işin adli bilişim kısmının da dikkate alınması gerektiği hatırlatılmıştır. Nitekim bir ihlalin incelenmesi noktasında, veri sorumlusunun ana serverına el konarak inceleme yapılması muhtemeldir. Öte yandan ihlallerin ceza hukuku ve özel hukuk sonuçları olabileceği de göz ardı edilmemelidir.

Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler kararında yer alan “gizlilik dereceli belgeler” ifadesinden ne anlaşılması gerektiği de bir diğer soru olarak gündeme gelmiştir. Buna cevaben sektörden sektöre değişebilecek, halka açık belgeler, şirket içi belgeler ve gizli belgeler şeklinde sınıflandırmanın veya erişebilecek kişi grubuna göre sınıflandırmanın yapılabileceği belirtilmiştir. Söz konusu karar uyarınca verilerin “fiziki ortamda” aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerektiği ifade edilmiştir.

Bir veri setinin anonim olduğunun kabul edilmesi için hangi koşulların yerine getirilmesi gerektiği bağlamındaki tartışmada, herhangi bir kişiye işaret etmeyecek bir veri seti, aktarıldığı kişinin elinde olan verilerle birleştiğinde kimliği belirli veya belirlenebilir bir

kişiye işaret eder hale geliyorsa, söz konusu veri setinin de anonim kabul edilemeyeceği belirtilmiştir. Zira kişisel verilerin her safhada anonim olması gerektiği vurgulanmıştır. Bu bağlamda, "big data" kavramı ile birlikte düşünüldüğünde herhangi bir verinin anonimleştirilmesinin neredeyse imkansız hale geleceği, nitekim Google Analytics gibi kurumların, bu tür veri havuzlarını kullanarak olağan akışta asla eşleştirilemez kabul edilebilecek verileri dahi eşleştirebildikleri belirtilmiştir. Anonimleştirme konusunda objektif yaklaşımın mı sübjektif yaklaşımın mı kabul edilmesi gerektiği de tartışılmıştır. Bir veri setinin herhangi bir üçüncü kişinin elindeki bir veriyle eşleştiğinde belirli bir kişiye işaret ediyor olması halinde söz konusu veri setine kişisel veri diyen görüşün objektif yaklaşım olduğu belirtilmiştir. Buna karşılık, bir veri setinin ancak aktarılması muhtemel kişilerin elinde olması muhtemel olan veya makul bir çaba ile elde edebileceği diğer verilerle birleştiğinde ilgili kişiye işaret ettiği durumlarda ilgili veri setine "kişisel veri" diyen görüşün sübjektif yaklaşım olduğu belirtilmiştir. Subjektif yaklaşımın günümüz gerçeklerine daha uygun bir yaklaşım olduğu konuşulmuştur Bu noktadan hareketle, Kurum'un veri sorumlusundan beklentisi, veriyi tamamen geri getirilemeyecek şekilde anonim hale getirmek değil, veri işlemenin her safhasında ve veriyi anonimleştirirken de makul tüm tedbirleri almak olmalıdır.

Azami muhafaza sürelerinin belirlenmesi ve bazı veri tabanları açısından (örneğin özlük dosyası tutulması gibi) benimsenecek imha politikaları içinse, ikili değerlendirme yapmak faydalı olacaktır; örneğin, çalışanların sağlık verileri için farklı, genel nitelikli veriler için farklı azami muhafaza süreleri tespit edilebilir. Bu kapsamda, Avrupa uygulamasında olduğu gibi "employment privacy notice" metodunun mümkün olup olmayacağı, Kurum'un herhalde mutlaka saklama sürelerine ilişkin net süreler görmek isteyip istemeyeceği gündeme gelmiştir. Bu soruya cevaben, süreç bazlı süre belirlenmesi noktasında karışıklıkların ortaya çıkmasının oldukça muhtemel olduğu, bu nedenle belirlenen sürelerin "aşırı" olmamasının yeterli görülmesi faydalı olacaktır.

5. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ Madde 5/1 (c) Hükmü Kapsamında Aydınlatma Yükümlülüğünün Farklı Birimler Nezdinde Yerine Getirilmesi Meselesi

ÖZET: Konu 29 Mart 2018 tarihli Platform toplantısında ele alınmıştır. "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5/1(c) hükmünde yer alan "Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir." cümlesinde geçen "birim" ve "nezdinde" ifadeleri uygulama açısından sıkıntılar yaratabilecektir. Bu bağlamda söz konusu ifadelerin ne anlama geldiği veya nasıl yorumlanması gerektiği konusunun Kurul tarafından bir ilke kararı ile açıklığa kavuşturulmasına ihtiyaç vardır. Veri işleme amacı değişmedikçe, veri sorumlusunun, aynı aydınlatma metni içinde veriyi işleyen her bir birimini sayması ve verinin hangi birimde hangi amaçla işleneceğini belirtmesi KVKK'nın lafzı ve amacı da gözetildiğinde, yeterli kabul edilmelidir.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de ("Tebliğ") yer alan ve tartışılması gereken en önemli hususlarda biri, Tebliğ'in madde 5/1(c) hükmüdür. İlgili maddeye göre;

"Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir."

İlgili madde kapsamında açıklığa kavuşturulması gereken hususlardan biri, "birim" kavramından ne anlaşılması gerektiğidir. Zira "birim" kavramının tanımına KVKK'da yer verilmemiştir. Tebliğ'in içeriğinden "birim" ile şirket departmanlarının (insan kaynakları, bilgi teknolojileri gibi) kastedildiği anlaşılmaktaysa da, tanım KVKK'da yoktur. Öte yandan, "birim" ifadesine ilişkin olarak genellikle ticari şirketler açısından yorumlar yapılmaktadır. Ancak KVKK'nın yalnızca şirketleri değil, devlet kuruluşları ve idari kurumları da kapsadığı düşünüldüğünde, bu tür kurumlara da uygulanabilir bir tanıma ihtiyaç vardır.

İlgili maddede açıklığa kavuşturulmasına ihtiyaç duyulan bir diğer husus ise, "nezdinde" ifadesinden ne kastedilmekte olduğudur. Nitekim bu ifadenin anlamının muğlak olduğu ve "her birimin ayrı bir bilgilendirme yapma yükümlülüğü" veya "yapılacak tek bilgilendirmede her bir birimin isminin ayrıca geçirilmesi yükümlülüğü" şeklinde farklı yorumlanmaya açık olduğuna dikkat çekilmiştir. Veri sahibine, kişisel verisinin hangi birim tarafından hangi amaçla işleneceğinin bildirilmesi, aydınlatma yükümlülüğünün doğru bir şekilde yerine getirilmesi için gerekli olmakla birlikte, bu işlemin tek bir doküman içinde yapılması mümkündür ve sürecin yönetimi açısından daha uygulanabilir olacaktır. Aksi takdirde, veri sorumluları, belki de aydınlatma yükümlüğünün amacını da aşar şekilde yönetilmesi zor bir sürece sürüklenebilirler. Ancak, ilgili madde hükmünde "aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir" ifadesi yer aldığından, konu hakkında Kurul'un uygulamadan ne beklendiğine dair bir ilke kararı yayınlaması faydalı olacaktır. Örneğin, eğer veri sorumlusunun birimleri arasında mutlak ayrımlar bulunmuyorsa ve veri işleme amaçları birbirleriyle örtüşüyorsa ya da yakınsa, tek bir aydınlatma metni içinde amaçların farklılaştırılması yoluna başvurulabileceği, ancak çok farklı veri işleme amaçları bulunan departmanlara sahip bir veri sorumlusunun ilgili birimlerinin, aydınlatma yükümlülüklerini ayrı ayrı yapmaları gerekebileceği Platform tartışmalarında ifade edilmiştir.

Aydınlatma yükümlülüğünün her bir birim "nezdinde" yerine getirilmesini sağlayacak daha pratik bir yöntem olarak, tek bir aydınlatma metni içerisinde ancak farklı sayfalarda ve veri sorumlusunun farklı birimlerine yönelik açılacak farklı başlıklar altında yapılandırılmış aydınlatmaların kullanılması öneriler arasında yer almıştır. Bununla birlikte, düzenlemenin veri sorumlusu olan ticari şirketler ile veri sorumlusu olan kurumlar arasında ayrım gözetilerek ele alınmasında fayda olduğu, zira şirketlerin, birimlere göre farklılaşacak olsa da, veri işleme süreçleri ve amaçlarının şirket yönetimince belirlendiği, ancak örneğin üniversitelerde her bir bölümün kendi süreçlerini kendilerinin belirlediğine dikkat çekilmiştir.

Platformdaki tartışmalar esnasında "farklı amaç" ifadesine dair yapılan bir yorum da, verinin işleme amacının, verinin ilk toplandığı sıradaki işleme amacından farklılaşması bağlamında olmuştur. İlgili yoruma göre, aydınlatma yükümlülüğünün, verinin toplandığı sırada işleme amaçlarını belirten tek bir aydınlatma metni üzerinden yapılması hayatın olağan akışına da uygundur, ancak daha sonra veriyi işleme amacı değişirse, o vakit ayrı aydınlatma metinleri ile aydınlatma yükümlülüğünün yerine getirilmesi tekrar edilebilecektir.

Konunun çalışan verileri kapsamında da ayrıca ele alınması gerektiğine dikkat çekilerek, her bir birim nezdinde hazırlanan ayrı aydınlatma metinlerinin çalışanlara imzalatılmasının pratik açıdan faydalı olmayacağı ifade edilmiştir. Bu doğrultuda çalışanlara yapılan aydınlatmanın, her bir birimin veri işleme amaçlarının farklılaştırıldığı tek bir doküman içerisinde yapılmasının en uygun çözüm olacağı, ancak ilişkinin devamı içerisinde değişen veya gelişen veri işleme faaliyeti söz konusu olursa, yeni / ilave aydınlatma metinlerinin hazırlanabileceği belirtilmiştir.

Bunlarla birlikte Tebliğ'in 5/1 (b) maddesine dikkat edilmelidir; zira veri sahibi ile veri sorumlusu arasındaki ilişkinin devamı içerisinde veri işleme amacının değişmesi halinde esasen 5/1 (b) maddesi uygulama alanı bulacaktır.

"Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir."

O halde, 5/1(b) maddesinin varlığı karşısında, 5/1(c) hükmünde veri işleme amacının değişiyor olmasının bir öneminin kalmayacaktır. Bu durumda sorunun özüne dönülecek olursa, sorunun maddenin yazılış şeklinin net olmamasından kaynaklanıyor olduğu düşünülmektedir. Hâlihazırdaki uygulamada ise, "veri sahibi kategorileri" açısından farklı aydınlatma metinleri hazırlandığı ve bu metinlerde işleme faaliyetleri hakkında detaylı bilgilendirmeler yapıldığı dile getirilmiştir.

