

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

**6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU
UYARINCA TÜRK TİCARET ŞİRKETLERİNİN
YÜKÜMLÜLÜKLERİ**

YÜKSEK LİSANS TEZİ

Yasin ÜSTÜN

Tez Danışmanı: Prof. Dr. Mehmet ERDEM

Aralık 2023

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANABİLİM DALI**

**6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU
UYARINCA TÜRK TİCARET ŞİRKETLERİNİN
YÜKÜMLÜLÜKLERİ**

YÜKSEK LİSANS TEZİ

Yasin ÜSTÜN

Tez Danışmanı: Prof. Dr. Mehmet ERDEM

Aralık 2023

ÖNSÖZ

Avukatlık mesleğini yapmaya başladığım ilk günden bugüne kadar Kişisel Verilerin Korunması Kanunu alanında birçok şirket ile çalışma fırsatına eriştim. Farklı sektörlerde faaliyet göstermelerine, farklı şehirlerde bulunmalarına rağmen birçok şirket yetkilisinin ve meslektaşımın bu süreçte hemen hemen aynı soruları sorduğunu, anlamlandırmakta sorun yaşadığı noktaların çok benzer olduğunu tespit ettim. Sahada edindiğim tecrübemi akademik çalışmalarına da yansıtmak, uygulamadaki eksiklikler ve sorunlara hukuki bir bakış açısı ile çözüm önerisi getirebilmek ve başta bu alana ilgi duyan herkese yol gösterici olabilmek amacıyla yüksek lisans tezimde, Türk ticaret şirketlerin kanun kapsamındaki yükümlülüklerini incelemeye karar verdim. Çok kıymetli hocalarımdan birçok yayına imza attığı Kişisel Verilerin Korunması Hukuku alanına ufak da olsa bir katkı sağlayabilmek gayesiyle çıktığım bu yolda benden desteğini esirgemeyen ve yanımda olan kişilere de ayrıca bu bölümde teşekkür etmek isterim.

Tezin teknik ve bilimsel açıdan yeterli olgunluğa erişebilmesini sağlayan, bilgisi ile yoluma ışık tutan ve yazım sürecinde desteğini her zaman hissettiğim tez danışmanım ve saygıdeğer hocam Prof. Dr. Mehmet ERDEM başta olmak üzere Galatasaray Üniversitesi Hukuk Fakültesi'nin değerli tüm hocalarına, aldığım her kararda yanımda olduğu gibi tezimi yazarken de yanımda olan ve aynı mesleği yapmaktan gurur duyduğum sevgili eşim Ayşe Nida GÜNAL ÜSTÜN'e, beni bugünlere getiren sevgili annem Ayşe ÜSTÜN'e, aldığım her kararda arkamda duran ve yüksek lisans sürecimde de bana her türlü desteği sağlayan babam Şevket ÜSTÜN'e, en büyük destekçim, çok sevgili kız kardeşim Elif ÜSTÜN'e ve adımı anmadığım ancak desteklerini her daim hissettiğim tüm hocalarıma, aile üyelerime ve dostlarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

ÖNSÖZ.....	ii
İÇİNDEKİLER	iii
KISALTMALAR.....	vi
RÈSUMÈ.....	viii
ABSTRACT	xii
ÖZET.....	xvi
GİRİŞ	1
I- Kişisel Verilerin Korunması Gereksinimi	1
II-Uluslararası Düzenlemeler	2
III-Ulusal Düzenlemeler.....	6
IV-Türk Hukukundaki Düzenlemeler.....	11
V-Çalışmanın Amacı, Kapsamı ve İnceleme Planı	13

BİRİNCİ BÖLÜM

KANUNA İLİŞKİN TEMEL KAVRAMLAR, TEMEL İLKELER VE KANUNDA YER ALAN KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

I-TEMEL KAVRAMLAR.....	17
A-Kişisel Veri.....	17
1-Kişisel Verinin Unsurları	17
a-Bir Verinin Varlığı.....	17
b-Verinin Gerçek Kişiyne İlişkin Olması.....	18
c-Verinin Kişiyi Belirli Kılması veya Verinin Kişiyi Belirlenebilir Kılması..	20
B-Özel Nitelikli Kişisel Veri	22
C-Veri Kayıt Sistemi	24
Ç-Kişisel Verilerin İşlenmesi	27
D-İlgili Kişi	28
E-Veri Sorumlusu	29
F-Veri İşleyen	32
G-Açık Rıza	33