Konu hakkındaki tartışmalara yön vermesi açısından, Kurum'un yayımlamış olduğu örnek envantere bakıldığında, Kurum'un "birim" kavramı ile anlatmak istediğinin şirket departmanları olarak anlaşılması gerektiği ve aydınlatma metinleri içerisinde açıkça hangi birimlerin hangi amaçlarla veri işlediğinin farklılaştırılmasının yeterli olacağı yorumunun doğru bir yorum olacağı dile getirilmiştir.

KVKK'da veri sorumlusuna getirilen yükümlülüklerin asıl amacı, veri sahibinin haklarını korumak olduğundan, 5/1(b) ve 5/1(c) hükümlerinin yazılış ve kapsamları da bu amaca paralel olarak ele alınmalıdır. Bu bağlamda aydınlatma metnin sayısı değil de içeriği önem arz etmektedir.

6. Aydınlatmanın Geçerliliği Sorunu ile Eksik Aydınlatmanın Sonuçlarının Değerlendirilmesi Dahil Aydınlatma Yükümlülüğünün Yerine Getirilmesine Dair Çeşitli Meseleler

ÖZET: Konu 29 Mart 2018 tarihli Platform toplantısında ele alınmıştır. Tebliğ'e göre aydınlatma metninde yer alması gereken zorunlu şartlardan birinin eksik olması halinde, "eksik" olarak nitelendirilecek bir aydınlatmanın idari ve hukuki sonuçları olmakla birlikte, Türk Ceza Kanunu açısından bir suç olarak nitelendirilmemesi gerekir.

Aydınlatma yükümlülüğünün tek taraflı bir yükümlülük olması nedeniyle veri sahibinin imzasının geçerlilik şartı olmadığı, ancak veri sahibinden alınacak bir onayın ispat açısından veri sorumlusunun menfaatine olacağı açıktır.

Aydınlatma yükümlülüğünün ne zaman yerine getirilmesi gerektiğini düzenleyen Tebliğ'in 4. maddesine bakıldığında, maddede yazılı olan veri işleme "sırasında" ifadesinin, verilerin işlenmesinden "önce" veya "en geç" verilerin işlenmesi sırasında olarak anlaşılması gerekir. Kurul'un bu bağlamda da bir görüş bildirmesi uygulama açısından aydınlatıcı ve uygulama birliğinin tesisi için önemli olacaktır.

Veri sorumlularının aydınlatma yükümlülüğü kapsamında hazırlayacakları aydınlatma metinlerinin içeriği bakımından, Tebliğ'in 4. Maddesinde aydınlatma metninde bulunması gereken asgari unsurlar belirlenmiştir. Platform toplantısında, bu unsurların eksikliğinin aydınlatma metninin geçerliliğini hangi yönde etkileyebileceği üzerine tartışılmıştır. Bu bağlamda, ilgili maddeden anlaşılması gerekenin, maddede sayılan hususlardan herhangi birini içermeyen bildirimin geçersiz sayılacağı, nitekim maddede yer verilen asgari unsurların "zorunlu" niteliğe sahip olduğu ifade edilmiştir. Diğer yandan, aydınlatmanın geçersiz olması halinde, ilgili aydınlatma metnine dayanılarak alınmış olan rızanın da geçerliliğinin etkilenelebileceği üzerinde durulmuştur.

Eksik bilgilendirme söz konusu olduğu takdirde, idare hukuku anlamında bir sorumluluğun doğacağının muhakkak olduğu, özel hukuk açısından ise eksik bilgilendirmenin tazminat yükümlülüğü doğurabileceği belirtilmiştir. Ceza hukuku kapsamında ise, hakimler ve savcıların ilgili Tebliğ'e nasıl bakacaklarının oldukça önem arz edeceği, bu doğrultuda eksik

yapılmış aydınlatmanın açık rızanın da geçerliliğini etkileyecek olması halinde hakim veya savcıların, cezai hükümleri işletme riskinin doğabileceğinin altı çizilmiştir. Ancak, bu sorunun daha önce İstanbul Medipol Üniversitesi'nde gerçekleşen seminerde de sorulmuş olduğu ve ilgili seminerde, aydınlatma yükümlülüğünün eksik yapılmasının Türk Ceza Kanunu kapsamında suç olarak değerlendirilmeyeceğinin söylendiği hatırlatılmıştır. Zira bir aydınlatma metninin, sadece tek bir unsurun eksik olması sebebiyle dahi "geçersiz" sayılması ve dolayısıyla hiç yapılmamış kabul edilmesi, ağır bir sonuç olacaktır. Bu konuda Kurum'un görüşüne ihtiyaç vardır.

Platformda aydınlatma yükümlülüğü kapsamında gündeme gelen diğer meselelerde ise hemfikir olunmuştur. Bu doğrultuda;

a. Kişisel verilerin başka bir veri sorumlusuna aktarılması halinde, aktarılan veri sorumlusunun da ayrıca aydınlatma yükümlülüğünü yerine getirmesi gerekir. Bunun yanında konuyla bağlantılı olarak, veri işleyenlerin veri sorumlusu adına aydınlatma işlemini yapıp yapamayacağı ve rıza alıp alamayacağı da değerlendirilmiştir. Bu bağlamda, prensip olarak aydınlatma yükümlülüğü veri sorumlusunun yükümlülüğüdür, ancak veri sorumlusunun talimatı ile veri işleyen durumundakiler veri sorumlusu adına ve onun talimatına istinaden kendisine verilen aydınlatma bildirimini veri sahibinin bilgisine sunabilir ve yine veri sorumlusu adına rıza alımı için gerekli işlemleri yapabilir.

KVKK madde 12'den hareketle, bir aydınlatmanın yapılacak olması veya rızanın alınacak olması durumunda veri sorumlusunun söz konusu yükümlülükleri yerine getirdiğini beyan etmesi, veri işleyenin ise söz konusu verilerin hukuka aykırı olarak işlenmediğinin beyan ve tekeffül edilmesini veri sorumlusundan isteme hakkı olmalıdır. Bu doğrultuda, veri işleyenler ve veri sorumluları arasında düzenlenen sözleşmelerde 12. madde hükmü yazılabilir. Veri sorumluları arasında düzenlenen aktarım protokollerinde veya veri sorumluları ile veri işleyenler arasında düzenlenen protokollerde de, Avrupa uygulamasına paralel olarak hangi verilerin nasıl, ne zaman ve niçin aktarıldığına ilişkin tablolar ek yapılabilir.

b. Aydınlatma yükümlülüğünün tek taraflı bir yükümlülük olması nedeniyle, veri sahibinden imza alınması geçerlilik şartı değildir, ancak veri sahibinden alınacak bir

onay ispat açısından veri sorumlusunun menfaatine olacaktır. Bunun yanında çalışan verileri açısından mümkün olan hallerde, çalışanın da dahil olacağı karşılıklı bir taahhüdün alınması faydalı olacaktır.

c. Aydınlatma metinleri ile açık rıza beyanları ayrı metinler olarak hazırlanmalıdır. Her halde önce aydınlatma yükümlülüğü yerine getirilmelidir.

d. Tebliğ'in 4. Maddesinde yer alan "sırasında" ifadesinden, verilerin işlenmesinden "önce" veya "en geç" verilerin işlenmesi sırasında yapılmış olması anlaşılmalıdır.

7. Veri Sorumlusuna Başvuru Tebliği ve Pratikte Karşılaşılabilecek Sorunlar

ÖZET: Konu 29 Mart 2018 tarihli Platform toplantısında ele alınmıştır. Veri sahibine sunulacak olan başvuru yöntemleri açısından, başvuru hakkının kullanılmasını engellememek suretiyle, veri sorumlusunun makul başvuru yöntemlerini aydınlatma metninde kendisinin belirleyebileceği, bununla birlikte Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'inde sayılan yöntemlerin hepsini sağlıyor olmasına gerek olmadığı düşünülmektedir. Bu konu bağlamında Kurum'un görüşünün sorulması uygulama açısından aydınlatıcı ve uygulama birliğinin tesisi için önemli olacaktır.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ madde 5/1'e göre;

"İlgili kişi, Kanunun 11 inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir."

İlgili maddede sayılan yöntemlerin, veri sorumlusu tarafından başvurucuya sağlanması zorunlu olan yöntemler olup olmadığı noktasında, Tebliğ'in lafzından, sayılan yöntemlerden herhangi birinin sağlanmasının yeterli olacağı değelendirilmiştir. Ancak diğer yandan yalnızca bir yöntemin sunuluyor olması durumunda da veri sahiplerinin başvuru haklarının kısıtlanması sonucu doğabilecektir. Bu bağlamda, ilgili hükmün lafzından, başvuru

yöntemlerinin veri sorumlusuna bırakılan bir tercih olmayıp, veri sahibine tanınmış seçimlik haklar olduğunun anlaşılması gerektiği ifade edilmiştir. Buna karşılık olarak, hükmün amacı bakımından önemli olanın, veri sahibinin veri sorumlusuna bir şekilde ulaşabilmesi olduğu ve bu sağlandığı sürece, sayılan tüm yöntemlerin aynı anda sunuluyor olmasının beklenmeyeceği belirtilmiştir. Netice olarak, bu hususun Kurum ile netleştirilmesi gerektiği konusunda hemfikir olunmuştur. Zira bu konu kapsamında, başvuru yöntemlerinin hepsinin sayılmamış olduğu bir aydınlatma metninin eksik aydınlatma kabul edilmesi riski de gündeme gelebilecektir.

8. KVKK madde 5/2 Kapsamında Kişisel Veri İşleme Şartlarının 95/46 sayılı Direktif ve General Data Protection Regulation ("GDPR") ile Birlikte Değerlendirilmesi; *açık rıza dışındaki hukuka uygunluk sebepleri, özel nitelikli kişisel veriler yönünden değerlendirme*

***ÖZET:** Konu 13 Nisan 2018 tarihli Platform toplantısında ele alınmıştır. Tüm işleme şartları açısından, işleme şartlarında yer alan "zorunlu" ve "gerekli" olma ifadelerinin, Avrupa Birliği düzenlemeleri de dikkate alındığında "gereklilik" olarak yorumlanmasının amaca uygun olacağı düşünülmektedir.*

***Kanunlarda açıkça öngörülme** işleme şartındaki "kanun" ifadesinin kapsamı ve sözleşmenin ifası işleme şartındaki "sözleşmenin ifası ile doğrudan doğruya ilgili olma" ifadesinin nasıl yorumlanması gerekeceği hususlarında Kurul'un ilke kararlarına ihtiyaç bulunmaktadır.*

***Sadakat kart uygulamaları** açısından da Kurul'un bir ilke kararı ile uygulamaya yön vermesi önemli olacaktır. Zira sadakat kart uygulamalarının tarafların arasında başka bir sözleşmesel ilişkiye dayandığı, bu nedenle sadakat kart uygulamaları kapsamında veri işlemenin de sözleşmenin ifası istisnasına girmesinin gerektiği yönünde görüşler de mevcuttur.*

***Kişisel verinin** ilgili kişinin kendisi tarafından alenileştirilmiş olması halinde, özellikle kişilerin sosyal medya profillerinde alenileştirilmiş olarak kabul edilebilecek veriler açısından Kurul'un bir ilke kararı ile konuyu ele alması faydalı olacaktır.*

KVKK'da meşru menfaat işleme şartında, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması ifade edilmektedir. Ancak, konu hakkındaki tartışmalara ve uygulamaya yön vermek adına, kanunun lafzından ziyade amaca uygun yorum prensibi ile hareket edilmesinin meşru menfaate dayanan işleme şartı için oldukça önemli olduğu düşünülmektedir. Zira maddede geçen "zarar verme" ifadesinin "denge testi" kapsamının ötesinde kaldığı, uluslararası dokümanlarda "aşırı müdahaleci olmamak" ifadesinin kullanılmakta olduğu gözetilerek değerlendirme yapmanın yerinde olacağı söylenmiştir. İşçinin sağlık ve sabıka verilerinin istihdam ilişkisi kapsamında işlenmesi hakkında da Kurul'un görüşünü bildirmesi uygulamanın bütünlüğü açısından çok faydalı olacaktır.

Platform tartışmaları sırasında;

a. ***Kanunlarda açıkça öngörülme*** işleme şartının ikincil mevzuatı da kapsayıp kapsamadığının ve Avrupa İnsan Hakları Sözleşmesi de dikkate alındığında, "meşru amaç" ve "ölçülülük" şartlarını taşımayan ve yalnızca kanuni bir düzenlemeye dayanan şekli bir kısıtlamanın, tek başına bir işleme şartı olarak kabul edilip edilemeyeceğinin netleştirilmesi gerektiği,

OHAL uyarınca KHK'lar ile getirilmekte olan düzenlemelerin bu işleme şartı kapsamında değerlendirilip değerlendirilemeyeceğinin ilke kararına bağlanmasının yararlı olacağı,

b. ***Fiili imkansızlık*** işleme şartının en çok kullanılan örneğinin "bilinci kapalı kişinin sağlık bilgisi"nin işlenmesi olmasına rağmen, ilgili maddenin KVKK 6. Madde hükmü ile ilişkilendirilmemiş olması nedeniyle sağlık, verilerinin işlenmesi anlamında bu işleme şartına dayanılıp dayanılamayacağının dayanılamamasının sorun teşkil edeceği,

c. ***Sözleşmenin İfası*** işleme şartının 95/46 sayılı Direktif ve GDPR'den farklı olarak, hükümde yer alan "**doğrudan doğruya** ilgili olması kaydıyla" ifadesinin nasıl yorumlanması gerektiğinin netleştirilmesi gerektiği yönünde kanaat bildirilmiştir.

Bu bağlamda, ilgili işleme şartlarının 95/46 sayılı Direktif ve GDPR'deki kapsamlarına da bakılmıştır.

Fiili imkansızlık:

KVKK	Directive	GDPR
Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması	Processing is necessary in order to protect the **vital interests of the data subject**	Processing is necessary in order to protect the **vital interests of the data subject or of another natural person**

Sözleşmenin ifası:

KVKK	Directive	GDPR
Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

Sözleşmenin ifası konusunda yorumlanması gereken bir diğer husus olarak ***sadakat kartları*** ele alınmıştır. Kurum katıldığı bir seminerde, herhangi bir hizmetin sunulması için açık rıza verilmesi şartını kabul etmeyeceğini ve bu durumda verilecek olan rızanın sakat olacağını, ancak sadakat kartlarının kullanımı için rızanın bir ön şart olarak alınabileceğini ifade etmiştir. Bununla birlikte Platformdaki tartışmalarda, sadakat kartlarının kullanımı için açık rızaya dayanma gereksiniminin kanuna aykırı bir yorum olacağı, nitekim sadakat kartlarının da aslında hizmet sözleşmesinin dışında başka bir sözleşmesel ilişkiye dayandığı, bu nedenle sadakat kartları kapsamında veri işlemenin de sözleşmenin ifası istisnasına girmesi gerektiği

görüşleri ileri sürülmüştür. Ancak fiili durumda firmaların çoğunlukla sadakat kart üyeliği tesis ederken işleme amacıyla uyumlu, sınırlı ve ölçülü olma temel ilkelerini aşan şekilde veriler toplamış olduklarından, bu verileri kaybetmemek adına açık rıza alma yoluna gittikleri belirtilmiştir. Bu dönemde birçok firmanın, veri sahiplerini sadakat kartlarına tanımlı menfaatleri iptal etme / silme gibi yöntemlerle korkutarak, rıza alma yoluna başvurduğu, ancak bunun yerine daha fazla puan vaadi ile rıza vermeye teşvik etmenin, Avrupa Birliği uygulamasında da görülen, daha doğru ve etkin bir yöntem olacağı belirtilmiştir. Bütün bunların yanında, sadakat kartlarına ilişkin olarak hâlihazırda tartışılması gereken bir sorunun, 7 Nisan 2018 ve hemen öncesinde gelen bildirimlerdeki "puanların silineceğine" yönelik ifadeler olduğu dile getirilmiştir. Rızanın alınmaması karşısında puan silmeye yönelik uygulamaların, veri sahiplerinin hâlihazırda tüketici hukuku uyarınca kazanmış oldukları haklarının da ihlali anlamına geldiği ifade edilmiştir.

Bu başlık altında, KVKK madde 5/2 (c) hükmünde yer alan ***"sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"*** ifadesinin Türk hukukunda tanımlanmış olan "3. Kişi yararına sözleşme" bakımından nasıl uygulanması gerekeceğinin de netleştirilmeye ihtiyacı vardır. Nitekim 3. Kişi yararına yapılan bir sigorta sözleşmesinde, veri sahibinin sözleşme tarafı olmayacağı ve veri sahibinden açık rıza alınmasının da oldukça zor olacağı dile getirilmiştir. Bu durumda *"meşru menfaat"* gibi diğer veri işleme şartının uygulanma alanı bulmasının mümkün olup olmayacağı tartışılmalıdır.

İlgili veri işleme şartına ilişkin olarak netleştirilmesi gerekecek bir diğer husus da, hükmün sonunda yer alan "verilerin işlenmesinin *gerekli* olması" ifadesidir. Nitekim diğer tüm veri işleme şartlarında "*gerekli*" olmak yerine "*zorunlu*" olmak kullanılmıştır. Bu bağlamda, söz konusu farkın KVKK gibi çerçeve kanun niteliğindeki bir düzenleme kapsamında amaca uygun olarak "gerekli" şeklinde yorumlanabileceği, nitekim ilgili işleme şartlarına Kurul'un rehberinde verilen örneklerin dahi "zorunlu" örnekler olmadığı ve Avrupa Birliği mevzuatında da hep "necessary" ifadesinin kullanılmış olduğu belirtilmiştir.

Konuya ilişkin olarak yapılan bir diğer değerlendirmede de, sözleşmenin ifası hükmünde yer alan "gerekli" ifadesinin daha sübjektif bir şekilde, "zorunlu" ifadesinin ise daha objektif bir şekilde yorumlanabileceği söylenmiştir. Nitekim her sözleşme ilişkisi içinde işlenmesi "gerekli" olacak veri kategorilerinin her bir sözleşme özelinde ayrıca değerlendirilmesi gerekeceği, ancak diğer veri işleme şartlarının mevzuattan veya dışarıdan gelen diğer

zorunluluklardan kaynaklı olması nedeniyle, "zorunlu" ifadesinin kullanılmış olabileceğine dikkat çekilmiştir. Buna karşın, meşru menfaatin de oldukça sübjektif bir veri işleme şartı olduğu ve buna rağmen burada da "zorunlu" kelimesinin tercih edilmiş olduğunun altı çizilmiştir. Ayrıca, KVKK'da lâfzî olmaktan çok amaca uygun şekilde yorumlanması gereken pek çok ifadenin yer aldığı, bu doğrultuda, veri işleme şartlarında bulunan "zorunlu" ifadelerinin de aynı şekilde "gerekli" şeklinde yorumlanmasının amaca uygun olacağı ve ticari hayatın akışı ile örtüşeceği dile getirilmiştir.

Kişisel verinin ilgili kişinin kendisi tarafından alenileştirilmiş olması halinde, Uygulama Rehberi'nde, "ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir" ifadesi kapsamında, özellikle kişilerin sosyal medya profillerinde alenileştirilmiş olarak kabul edilebilecek veriler açısından, uygulamanın bütünlüğü için Kurul'un bir ilke kararı konuya değinmesi yararlı olacaktır.

Konuya ilişkin olarak Kurum'un yeni rehberinde yer alan görüşün, "kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir" şeklinde olduğu, burada açık rızadan ziyade rızanın varsayılabileceği koşullara işaret edildiği belirtilmiştir. Bu doğrultuda, örnek olarak kartvizit bastıran bir kişinin, kartvizitinde bulunan iletişim bilgileri ile kendisine ulaşılmasını istediği ve verilerini bu sebeple alenileştirildiğinin kabul edilip edilemeyeceği tartışılmıştır.

Veri sahipleri tarafından alenileştirilen verilerin, ilgili kişinin alenileştirme amacının dışına çıkarak ve ölçülülük ilkesine aykırı bir şekilde işlenmesinin ceza hukukunda nasıl değerlendirilebileceği de gündeme gelmiştir. Böyle bir durumda ceza mahkemelerinin failin lehine yorum yoluna başvurabileceği ve mahkemeler tarafından kişinin, verilerini alenileştirerek her şekilde işlenmesine rıza gösterdiği gibi bir yorumun yapılabileceği belirtilmekle birlikte, ölçülülük ilkesinin altı çizilmiştir. Uygulamada ceza hakimlerinin ölçülülük ilkesinin bariz bir şekilde aşıldığı somut olaylarda farklı bir yoruma gidebileceği belirtilmiştir.