1-Açık Rızanın Unsurları	34
a-Belirli Bir Konuya İlişkin Olma.....	34
b-Bilgilendirmeye Dayalı Olma.....	35
c-Özgür İradeyle Açıklanmış Olma.....	36
H-Veri Sorumluları Sicili (VERBİS)	41
I-Kişisel Verilerin İmhası	42
1-Kişisel Verilerin Anonim Hale Getirilmesi	42
2-Kişisel Verilerin Silinmesi	43
3-Kişisel Verilerin Yok Edilmesi.....	44
II-KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER.....	44
A-Hukuka ve Dürüstlük Kuralına Uygun Olma	45
B-Doğru ve Gerektiğinde Güncel Olma	47
C-Belirli, Açık ve Meşru Amaçlar İçin İşlenme.....	48
Ç-İşlendikleri Amaçla Bağlantılı, Ölçülü ve Sınırlı Olma	51
D-İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme	56
III- KİŞİSEL VERİLERİN İŞLENME ŞARTLARI	58
A-KİŞİSEL VERİLERİN İŞLENME ŞARTLARI	58
1-Açık Rıza	58
2-Kanunlarda Açıkça Öngörülmesi.....	64
3-Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin Ya Da Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması	67
4-Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması	68
5-Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması	70
6-İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması	72
7-Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması	74
8-İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması.....	76
B-ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI.....	85
1-Sağlık ve Cinsel Hayata İlişkin Özel Nitelikli Kişisel Veriler Bakımından ...	85
2-Sağlık ve Cinsel Hayat Dışındaki Özel Nitelikli Kişisel Veriler Bakımından	88

İKİNCİ BÖLÜM

TÜRK TİCARET ŞİRKETLERİNİN 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ YÜKÜMLÜLÜKLERİ

I-AYDINLATMA YÜKÜMLÜLÜĞÜ.....	90
A-Aydınlatma Yükümlülüğünü Yerine Getirecek Kişi	91
B-Aydınlatma Yükümlülüğünün Kapsamı	91
C-Aydınlatma Yükümlülüğünün Yerine Getirileceği Zaman.....	97
D-Aydınlatma Yükümlülüğüne İlişkin Diğer Usul ve Esaslar	98
II-VERBİS KAYIT YÜKÜMLÜLÜĞÜ	105
A-VERBİS'E KAYDOLMASI GEREKEN VERİ SORUMLULARI	106
B-VERBİS KAYIT YÜKÜMLÜLÜĞÜNÜN DOĞDUĞU VE YÜKÜMLÜLÜĞÜN YERİNE GETİRİLDİĞİ AN	109
III-VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER	111
A-GENEL OLARAK.....	111
B-KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK İŞLENMESİNİ ÖNLEME YÜKÜMLÜLÜĞÜ.....	112
C-KİŞİSEL VERİLERE HUKUKA AYKIRI OLARAK ERİŞİLMESİNİ ÖNLEME YÜKÜMLÜLÜĞÜ.....	123
Ç-KİŞİSEL VERİLERİN MUHAFAZASINI SAĞLAMA YÜKÜMLÜLÜĞÜ. 127	
D-VERİ İHLALİ BİLDİRİM YÜKÜMLÜLÜĞÜ	129
IV-İLGİLİ KİŞİLER TARAFINDAN YAPILAN BAŞVURULARIN CEVAPLANMASI YÜKÜMLÜLÜĞÜ	132
V-KURUL KARARLARININ YERİNE GETİRİLMESİ YÜKÜMLÜLÜĞÜ	140
VI-KİŞİSEL VERİLERİN İMHA EDİLMESİ YÜKÜMLÜLÜĞÜ	142
VII- AYDINLATMA YÜKÜMLÜLÜĞÜNÜN TTK M. 1524 BAĞLAMINDA DEĞERLENDİRİLMESİ	151
VIII- KİŞİSEL VERİLERİN İŞLENMESİ VE İMHASI SÜREÇLERİNİN TTK M. 64 VE TTK M. 82 BAĞLAMINDA DEĞERLENDİRİLMESİ	153
IX- VERİ İHLALİ BİLDİRİM YÜKÜMLÜLÜĞÜNÜN TTK M. 82/ F. 7 BAĞLAMINDA DEĞERLENDİRİLMESİ	155
X- KVKK KAPSAMINDAKİ YÜKÜMLÜLÜKLERİNİ YERİNE GETİRMEYEN TÜRK TİCARET ŞİRKETİNİN EYLEMLERİNİN TTK M. 55/ F. 1/ E BENDİ UYARINCA HAKSIZ REKABET BAĞLAMINDA İNCELENMESİ	156
XI- KVKK KAPSAMINDAKİ SORUMLULUĞUN TESPİTİNDE TTK M. 366/ F. 2 VE TTK M.375 HÜKÜMLERİNİN ETKİSİ	160
SONUÇ.....	165
KAYNAKÇA.....	170
ÖZGEÇMİŞ.....	176