Alenileştirmeye ilişkin tartışılması gereken bir husus da, sosyal medya hesaplarıdır, nitekim sosyal medya hesaplarında paylaşılan verilerin, hangi durumda alenileştirilmiş sayılacağı belirsizdir. Bu hususa ilişkin olarak ceza hukukunda yapılan yorumun, alenileştirmenin anlamının "belirsiz" sayıda kişiye ulaşabilme "kabiliyeti" olduğuna dikkat çekilerek, kişinin

paylaşmış olduğu verilerin belirsiz sayıda kişinin erişimine açık olması halinde, aleni sayılabileceği belirtilmiştir. Ceza hukuku uyarınca, kamuya açık bir web sitesine konulan bir verinin, o web sitesine yalnızca 1 kişi tıklamış olsa dahi aleni sayılacağı; çünkü bu web sitesinin belirsiz sayıda kişiye ulaşabilme kabiliyeti olduğu ifade edilmiştir. Bu durumda da herkesin erişimine açık olmayan ve sınırlı bir takipçi çevresi olan bir sosyal medya hesabının da aleni olarak değerlendirilemeyeceğini düşünmek gerekecektir.

Meşru Menfaat işleme şartı, Avrupa Birliği uygulamasına paralel olmakla birlikte, KVKK madde 5/2(f) hükmünde düzenlenen meşru menfaat ile Avrupa Birliği mevzuatından düzenlenen "legitimate interest" arasında lâfzî olarak büyük bir fark vardır. Nitekim KVKK'da yalnızca veri sorumlusunun meşru menfaatinden bahsedilirken, 95/46 sayılı Direktif'te veri sorumlusunun yanında 3. Kişi ve verinin açıklandığı diğer kişilerin de meşru menfaatinden bahsedilmektedir. GDPR'da da veri sorumlusunun yanında 3. Kişinin menfaatinden bahsedildiği görülmektedir. Ayrıca, KVKK'nın ilgili hükmünde "zorunlu olması" ifadesi kullanılırken, Avrupa Birliği mevzuatında "gerekli (necessary)" denmiş olmakla, Working Party kararlarının bu veri işleme şartının yorumlanması açısından Türkiye uygulamalarına fazla ışık tutamayabileceğine dikkat çekilmiştir.

KVKK	**Directive**	**GDPR**
İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Meşru menfaat işleme şartı kapsamında "temel hak ve özgürlüklere zarar vermemek" ifadesi irdelendiğinde, hükümde geçen "zarar vermemek" ifadesinin, "temel hak ve özgürlükleri aşmamak kaydıyla" olarak okunması gerektiği belirtilmiştir. Nitekim, hem Kurul'un yapmış olduğu açıklamalar hem de rehberde yer alan ifadeler uyarınca, meşru menfaat şartının uygulanmasında ilk bakılması gereken veri sorumlusunun meşru bir menfaatinin bulunup bulunmadığı ve ikinci olarak ise tarafların menfaatlerine ilişkin bir "dengeleme testi" yapılmasıdır. Bu doğrultuda, "zarar verme" şeklindeki ifadenin "denge testi" kapsamının ötesinde olduğu, uluslararası dokümanlarda "aşırı müdahaleci olmamak" ifadesinin kullanılmakta olduğuna işaret edilmiştir.

Bütün bunların yanında, ilgili işleme şartı uyarınca söz konusu menfaatin "meşruluğu"nun hangi ölçüte göre değerlendirileceğinin oldukça sübjektif ve belirsiz olduğuna dikkat çekilerek, ceza kanununda da çeşitli hükümlerde "meşru" ifadesinden bahsedildiği, ancak bu ifadenin Yargıtay tarafından oldukça farklı şekillerde yorumlandığı belirtilmiştir. Şirketlerin veri işleme faaliyetleri düşünüldüğü zaman, yalnızca kar elde etmeye yönelik bir veri işlemenin meşru menfaat kapsamında değerlendirilemeyeceği, ancak verimlilik amacıyla gerçekleştirilen veri işleme faaliyetlerinin, meşru menfaat kapsamında tutulabildiği ifade edilmiştir. Nitekim bulut yedekleme hizmeti kullanmak isteyen bir şirketin, verilerini bulutta saklamak yönünde meşru bir menfaatinin bulunduğunu söylemek mümkündür.

Tartışma ve uygulamaya yön vermek adına, kanunun lafzından ziyade amaca uygun yorum prensibi ile hareket edilmesinin meşru menfaate dayanan işleme şartı için oldukça önemli olduğunda hem fikir olunmuştur. Zira veri sorumlusu tarafından yalnızca kar sağlama amacı gütmeyen, verimliliğe yönelik veri işleme faaliyetlerinin, meşru menfaat kapsamında tutulması gerektiği ve bu şekilde yapılacak bir yorumun, Avrupa Birliği mevzuatı ve uygulamasına da paralel olacağı belirtilmiştir. Nitekim KVKK'nın genel gerekçesinde de, Direktif'e ilişkin uygulamaların takip edileceği yer almakta ve rehberde "zorunlu olmak" ifadesinin açıklanmamış olmasının Kurum'un da maddenin lafzı üzerinde durmadığını gösterdiği düşünülmektedir.

İşçi – işveren ilişkisi açısından da, işçinin sağlık ve sabıka verilerinin istihdam ilişkisi kapsamında işlenmesine dair Kurul'un görüş vermesi uygulamaya yol gösterme açısından çok faydalı olacaktır. Zira bu konuda fikir ayrılıkları ve uygulama farklılıkları bulunmaktadır.

Özel nitelikli verilere işaret etme kabiliyeti olan veriler açışından ise, veri sorumlusunun işleme amacına bağlı olarak değerlendirme yapılması gerekeceği; örneğin, bir kişinin CV'de yer alan fotoğrafından ırk, din, etnik köken, sağlık gibi özel nitelikli verilerin dolaylı olarak elde edilebildiği gündeme gelmiştir. Bu bağlamda, üzerinde fotoğraf olan CV'yi saklayan, ancak bu fotoğraflar üzerinde özel nitelikli verileri analiz ederek veri tabanına kaydetmeyen ve özel nitelikli verileri işleme amacı bulunmayan bir veri sorumlusunun, salt bu sebeple özel nitelikli veri işliyor olarak değerlendirilmemesinin yerinde olacağı belirtilmiştir. Zira her türlü fotoğrafın otomatikman özel nitelikli veri olarak kabul edilmesinin uygulamada büyük zorluklar yaratacağı, önemli olanın veri sorumlusunun veri işleme amacının ne olduğu vurgulanmıştır. Nitekim her ne kadar fotoğraftan özel nitelikli verilerin elde edilmesi mümkün ise de, elinde bulunan fotoğrafları bu özel nitelikli verilere göre detaylandırarak ve özel nitelikli veri kategorileri oluşturarak işlemeyen bir veri sorumlusunun, özel nitelikli veri işliyor olarak değerlendirilemeyeceği konusunda hemfikir olunmuştur.

9. Veri Saklama ve İmha Sürelerine Dair Genel Prensipler Neler Olabilir?

ÖZET: Konu 11 Mayıs 2018 tarihli Platform toplantısında ele alınmıştır. Veri saklama ve imha sürelerine ilişkin tespitlerin Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in lafzından yola çıkılarak "veri kategorisi" bazında yapılması doğru olacaktır. Bunun yanında, Avrupa'da bugüne kadar ki örneklere bakıldığı zaman, sürelerin 95/46 sayılı Direktif uyarınca "veri kategorisi" değil, "dokümantasyon" (records) üzerinden belirlendiği, ancak son dönemlerde GDPR'ın özellikle çalışan verileri için çalışma süresinin bitiminde hangi verinin ne kadar tutulacağının ayıklanması gerektiğini belirterek "veri kategorisi" bazında ayrımı işaret ettiği görülmektedir.

Öte yanda, veri saklama ve imha sürelerinin GDPR ile paralel olarak veri kategorisi bazında belirlenmesini gerektirecek önemli bir husus da, GDPR'ın Avrupa Birliği vatandaşlarının verilerinin, Avrupa Birliği sınırları dışında işlenmesi durumunda dahi uygulama alanı bulacağıdır. Bu doğrultuda, saklama ve imha sürelerinin veri kategorisi bazında belirlenmesinin gerekli ve faydalı olacağı konusunda hemfikir olunmuştur.

Platform toplantısında saklama ve imha sürelerinin veri kategorileri bazında belirlenmesi genel prensibinde hem fikir olunduktan sonra, bazı veri kategorileri yönünden gerekli veya makul kabul edilebilecek sürelerin ne kadar olması gerektiği veya olabileceğine ilişkin görüş alış verişi yapılmıştır. Bu bağlamda ortaya konan tespit ve öneriler şunlar olmuştur:

a. Çalışan Adayı Verileri

Çalışan Adayı verilerine ilişkin veri kategorilerine örnek olarak, "**Kimlik Verisi**", "**İletişim Verisi**", "**CV**" ve "**Kamera Kayıtları**" gibi kategoriler söz konusu olabilecektir.

Platformda, çalışan adaylarının CV'lerinin saklama sürelerinin işlenme amacıyla uyumlu ve sınırlı olacak şekilde asgari süre olarak belirlenmesinin faydalı, bununla birlikte çalışan adayı CV'lerinin ortalama bir yıl süre ile saklanmasının makul olacağı görüşüne çoğunluk katılımı sağlandı. Zira işçi bulmanın da bir maliyet yarattığına dikkat çekilerek, işe alımların sonrasında gerçekleşen işten ayrılmalarda veya ortaya çıkan benzer pozisyon ihtiyaçlarında kayıtlarda bulunan mevcut CV'lerden daha hızlı, pratik ve az maliyetli tarama yapılabildiği vurgulanmıştır. Bu konuda yabancı rehberlerde de çeşitli sürelerin düzenlendiğine dikkat çekilerek, Fransız Veri Koruma Otoritesi'nin ("**CNIL**") bu konuda verdiği tavsiyenin çalışan adayı CV'lerinin iki yıl tutulması yönünde olduğu belirtilmiştir. Bununla birlikte, CV'lerin içerdiği tüm veriler ile bir bütün olarak ele alınmaktansa, iletişim, eğitim, tecrübe bilgisi gibi veriler dışında fotoğraf, medeni durum gibi verilerin uzun süreler ile saklanmasının doğru olmayacağı ve saklama süresi boyunca bu tür verilerin karartılmasının tavsiye edildiği belirtilmiştir.