KISALTMALAR

108 Sayılı Sözleşme	:108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
a.g.e.	:Adı geçen eser
AB	:Avrupa Birliği
BM	:Birleşmiş Milletler
Bkz	:Bakınız
C.	:Cilt
Direktif	:95/46EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif
f.	:Fıkra
GDPR	:General Data Protection Regulation
ICO	:İngiltere Veri Koruma Otoritesi
KVKK	:6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kurum	:Kişisel Verileri Koruma Kurumu
Kurul	:Kişisel Verileri Koruma Kurulu
m.	:Madde
OECD	:Organisation for Economic Co-Operation and Development
RG	:Resmi Gazete
S.	:Sayı
s.	:Sayfa
T.	:Tarih

TMK	:Türk Medeni Kanunu
TTK	:Türk Ticaret Kanunu
vd	:ve devamı
VERBİS	:Veri Sorumluları Sicili



RÉSUMÉ

Le premier texte législatif de nature générale régissant la protection des données personnelles en Turquie est la loi n° 6698 sur la protection des données personnelles. Cette loi a été publiée dans le Journal officiel le 7 avril 2016. Conformément au système prévu par cette loi, la Commission de Protection des Données Personnelles a été créée et certaines missions et compétences lui ont été attribuées. Les décisions de la Commission de Protection des Données Personnelles ont eu une influence considérable sur la généralisation de la protection des données personnelles en Turquie. De plus, le montant élevé des amendes infligées par la Commission de Protection des Données Personnelles, ainsi que sa publication régulière de ses décisions, ont contribué à maintenir l'actualité du sujet et à accroître la sensibilisation à cette question. Lorsque l'on examine les décisions de la Commission de Protection des Données Personnelles, on constate que les responsables de traitement de données auxquels des sanctions administratives sont infligées sont généralement des entreprises. En particulier, il convient de noter que, à l'exception de certaines entreprises étrangères spécifiques, la grande majorité des sujets exposés aux sanctions, sont des entreprises turques. Par conséquent, nous avons préféré aborder les obligations à respecter par un responsable de traitement de données dans le contexte de la Loi sur la Protection des Données Personnelles, en mettant l'accent sur les entreprises turques, plutôt que d'examiner les institutions publiques, les personnes physiques et les entreprises étrangères, afin de ne pas disperser le sujet. En raison de cette approche, nous avons défini le sujet de notre thèse comme "Les Obligations des Entreprises Turques en vertu de la loi N° 6698 sur la Protection des Données Personnelles". Bien que nous utilisions fréquemment la notion de responsable de traitement dans notre étude, nous avons essayé de donner autant que possible nos exemples à travers une entreprise. De même, dans la plupart des décisions que nous avons traitées, nous avons fait de notre mieux pour que l'entreprise sanctionnée soit une entreprise, afin qu'elle serve également d'exemple.

La section d'introduction de notre étude, nous avons évoqué l'histoire du droit de la protection des données personnelles, les sources nationales et internationales. En particulier, étant donné que différentes approches ont été adoptées dans le monde en ce qui concerne la protection des données personnelles, nous avons d'abord examiné l'émergence du droit à la protection des données personnelles, puis son développement en Turquie et dans d'autres pays, et enfin son évolution dans le droit international.

Dans la première partie de notre travail, nous avons examiné les notions de base, les principes fondamentaux et les conditions de traitement des données personnelles prévues par la loi. Nous avons examiné en détail les concepts de base, car nous avons constaté que de nombreuses défenses présentées à la Commission de Protection des Données Personnelles par les entreprises exposées au risque de sanctions pécuniaires administratives en vertu de la loi sur la protection des données personnelles reposent sur ces concepts fondamentaux. Par exemple, une entreprise qui risque de faire l'objet de sanctions, peut prétendre qu'elle n'est pas responsable du traitement des données ou l'activité n'est pas une activité de traitement des données