Platform tartışmaları sırasında, saklama sürelerinin belirlenmesi konusunda tercih edilebilecek güvenli bir yol olarak da, saklama süresinin uzunluğuna yönelik çalışan adayına bir tercih sunulması ve bu doğrultuda çalışan adayından, daha sonra açılacak pozisyonlara ilişkin değerlendirilmesi amacıyla CV'sinin saklanıp saklanmaması hususunda tercihini belirtmesinin istenmesi bir öneri olarak iletilmiştir.

Öte yandan, saklama süresinin sonunda imha edilecek aday başvuru ve CV'lerine dair tüm kayıtların silinmesi gerekeceği belirtilmiştir.

Çalışan adaylarına ilişkin kamera kayıtlarının ise ortalama iki ay süre ile saklanmasının uygun olduğu, nitekim herhangi bir suç işlendiğinde suç duyurusunda bulunulması için iki aylık kamera kayıtlarının görüntülenebilir olması gerektiği ifade edilmiştir.

Çalışan adayları ile yapılan iş görüşmelerinde tutulan notlara ilişkin olarak, GDPR tartışmalarında da özellikle değinilen noktanın dikkate alınması ve çalışan adayının negatif özelliklerini veya özel nitelikli verilerini içeren notların kayda alınmasının daha farklı değerlendirilmesi gerektiğine ve bu noktada meşru menfaat savunmasının çok daha zor yapılabileceğine dikkat çekilmiştir.

b. Çalışan Verileri

Şirket çalışanlarının özlük dosyası verilerine ilişkin saklama sürelerinin belirlenmesinde, sektör bazında belirlenen tehlike seviyelerine göre farklı süre belirlemesi yapılıp yapılmadığı gündeme getirilmiştir. Bu bağlamda, iş sağlığı ve güvenliğine ilişkin verilerde tehlike bazında bir ayrım yapılabileceği, ancak çalışanlara ilişkin diğer veri kategorilerinde böyle bir ayrıma gerek duyulmadığı görüşü öne çıkmıştır. Çalışanların kimlik verisi, iletişim verisi, finansal verileri, eğitim verileri, performans verileri gibi verilerin, çalışma süresinin bitiminden itibaren özellikle dava zamanaşımlarına bağlı olarak 5 ila 10 yıl sürelerle saklanmasının doğru bir yaklaşım olacağı, sağlık verilerinin ise zaten ilgili kanun gereği 15 yıl süre ile saklanmakta olduğu ifade belirtilmiştir. İlgili kanunların gereği olarak süresiz saklanması gereken belgeler de bulunmaktadır, çalışma belgesi gibi.

Bunun yanında, veri envanteri dikkate alındığı zaman, çalışanların özlük verilerinin işlenmesine ilişkin hukuki sebebin, envantere sözleşmenin ifası olarak yazılmakta olduğu, ancak iş ilişkisi sona erdikten sonra verileri 10 yıl boyunca saklamanın altında yatan hukuki sebebin bir hakkın yerine getirilmesi olduğuna dikkat çekilerek, bu hususun veri envanterinde nasıl ele alınması gerektiği hususu da tartışılmıştır. Bu durumda her iki hukuki sebebin de yazılması gerekeceği belirtilmiştir.

c. Müşteri Verileri

Müşteri verilerinin, ilgili sektöre ve müşteriye göre farklılık arz edebileceğine dikkat çekilerek; mağaza müşterileri, elektronik ticaret müşterileri, finans sektörü müşterileri, sağlık

sektörü müşterileri, üye müşteri verileri gibi farklı tipler için ayrı değerlendirme yapılmasının gerekeceği ifade edilmiştir.

Örneğin, bankacılık ve finans gibi regüle sektörlerde gündeme gelen bir sorun olarak, henüz müşteri olmayan kişilerin istihbarat verilerinin işlenmesine dikkat çekilmiştir. Bu noktada Kurum'un daha önceki bir yorumunun, henüz müşteri olmayan kişilerin verilerinin saklanmaması gerektiğine ilişkin olduğu ve bu yaklaşımın bankalar açısından her yeni başvuruda tekrar değerlendirme yapma zorunluluğu doğuracağı belirtilmiştir. Bunun yanında, Risk Merkezi'nin de çok sayıda veri işlediğine dikkat çekilerek, bu verilerin kişilerin onayı ile Kredi Kayıt Bürosu ("**KKB**") vasıtasıyla paylaşıldığı ve bu noktada söz konusu müşteri verilerinin şirketin kendisi, Risk Merkezi veya KKB gibi kuruluşlardan hangisine ait olacağının kabulünün dahi tartışılabileceği ifade edilmiştir.

Müşteri verilerinin saklama sürelerinin belirlenmesi konusunda sektörel yükümlülüklerin detaylı olarak incelenmesi gerekeceği, nitekim bilançosal yükümlülükler sebebiyle tüm finansal kuruluşların düzenli olarak bilanço temizliği yapmaları gerektiği ve benzer yükümlülüklerin söz konusu olabileceği belirtilmiştir.

Herhangi bir durumda müşteri verilerinin saklanmasına ilişkin olarak, sözleşme zaman aşımı süresinin 10 yıl olmasından hareketle, bu süreye bir yıl daha eklenmesi ile verilerin 11 yıl saklanmasının KVKK kapsamında kabul edilebilir olup olmadığının tartışılmasında fayda olacaktır.

Ayrıca, finans sektörü söz konusu olduğu zaman, verilerin MASAK yükümlülükleri dolayısıyla da tutulması gerektiği ve TCK madde 282 hükmündeki zamanaşımı süresi dikkate alındığı takdirde, eylemden itibaren 15 yıllık bir zamanaşımının söz konusu olduğuna dikkat çekilmiştir.

Verilerin saklanması sürelerinin başka yasalardan kaynaklanan yükümlülükler gereği uzayabildiği görüldüğünden, veri sorumlusunun uygulayacağı imha yöntemlerinin bu bağlamda önemli olacağının altı çizilmiştir. Bu nedenle veri sorumlularına silme ve yok etme işlemleri arasındaki farkların ve olası maliyetlerin detaylı bir biçimde anlatılması gerekecektir.

d. Elektronik Ticarette Müşteri Verileri

Elektronik ticaret şirketlerine her zaman önerilmesi gereken öncelikli hususun, müşterilerine üye olmaksızın alışveriş yapma imkânını getirmeleri yönünde olması gerektiği belirtilmiştir. Bu doğrultuda, üye olmayan müşterilerin verilerinin sözleşmenin ifası gereği işlenmesi ve genel zamanaşımı süresinin ardından bu verilerin imha edilmesi yerinde olacaktır.

Üyelik sahibi müşterilere ilişkin olarak ise, müşterinin verisinin, üyeleri avantajlardan yararlandırabilmek adına, meşru menfaat kapsamında üyelik süreci boyunca ve üyelik sona erdikten sonra da yine genel zamanaşımı süresi boyunca saklanmasının uygun olacağı önerisi yapılmıştır.

Bu kapsamda, e-ticaret şirketlerinin, uzun bir süredir kullanılmayan ve aktif olmayan üyelerinin verilerini ise, yurtdışındaki belli bir süre herhangi bir işlemde bulunmayan üyelik hesaplarının ve bu hesaplara ilişkin verilerin, belirli bir süre sonra tekrar geri getirilebilecek şekilde silinmesi uygulamasına paralel olarak silebilecekleri şeklinde görüşler belirtilmiştir.

Kişisel verilerin, sözleşmenin ifası kapsamında rıza alınmaksızın işlendiği ancak elektronik ticaret mevzuatı kapsamında gerekli elektronik ticari ileti onayının alındığı bir varsayım içerisinde, sözleşmenin ifası kapsamında işlenen kişisel verilerin saklama sürelerinin dolması, ancak elektronik ticari ileti onayının geri çekilmemiş olması durumu da değerlendirilmiştir. Bu iki hususun birbiri ile çeliştiği, nitekim veri sorumlusunun geri çekilmeyen onay uyarınca elektronik ticari ileti gönderme hakkına sahip olduğu, ancak KVKK uyarınca elindeki kişisel verileri silmesi gerekeceği ifade edilmiştir.

e. Potansiyel Müşteri Verileri

Henüz veri sorumlusu ile arasında herhangi bir sözleşmesel ilişki bulunmayan, ancak böyle bir ilişki kurması muhtemel olan potansiyel müşterilerin verilerinin de veri sorumlusu tarafından saklanabildiği belirtilerek, bu saklamanın hangi işleme şartlarına dayanarak ve ne kadar süre ile gerçekleştirilebileceği tartışılmıştır. Ayrıca, bu veriler içerisinde kişisel verilerinin işlenmesine ilişkin açık rıza vermemiş, ancak elektronik ticari ileti onayı vermiş kişilerin verilerinin de bulunduğu ve elektronik ticari ileti onayının, KVKK kapsamında bir

hukuka uygunluk sebebi olarak değerlendirilip değerlendirilemeyeceği de gündeme getirilmiştir.

Potansiyel müşteri verilerinin sözleşmenin ifası kapsamında saklanıp saklanamayacağı konusunda; henüz ortada bir icap olmadığı takdirde herhangi bir sözleşmeden de bahsedilemeyeceği ve yalnızca bir sözleşme kurulması ihtimalinden yola çıkılarak sözleşmenin ifasına dayanılamayacağı ifade edilmiştir. Bu noktada, verilerin nasıl toplanmış olduğunun da önem kazanacağına dikkat çekilerek, sözleşme yapma düşüncesi ile kartvizitini vermiş olan bir kişinin potansiyel müşteri sınıflandırması ile veri sorumlusunun örneğin linked-in üzerinden profilleme yoluyla belirlediği potansiyel müşteri verileri arasında bir fark bulunduğu belirtilmiştir.

Potansiyel müşteri verilerinin değerlendirilmesinde başvurulabilecek bir diğer yöntemin, bu verileri cookie'ler ile kıyaslamak olduğu ifade edilmiştir. Nitekim, bir kişinin e-ticaret yapan web sitesine uğraması ile, kişinin bilgisayarına bir takım cookie'lerin konmakta olduğu ve bu cookie'lerin, kişiyi potansiyel müşteri olarak gördüğü ve cookie'lerin bu kişilerin bilgisayarlarında tutulması için CNIL'in belirlediği sürenin ise 13 ay olduğu anlatılmıştır. Bu doğrultuda, CNIL'in belirlemiş olduğu bu süreden yola çıkılarak, potansiyel bir müşterinin gerçekten sözleşme yapma iradesinin bulunup bulunmadığını ölçmek için 13 aylık bir sürenin makul olduğu ve saklama süresinin de bu şekilde 13 ay olarak belirlenebileceği belirtilmiştir.

f. Gerçek Kişi Tacir ve Pay Sahiplerine Ait Veriler

Türk Ticaret Kanunu kapsamında, pay defterlerinin saklanmasına ilişkin azami bir sürenin belirtilmemiş olduğuna dikkat çekilerek, pay defterinin süresiz olarak tutulması gerekeceği ifade edilmiş, bu doğrultuda, pay defteri uygulaması açısından ortaklık verilerini süresiz olarak saklamanın hukuka uygun olacağı ifade edilmiştir.

Öte yandan, Kurul'un, herhangi bir gerçek kişinin kişisel verileri ile gerçek kişi bir tacirin ticari faaliyetinden kaynaklanan kişisel verilerini eşdeğer bir biçimde değerlendirmekte olduğuna dikkat çekilmiştir. Ancak, gerçek kişi tacirin ticari bir faaliyet kapsamında karşı tarafa aktarmış olduğu kişisel verilerine ilişkin herhangi bir rıza alınmasının uygulamada sorunlar yaratabileceği ve Kurul'un bu konuda bir ilke kararı vermesine ve ayrıma gitmesine ihtiyaç olduğu belirtilmiştir.

Platformdaki tartışmalar sırasında Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in madde 12/b hükmü de gündeme gelmiştir. İlgili maddede yer alan "kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; **üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder**" ifadesinden, bu tür bir imhanın nasıl temin edebileceği sorulmuştur. Bu soruya ilişkin olarak, gerekli yükümlülüğün yerine getirilmesi için veri sorumlusu ve veri işleyen arasındaki aktarımlar kapsamında düzenlenen veri işleme sözleşmelerine, "veri işlemenin sona erdiği an itibariyle, verilerin yok edilmesi gerektiği" şeklinde maddeler eklenebileceği belirtilmiştir. Ancak veri sorumluları arasındaki veri aktarımında söz konusu maddenin uygulanabilir olmayacağı, nitekim her iki tarafın da veri sorumlusu olduğu ve bizdeki uygulamada "joint controller" kavramının yer almadığı, bu nedenle her iki tarafın da veri sorumlusu olarak kendi yükümlülüklerini yerine getirmesi gerekeceği de ifade edilmiştir.

Son olarak, veri kategorilerine ilişkin belirlenen saklama sürelerinin VERBİS sistemine girilmesi esnasında, kanunda belirlenen süreler boyunca saklanacak veriler için "kanuni zamanaşımı süresi" gibi bir ifadenin kullanılmasının uygunluğu / yeterliliği değerlendirilmiş ve böyle bir ifadenin büyük ihtimalle kabul görmeyeceği, ilgili sektöre ilişkin düzenlemelerin incelenerek verilerin saklanabileceği maksimum kanuni sürelerin spesifik olarak belirtilmesi gerekeceği belirtilmiştir.

10. Anayasa Mahkemesinin 2016/125 Esas 2017/143 Karar sayılı ve 28.09.2017 tarihli Kararı ile Kurul'un Uygulama Rehberi çerçevesinde "açık rıza" meselesinin; "*battaniye rıza", "rıza kirliliği", "yanıltıcı rıza", "geçersiz rıza" ve "gereksiz rıza" kavramları*

***Özet:** Konu 24 Mayıs 2018 tarihli Platform toplantısında ele alınmıştır. Veri sahibi kadar veri sorumlusunun hak ve menfaatleri açısından ve uygulamanın belirli bir yönde ilerleyebilmesi için, açık rızanın diğer veri işleme şartları karşısındaki yerine dair tüm yorum ve değerlendirmelerin etraflıca ele alınarak, bu konuda bir fikir birliğine varılması önem arz etmektedir. Bu bağlamda, "battaniye rıza", "rıza kirliliği", "yanıltıcı rıza", "geçersiz rıza" ve "gereksiz rıza" kavramlarına Kurul'un vereceği bir ilke kararı ile netlik*

kazandırılmasına ihtiyaç vardır. Kurul, veri sahibinden açık rıza alınmasının kişisel veri işleme şartları içindeki yerini tespit ederken, Anayasa Mahkemesinin bu konuda yaptığı ve aslen Kurul kararlarından farklılaşan değerlendirmesini de dikkate almalıdır.

KVKK madde 5/2'de sayılan kişisel veri işleme şartlarının belirsizliği veya değişkenliği karşısında, diğer kişisel veri işleme şartlarının yanında açık rıza almış olmayı da bir tür güvence olarak gören bir veri sorumlusunun, bu amaçla ve öncesinde doğru ve tam yapılmış bir aydınlatmaya dayanarak aldığı açık rızanın "geçersiz" sayılmaması, en fazla "gereksiz" kabul edilmesi yönünde görüşler ileri sürülmüştür. Kurum'un bu konudaki görüşüne ihtiyaç vardır.

KVKK'nın kişisel verilerin işlenme şartlarına ilişkin 5. maddesinin lafzına bakıldığında, açık rızanın, maddenin ikinci fıkrasında sayılan diğer işleme şartlarından hiyerarşik olarak daha üstün kılındığı şeklinde bir okunma yapmak mümkündür. Kurum tarafından yayımlanan Kişisel Verilerin Korunması Kanunu'na İlişkin Uygulama Rehberi'nde ise açıkça, "açık rıza, kanunda hem özel nitelikli kişisel veriler, hem de özel nitelikli olmayan kişisel veriler bakımından hukuka uygunluk sebeplerinden bir tanesidir" denilmiş ve bu suretle açık rıza ve diğer hukuka uygunluk sebepleri eşit seviyede tutulmuştur. Her ne kadar KVKK'da bu şekilde yazılmış olsa da, Kurum'un daha sonra yaptığı yorumlarında ve rehberlerinde KVKK ve GDPR'ı eşleştirmiş olduğu ve GDPR'dan yola çıkarak tüm veri işleme şartlarını eşit olarak görmeye başladığı anlaşılmaktadır. Hatta diğer işleme şartlarının varlığı halinde açık rızanın alınmaması, bu durumlarda alınan rızanın "geçersiz" sayılacağını belirtmişlerdir. Nitekim Kurum'un 5 Mart 2018 tarihinde İstanbul Medipol Üniversitesi'nde katılmış olduğu etkinlikte, "hukuka uygun işleme halleri varken, açık rıza alınmasını, *rıza kirliliği* yaratmak olarak yorumluyoruz" şeklinde bir beyanı olmuştur. Bu durumda, diğer işleme şartları varken ilgili kişinin açık rızası da alınmış ise, rıza daha sonra geri çekilirse, söz konusu verinin işlenemez hale gelmesi veya veri sorumlusunun idari para cezası yaptırımı ile karşılaşması gibi olası sonuçları değerlendirmek gerekir.

Diğer taraftan bu konu kapsamında mutlaka dikkate alınması gereken Anayasa Mahkemesi Kararı vardır. Anayasa Mahkemesi'nin, KVKK'nın 5. Maddesinin (2) numaralı fıkrasının (c), (ç), (e) ve (f) bentlerinin iptal taleplerinin incelenmesine ilişkin vermiş olduğu Kararı'nda[1],

[1] 2016/125 Esas, 2017/143 Karar sayılı ve 28.09.2017 tarihli Anaya Mahkemesi Kararı.

"açık rızaya getirilen istisnaların, esas kural haline getirildiği veya açık rızaya ihtiyaç duyulmasını imkânsız hale getirdiği söylenemez" yönünde değerlendirmesi[2] mevcuttur. Aynı Kararda "bir başka deyişle, dava konusu kurallar, maddede belirtilen konularda gereklilik veya zorunluluk halinde ortaya çıkabilecek bir ihtiyacın karşılanmasına yönelik olup, hakkın özüne dokunmamaktadır" da denmektedir. Bu durumda, Anayasa Mahkemesi'nin açık rızayı da esas kural niteliği taşıyan bir işleme şartı olarak kabul ettiği görülmektedir.

Bu doğrultuda, açık rıza ve diğer hukuki işleme şartlarının hiyerarşik ilişkileri bakımından Kurum ile Anayasa Mahkemesi'nin yorumları farklı olmuştur.

Kurum'un 23 Mayıs 2018 tarihinde düzenlemiş olduğu "6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) Karşılaştırılması" başlıklı Çarşamba Semineri'nde, *"Aynı anda işleme nedeni varken açık rıza almak hukuka aykırı olarak kabul edilir mi?"* sorusuna yönelik olarak, *"Öncelikli olan işleme nedenine bakmaktır, her durumda açık rıza almaya gerek yok. İşleme nedenleri yoksa açık rıza alınmalıdır ancak her olay kendi içerisinde ayrıca değerlendirileceği için, işleme nedeni varken açık rıza almak doğrudan hukuka aykırı denilemez."* şeklinde verdiği cevaptan ise, alınan rızayı baştan ve her halde geçersiz saymayıp, vaka bazında değerlendirme yapacağı anlaşılmıştır.

Veri sahibi kadar veri sorumlusunun hak ve menfaatleri açısından ve uygulamanın da belirli bir yönde ilerlemesi için, açık rızanın diğer veri işleme şartları karşısındaki yerine dair yorum ve değerlendirmeleri etraflıca ele almak ve bu konuda bir fikir / yorum birliğine varmak gerekli ve önemlidir. Platform toplantılarında yapılan uzun ve kapsamlı tartışmalar doğrultusunda;

a. KVKK gibi uygulaması yeni yeni şekillenmekte olan bir düzenleme karşısında, veri sorumlularının özellikle bazı muğlâk durumlarda bir tür garanti olarak rıza almalarına - öncesinde sağlıklı aydınlatma yapılmış olmak kaydıyla - *geçersiz* işlem denmesinin bu aşamada ağır bir sonuç olduğu,

[2] Anılan Kararın 42. Paragrafında yer alan ifadeler.

b. İşleme şartlarının arasında bir hiyerarşi olmaması gerektiği, T.C. Anayasası'nın ilgili hükmünde de bir hiyerarşi bulunmadığı ve rızanın geri çekilmesi halinde diğer işleme şartlarına dayanarak veri işleme faaliyetinin sürdürülebileceği,

c. Ancak, bu durumun baştan veri sahibi tarafından da bilinmesi ve sonuçlarının irdelenmesinin gerekli olduğu,

d. Bu bağlamda veri sahibine sunulacak aydınlatma yükümlülüğünün içeriğinin çok önemli olacağı,

e. Veri sahiplerinin bir yanılgıya düşmesinin önüne geçmek için rızanın hangi sebeple alındığının aydınlatma metninde açıkça baştan yazılmasının, rızanın geri çekilmesi halinde ise, hangi verilere ilişkin olarak işlemenin devam edeceği ve hangilerinin duracağının açıkça bildirilmesinin, alınan rızanın yanıltıcı ve geçersiz kabul edilmemesi adına bir çözüm olabileceği tespit ve önerileri yapılmıştır.