personnelles, car il n'y a pas de système d'enregistrement de données. La question de savoir qui est le responsable de traitement et qui est le sous-traitant est un sujet qui a été inclus dans de nombreuses décisions, guides et annonces de la Commission de Protection des Données Personnelles. En fait, dans certaines affaires, il peut même être discuté s'il existe ou non des données personnelles. Il est donc essentiel de bien comprendre les concepts de base dans le domaine du droit à la protection des données personnelles. Une compréhension adéquate des concepts de base nous permettra également de répondre aux questions de savoir qui doit remplir les obligations prévues par la loi et s'il existe une obligation ou non. Par exemple, si une action n'est pas qualifiée de traitement de données personnelles, il ne sera pas nécessaire de s'appuyer sur les conditions de traitement des données spécifiées dans la loi. D'autre part, si une activité de traitement de données est en cours, elle devra être fondée sur l'une des conditions de traitement des données. Ainsi, la première question à examiner est de savoir si l'action de l'entreprise est qualifiée de traitement de données personnelles. Ou si la Commission de Protection des Données Personnelles souhaite imposer une sanction pécuniaire administrative dans un litige donné, le responsable de traitement est la partie concernée. Pour cette raison, la première chose que la Commission de Protection des Données Personnelles doit déterminer est qui est le responsable de traitement. Dans certaines affaires, il peut être très difficile d'identifier qui est le responsable de traitement. Par conséquent, les concepts de base revêtent une importance particulière dans la loi sur la protection des données personnelles, contrairement à d'autres lois. C'est pourquoi nous avons essayé de les aborder aussi en détail que possible.

Un autre sujet que nous avons abordé dans la première partie concerne les principes généraux. Les principes généraux ont été l'objet de nombreuses décisions de la Commission de Protection des Données Personnelles et ont été un sujet important qui a entraîné de nombreuses sanctions administratives contre les entreprises. Une raison de l'importance de ce sujet est que même si une entreprise se fonde sur l'une des conditions de traitement des données spécifiée par la loi, si l'activité de traitement des données n'est pas conforme aux principes généraux, le traitement des données personnelles effectué sera contraire à la loi. De plus, les principes généraux sont des principes qui doivent être pris en compte à chaque étape du traitement des données personnelles, de sorte qu'un responsable de traitement doit en réalité se demander constamment si son activité de traitement des données est conforme aux principes généraux. Dans cette partie de l'étude, nous avons particulièrement abordé la question des principes généraux à la lumière des décisions de la Commission de Protection des Données Personnelles. Étant donné que le sujet des principes est généralement abstrait, de nombreuses décisions ont été prises en compte dans cette partie de l'étude pour qu'elle puisse être concrétisée.

La dernière question que nous abordons dans la première partie concerne les conditions de traitement des données personnelles. En procédant à une distinction binaire, le législateur a réglementé les conditions de traitement des données personnelles de nature générale et les conditions de traitement des données personnelles de nature spéciale. Dans cette partie de notre étude, nous avons abordé le sujet à partir de la distinction fondamentale faite par le législateur. Par ailleurs, dans cette partie, nous avons essayé de présenter des exemples à la lumière des décisions de la Commission de Protection des Données Personnelles. En particulier, dans de nombreuses décisions de la Commission de Protection des Données Personnelles, nous avons observé que la question la plus difficile pour les entreprises dans la pratique est de déterminer correctement les conditions de traitement des données personnelles, car

il est constamment répété que le responsable du traitement des données peut traiter des données personnelles sans se fonder sur aucune condition de traitement, ou même sans obtenir un consentement explicite, bien que cela soit nécessaire. En pratique, je tiens à souligner que les questions que j'ai reçues tant de la part des entreprises avec lesquelles j'ai eu l'occasion de travailler et de mes collègues qui ont fourni des services de conseil en cette matière notamment sont de savoir si un consentement exprès est requis ou si le traitement des données peuvent être traités dans le cadre d'intérêts légitimes. Par conséquent, pour déterminer si l'action entreprise est qualifiée de traitement de données personnelles, la première étape nécessite une compréhension correcte des conditions de traitement des données personnelles. Pour les raisons que nous avons mentionnées, nous avons essayé de progresser avec des exemples dans cette partie de l'étude, en nous appuyant sur les décisions de la Commission de Protection des Données Personnelles.

Dans la deuxième partie de notre étude, nous avons examiné les obligations des entreprises commerciales turques en vertu de la Loi sur la Protection des Données Personnelles n° 6698, qui constitue également le titre de notre thèse. Dans cette section, nous avons abordé les obligations liées à l'obligation d'informer, à l'obligation d'enregistrement dans le VERBİS, aux obligations liées à la sécurité des données, à l'obligation de répondre aux demandes formulées par les personnes concernées, à l'obligation de se conformer aux décisions de l'organisme de protection des données personnelles, et à l'obligation de détruire les données. Enfin, nous avons évalué ces obligations à la lumière des articles 1524, 64, 82, 55, 366 et 375 du Code de commerce turc n° 6102.