Bu noktada yer yer kullanılmakta olan "battaniye rıza", "rıza kirliliği", "yanıltıcı rıza", "geçersiz rıza" ve "gereksiz rıza" kavramlarının Kurum tarafından tanımlanmasına ihtiyaç olduğu belirtilmiştir.

Öte yandan, açık rıza dışındaki işleme şartlarının - özellikle bazılarının - kapsamının tam olarak belirli olmaması ve bu nedenle veri sorumlularının kendilerini güvence altına almak amacıyla açık rıza yoluna başvurma eğilimi gösterdikleri bilinmektedir. Kurum'un bu konuda da bir görüş bildirmesine ihtiyaç vardır, nitekim Avrupa'daki çözümlerin bu şekilde oluştuğu belirtilmiştir.

Veri sorumlularının kendilerini güvence altına almak amacıyla ayrıca açık rızaya başvurması hali, genellikle meşru menfaate dayanan işleme nedeni ile birlikte görülmektedir. "Meşru menfaat" ifadesinin oldukça geniş, sübjektif ve yoruma açık olması, GDPR ve KVKK kapsamında düzenlenen meşru menfaat şartında bulunan "zorunluluk/gereklilik" farkları, meşru menfaatin yalnızca veri sorumlusunun meşru menfaati olarak mı yoksa ilgili kişinin meşru menfaati ile birlikte mi dikkate alınacağı gibi hususlara açıklık getirilmesine ihtiyaç duyulmaktadır.

KVKK ile uyumunu tamamlamış, makul bir çaba içinde olduğu görülen veri sorumlularının, veri sahiplerini hiçbir şekilde yanıltmadan, sadece konunun belirsizliklerine karşı güvence sağlamak gayesiyle almış oldukları rızaların "geçersiz" veya "battaniye" rıza olarak değerlendirilmek yerine, duruma göre en fazla "gereksiz" olarak kabul edilmelerinin KVKK'nın amacı ile de uyumlu olacağı düşünülmektedir.

Rıza kirliliği meselesine ilişkin olarak ise, bir veri sorumlusunun, tek bir veri işleme faaliyeti için müşterisinin işlem yaptığı farklı platformlarda (bankamatik, şube gibi) her seferinde tekrar rıza almasının *rıza kirliliği* olarak tanımlanabileceği ifade edilmiştir.

Battaniye rıza ve *geçersiz rıza* kavramlarının ise aynı küme altında değerlendirilebileceği belirtilmiştir. Bu doğrultuda, *battaniye rıza* kavramının KVKK'nın 4. Maddesine doğrudan aykırı olduğu; çünkü veri sahibinden olası her veri işleme faaliyeti için tek bir rıza alınması anlamına geleceği ifade edilmiştir. *Geçersiz rıza* kavramına örnek olarak da, Whatsapp'ın kullanıcı politikası verilebilir, zira Whatsapp'ın kullanıcı politikasında politikanın her zaman veri sahibine haber vermeden değiştirilebileceğinin ifade edildiği belirtilmiştir. Bunların yanında *yanıltıcı rıza* kavramının ise, kasıtlı olarak yapılmış bir eylemi gerektirdiği ve kişinin iradesini sakatlama amacıyla alınan rızanın *yanıltıcı* nitelikte olacağı söylenmiştir.

Öte yandan, "açık rıza varsa her türlü veriyi işleyebilirsin, hukuka uygunluk sebepleri varsa yalnızca o amaçla sınırlı verileri işleyebilirsin" şeklindeki bir değerlendirmenin hatalı ve KVKK'nın temel ilkelerini aykırı olacağı, rıza alınsa dahi veri işleme faaliyetinin KVKK'nın temel ilkelerine aykırı olamayacağı açıktır.

Esasen "gereksiz rıza" kavramının Kurum tarafından hiç sarf edilmemiş olduğuna dikkat çekilerek, yukarıda anlatılanlar kapsamında, diğer işleme şartlarının yanında alınmış, ancak doğru aydınlatma metninin kullanılması yoluyla veri sahibini yanıltıcı herhangi bir etki doğurmayan bir açık rızanın, en fazla "gereksiz" olarak nitelendirilmesine dair görüşün Kurum'a sunulabileceği ve bu konuda da bir ilke kararına ihtiyaç duyulduğu belirtilmiştir.

11. Açık Rızanın Hizmetin Ön Şartı Yapılması Halinin Kurum'un Yayınladığı Özet Kararlar Işığında Değerlendirilmesi; *e-ticaret uygulamaları açısından değerlendirmeler*

ÖZET: Konu 24 Mayıs 2018 tarihli Platform toplantısında ele alınmıştır. Açık rızanın hizmet şartına bağlanmasına ilişkin olarak, veri işleme faaliyetinin hizmetin sunulabilmesi için gerekli olduğu durumlarda, veri işleme şartlarından sözleşmenin ifası kapsamında kalınacak ve bu nedenle açık rızanın hizmetin ön şartı yapılmaması doğru olacaktır. Hizmetin temel seviyede sunumu için işlenmesi gerekli olmayan ancak, taraflara ilave menfaatler sağlayabilecek olan ek hizmetlerin sunulabilmesi amacıyla toplanacak veriler yönünden ise, açık rıza alma yoluna başvurulabilecektir. Sözleşmenin asli unsurlarının bu kapsamda her somut olay için ayrıca belirlenmesi gerekli ve diğer taraftan özel nitelikli veriler açısından sözleşmenin ifası için zorunlu olsa bile açık rıza alınması yerinde olacaktır.

Yapılan Platform toplantısında, Kurum'un, daha önce katılmış olduğu etkinliklerde açıkça, "açık rızanın hizmetin ön şartı olarak getirilemeyeceğini, ancak sadakat kartı gibi uygulamalar açısından açık rızaya başvurulabileceğini" belirtmiş olduğuna dikkat çekilerek, Kurul'un yayımlamış olduğu karar özetlerinde de açık rızanın hizmet şartına bağlanamayacağının yine açıkça belirtilmiş olduğu ifade edilmiştir. Kurul'un yaklaşımı doğrultusunda, açık rızanın hizmet şartına bağlanması ve ayrıca esasında kendi içinde bir tür sözleşmesel ilişki olan sadakat kart uygulamalarının nasıl değerlendirilebileceği tartışılmıştır.

"Hizmetin ifası" kavramının oldukça geniş bir kavram olduğuna dikkat çekilerek, bir elektrik dağıtım şirketi örneğinde olduğu gibi, alternatif hizmet sağlayıcılarının bulunmadığı yoğun pazarlarda, açık rızanın hizmet şartına bağlanmasının hukuka aykırı olacağı ifade edilmiştir. Ancak bizatihi veri sorumlusu tarafından sunulan değerin, o verilerin işlenmesinden kaynaklı olarak sunulabilecek bir değer olması ihtimalinde ise, temel prensiplere aykırı olmamak kaydıyla, açık rıza aranabileceği belirtilmiştir.

Aynı doğrultuda alternatif hizmet sağlayıcılarının bulunduğu pazarlarda bizatihi hizmetin bir parçası olarak işlenen veriler için, temel ilkelere uygun olmak şartıyla, hizmetin gerekliliği uyarınca açık rıza alınabileceği ifade edilmiştir. Bu kapsamda, özellikle sözleşmenin asli

konusunun ne olduğunun tespiti önemli olacaktır. Yapılan tartışmalar etrafında, sözleşmenin asıl konu ve amacını aşan ve sözleşmenin ifası kapsamında gerekli tutulamayacak veri işleme faaliyetleri açısından açık rıza alınması gerekeceği belirtilmiştir.

Öte yandan, kişisel verilerin işlenmesi suretiyle tüketicilerin davranışlarını belirleme algoritmalarının hizmetin kolaylaştırılması için mi yoksa tüketiciye daha çok ürün satmak için mi yaratıldıkları tartışılabilir olsa da, dünyanın hızla tekilleşmeye doğru gittiği ve buna karşı durmanın imkânsız olduğu gerçeği de kabul edilmelidir. Bu durum karşısında, tüketicilerin kişisel verilerinin işlenmesinin hizmetin kalitesi açısından pek çok yararının da bulunduğu ve önemli olanın bu tür teknolojik değişimlere karşı tamamen kapanmak yerine, temel ilkelerden sapmadan, bu gelişmelere uyumlu bir şekilde yorum yapmak olduğu ifade edilmiştir. Aynı cookie politikalarında olduğu gibi, sözleşmenin ifası için zorunlu unsur olan işleme faaliyetlerinin sözleşmenin ifası kapsamında tutulması, bunu aşan unsurlar için rıza alınması yoluna gidilmeli ve ancak her zaman tüm işleme faaliyetlerinin açık bir şekilde aydınlatma metninde yer alması gereklidir.

Buna karşın, özel hukukta bir sorumluluğun doğması için mutlaka maddi veya manevi bir zararın doğması şartının arandığı, ancak ceza hukukunda böyle bir zorunluluğun bulunmadığına dikkat çekilmiştir. Ceza hukuku kapsamında kişinin cezalandırılması için tehlikenin varlığının dahi yeterli olduğu ve aynı şekilde idari para cezalarının verilmesi için de zararın oluşması şartının aranmadığı ifade edilmiştir. Bu bağlamda, "veri minimizasyonu" prensibinin de aynı şekilde potansiyel tehlikelerden uzak durmak amacıyla benimsenmesi gerektiğine dikkat çekilerek, önemli olanın kolay hayat ile kişisel mahremiyet arasında bir denge kurulması olduğu belirtilmiştir.

Bir e-ticaret sitesine alışveriş amacıyla giren bir kimsenin, yalnızca sözleşmenin ifası için zorunlu olan verilerini vererek alışverişini tamamlayabilme olanağının bulunması gerektiği ve bu şekilde "guest checkout" sistemlerini benimseyen platformların da gittikçe artmakta olduğuna dikkat çekilmiştir. Bunun yanında, böyle bir sistemi benimsemiş olan bir e-ticaret sitesinin, her alışverişinde tekrar verilerini girmek istemeyen müşterilerine verdiği hizmeti kolaylaştırmak için bir üyelik seçeneği sunması durumunda, üyelerden rıza alınmasının gerekli olup olmayacağının da tartışmalı olduğu ve bu durumun sözleşmenin ifası olarak nitelendirilebileceği belirtilmiştir.

Tartışmalar sırasında, eskiden, "payment by data" kavramının var olduğu ve belirli bir hizmet için para vermeyen kişinin, o hizmeti verileri ile satın almakta olduğunun kabul edildiği ve ayrıca rızaya gerek duyulmadığı ve aynı doğrultuda Direktif zamanında da zımni rızanın kabul edildiği, ancak şu anda GDPR ve KVKK uyarınca zımni rızaların işlevsiz kaldığı ifade edilmiştir. Bu doğrultuda hâlihazırda üye olmadan alışveriş yapabilme imkânı sunan e-ticaret sitelerinin yaklaşımının doğru olduğu, bu kapsamda işlenen verilerin sözleşmenin ifası kapsamında rızaya gerek olmadan işlenebileceği, ancak orada da sözleşmenin zorunlu unsurlarının dışına çıkan verilerin talep edilmesi halinde rızaya ihtiyaç duyulacağı görüşü bildirilmiştir.

12.GDPR'ın Türkiye'ye Etkileri Üzerine ve Uygulamada Ortaya Çıkan Sorunlara dair KVKK ve GDPR Karşılaştırmalı Değerlendirme

ÖZET: Konu 24 Mayıs 2018 tarihli Platform toplantısında ele alınmıştır. GDPR ile KVKK arasında sağlık verilerinin işlenmesi, veri güvenliğinin ihlali, yurtdışına aktarım, kılık kıyafete ilişkin verilerin özel niteliği gibi konularda ve bunlarla sınırlı olmaksızın aydınlatma yükümlülüğü ve rızanın şekline ilişkin hususlarda farklar bulunduğu görülmektedir. İlk bakışta birbirine oldukça benzer görünen işleme şartları arasında da önemli farklılıklar olduğu, bunların bir ihtimal yazım tekniğinden kaynaklanıyor olabileceği düşünülmektedir. Nitekim Kurul'un çeşitli uygulamalarında GDPR yorumlarını dikkate aldığı görülmektedir.

108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, özellikle uluslararası veri aktarımına ilişkin önemli düzenlemeler içeren, AB Konseyi üyesi olmayan devletlere de açık bir düzenleme olarak kişisel verilerin korunması konusunda çok önemli bir uluslararası belgedir. 25 Haziran 2018'de onaylanması beklenen güncellenmiş halinin Türkiye tarafından onaylanması halinde, uygulama için önemli bir kaynak olabileceği düşünülmektedir.

GDPR'nin sıklıkla gündeme geldiği alan, uluslararası şirketlerin Türkiye iştirakleridir. Bu kapsamda, Türkiye'de kurulu yabancı sermayeli şirketlerin veri işleme faaliyetleri KVKK'ya tabi olmakla birlikte, Avrupa menşeli ana ortakların kendi GDPR uyumlarını tesis etmek amacıyla Türkiye iştiraklerinden de bekledikleri işlem ve süreçler olabilmektedir. Bu

bağlamda, yabancı sermayeli Türk şirketlerinin her iki düzenlemeyi de dikkate almaları gerekliliği doğabilmektedir.

Türkiye'de, özellikle bazı sektörlerin GDPR'ye uyumluluk açısından da kendilerini test etmeleri faydalı olabilecektir, bu sektörlere örnek olarak elektronik ticaret ve pazarlama, turizm, sağlık, dijital reklam, web sitesi yönetimi, sosyal medya yönetimi, eğitim sektörü gibi yurtdışına ağırlıklı olarak hizmet veren sektörler sayılabilir.

Platform toplantısında, Türkiye'deki yabancı ortaklı şirketlerin GDPR uyumları açısından Binding Corporate Rules ("BCR") kullanımına ilişkin görüşleri gündeme geldiğinde, bir grup uygulamacı BCR'nin oldukça yararlı olduğunu belirtirken, diğer bir grup ise BCR izinlerinin bir iki seneye yayılan bir sürede çıkması ve masraflı olması nedeniyle tercih edilen bir yöntem olmadığını belirtmişlerdir.

Toplantı katılımcılarının bazıları, uluslararası büyük firmaların, Türkiye'de bulunan veri işleyenlere kendi Avrupa Birliği uygulamalarını ve şirket içi kurallarını dayatmak istediklerine dikkat çekerek, bu süreçlerin Türkiye'de bulunan şirketlere ciddi yükümlülükler getirdiği, ancak şirketlerin de bu büyük şirketler ile çalışabilmek için doğrudan ilgili taahhütleri verdiklerini gündeme getirmişlerdir.

Bilindiği kadarıyla, Kurum, BCR'ye olumlu baktığını ifade etmiş olsa da, düzenleme KVKK'da yer almadığından, BCR'nin Türkiye'den dışarı çıkan verilere ilişkin uygulamasının oldukça kısıtlı olduğu, halihazırda Türkiye'deki yaygın sistemin, yurtdışına veri aktarımı konusunda ya açık rıza ya da Kurul izni olduğu belirtilmiştir.

Toplantıda bir diğer gündem maddesi olarak, 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ("Protokol") ele alınmıştır. Protokol'ün 1981 yılında kabul edilmesinin ardından, ilkelerin ulusal hukuka geçirilmesi zorunluluğu nedeniyle KVKK'nın yürürlüğe girdiği 2016 yılına kadar Türkiye iç hukukuna dahil olamadığı, ancak artık Protokol'ün Anayasa madde 90 uyarınca kanun hükmünde olduğu belirtilerek, halihazırda yenilenmekte olan Protokol'ün, önümüzdeki yıllarda çok daha fazla önem kazanacağına, nitekim özellikle uluslararası veri aktarımına ilişkin önemli düzenlemeler içerdiği ve kapsamının GDPR'dan çok daha geniş olduğuna, hatta Protokol'ün sadece AB Konseyi üye devletlerine değil, diğer ülkelere de açık olduğuna ve halihazırda

kişisel verilerin korunması konusunda bağlayıcı uluslararası nitelikteki tek metin olduğuna dikkat çekilmiştir. 25 Haziran'da onaylanması beklenen güncellenmiş Protokol'ün Türkiye tarafından da onaylanması halinde, mahkemeler nezdinde de önemli bir kaynak olarak kullanılabileceğinin düşünüldüğü belirtilmiştir. Bu doğrultuda, Platform'un daha önceki tartışmalarında da ele alınan, rızanın diğer işleme şartları karşısındaki statüsünün dahi Protokol'ün yenilenmiş versiyonu ile daha fazla aydınlığa kavuşabileceği düşünülmektedir.

Başka bir gündem maddesi olarak, GDPR ile KVKK arasında sağlık verilerinin işlenmesi, veri güvenliğinin ihlali, yurtdışına aktarım, kılık kıyafete ilişkin verilerin özel niteliği gibi konularda farklar bulunduğuna dikkat çekilmiştir. Bu bağlamda GDPR'nin veri güvenliğine ilişkin düzenlemelerinin kapsamlı ve kademeli yapısının Türkiye uygulaması için de örnek olabileceğine dair görüşler bildirilmiştir. Bu doğrultuda, öncelikle GDPR madde 4/12 uyarınca veri ihlalinin "iletilen, saklanan veya sair şekilde işlenen kişisel verilerin kazara veya hukuka aykırı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlal" olarak tanımlanmış olduğu, ancak KVKK'da bu şekilde bir tanımın yapılmadığı ifade edilmiştir. Ayrıca, GDPR'de hangi durumlarda ne kadar idari para cezası düzenleneceğine dair kriterlere yer verilmiş olduğuna dikkat çekilmiştir.

Öte yandan toplantı katılımcılarından bazıları daha önce bir IAPP eğitiminde yapılan bir tartışmaya dikkat çekmişledir. İlgili tartışmada, uluslararası bir grup şirketin bünyesinde yer alan ve Türkiye'de bulunan bir şirketin yurt dışında bulunan bulut hizmetini veya veri merkezini kullanması durumunda; eğer veri işleyen (bulut hizmet sağlayıcısı gibi) Avrupa'da ise, veri sorumlusunun Türkiye'de bulunsa dahi GDPR'ye tabi olabileceğinin ifade edildiği belirtilmiştir. 95/46 sayılı Direktif düzenlemesinin de bu yönde olduğu ifade edilmiştir.

Bununla birlikte, veri işleme faaliyetlerinin niteliğinden bağımsız olarak yalnızca veri işleyenin Avrupa'da mukim olması nedeniyle, Türkiye'de bulunan veri sorumlusunun özellikle veri ihlalleri bakımından GDPR'ye tabi olmasının fazla ileri bir yorum olabileceği düşünülmüştür.

GDPR ile KVKK arasında görülen farklılıklardan birinin de aydınlatma yükümlülüğünde ortaya çıktığına dikkat çekilerek, GDPR uyarınca ilgili kişinin kendi kişisel verilerinin ne şekilde işleneceğini hâlihazırda biliyor olması durumunda, veri sorumlusunun ayrıca aydınlatma yükümlülüğünün bulunmadığı ifade edilmiştir.

Bunların yanında, GDPR ile KVKK arasındaki en büyük farklılıklardan birinin özel nitelikli verilerin işlenmesi noktasında ortaya çıktığı ve GDPR'de özel nitelikli veriler için pek çok işlenme şartı öngörüldüğü, ancak KVKK'da az sayıdaki işleme şartı dışında özel nitelikli verilerin, özellikle sağlık verilerinin yalnızca açık rıza ile işlenebildiğine dikkat çekilmiştir.

Rızaya ilişkin GDPR tanımında yer alan "açık olumlu davranış" ifadesinin ise, bizdeki gibi bir rıza açıklaması anlamına gelmediği, nitekim örnek olarak bir internet sayfasında açıkça rıza butonuna tıklamayan ancak, bir sonraki sayfaya ilerleme şeklinde açık olumlu bir davranış gösteren kişinin, GDPR uyarınca rıza göstermiş olduğunun kabul edildiği belirtilmiştir.

GDPR ile KVKK arasıda kişisel veri işleme şartlarının farklılıkları kapsamında, Platformun önceki toplantılarında tartışılan konular tekrar gündeme getirilmiş, ilk bakışta birbirine oldukça benzer görünen işleme şartları arasında, önemli farklılıklar olduğu, bunların bir ihtimal yazım tekniğinden de kaynaklanıyor olabileceği belirtilmiştir. Nitekim Kurul'un da çeşitli uygulamalarında GDPR yorumlarını dikkate aldığının görüldüğü ifade edilmiştir.

*İşbu "Kişisel Verilerin Korunması Platformu Çalışma Notları" 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.