Dans la deuxième partie de notre travail, nous avons abordé les obligations des entreprises turques en vertu de la loi n° 6698 sur la protection des données personnelles, qui constituent le titre de notre thèse. L'un des premiers engagements que nous abordons dans cette section est l'obligation de prévenir le traitement illicite des données personnelles. Au cœur de cette obligation se trouve la responsabilité du responsable du traitement de déterminer correctement la base légale du traitement des données et d'effectuer les activités de traitement en conséquence. Dans ce sens, nous avons d'abord expliqué les attentes du législateur à l'égard des entreprises commerciales turques, ce qui devrait être fait. Ensuite, nous avons abordé les situations dans lesquelles cette obligation a été violée à la lumière des décisions de la Commission de Protection des Données Personnelles. En outre, dans cette section, nous avons accordé une attention particulière à l'obligation de prévenir l'accès illégal aux données personnelles. En particulier, nous avons examiné cette question en détaillant les mesures administratives et techniques spécifiques que les entreprises doivent prendre, conformément à la loi sur la protection des données personnelles. Il convient de noter que si un accès illégal à des données personnelles est obtenu, la Commission de Protection des Données Personnelles impose systématiquement des sanctions pécuniaires administratives, en se référant au non-respect de cette obligation. Par conséquent, dans les cas concernés par les décisions, nous avons cherché à identifier ce qui n'avait pas été correctement fait et à proposer des solutions. Car la Commission de Protection des Données Personnelles dans la plupart de ses décisions se limite à constater l'illégalité sans proposer de solution. Les points où elle constate généralement l'illégalité sont souvent les méthodes et procédures couramment utilisées par les entreprises commerciales turques. Ainsi, dans cette section de notre travail, nous avons également inclus nos recommandations pour le respect de cette obligation.

Au cœur de notre étude se trouve la nécessité de se concentrer sur les obligations, mais il est essentiel de souligner que ce sont des personnes physiques qui

rempliront cette obligation pour les entreprises commerciales turques. En revanche, l'entité susceptible de recevoir une amende administrative imposée par la Commission de Protection des Données Personnelles est toujours le responsable du traitement des données. Même si la violation résulte entièrement de la faute d'un employé, c'est l'entreprise qui en supportera les conséquences, ce qui conduit souvent au sujet du recours. Dans de tels cas, il est clair que l'entreprise peut recourir à son employé. D'autre part, bien qu'il n'y ait pas de violation évidente des données dans l'entreprise, aucune mesure n'a pu être prise dans le cadre du respect de la Loi sur la Protection des Données Personnelles; une étude peut avoir été réalisée mais incomplète, ou le cas le plus courant, une l'étude a peut-être été réalisée mais est restée sur papier. Dans de tels cas, nous avons tenté d'aborder la question de la responsabilité de manière générale, sans sortir du cadre de cette étude. Nous avons essayé d'évaluer le sujet en fonction de la structure dynamique des entreprises commerciales turques et des exigences de la vie commerciale. Il convient de noter que le risque de non-conformité à la loi sur la protection des données personnelles est extrêmement élevé dans le cadre de cette loi. Il est facile de détecter quand la violation est attribuable à la faute d'un employé. Cependant, il est plus difficile de déterminer qui est responsable en cas de négligence ou de lacunes plutôt que d'une violation flagrante de la loi. Par conséquent, à la fin de cette section, j'ai également partagé mes propres opinions, dans l'espoir de contribuer, même modestement, à ce domaine, sachant que mes connaissances sont comparables à une goutte d'eau dans l'océan par rapport à celles des experts du domaine.

Dans l'ensemble de notre travail, nous avons fréquemment fait référence aux guides publiés par l'Autorité de Protection des Données Personnelles et aux décisions de la Commission de Protection des Données Personnelles. Nous avons essayé de le faire dans toutes les parties de cette étude. Car, la loi qui constitue l'objet notre étude n'a que sept ans d'histoire. Compte tenu des décisions judiciaires sur la protection des données personnelles, il est entendu que les évaluations et les déterminations sont souvent faites conformément aux principes généraux plutôt qu'à la Loi sur la Protection des Données Personnelles n° 6698. La loi n'a été publiée que sept ans auparavant et le processus judiciaire en Turquie est souvent très long. Par conséquent, le domaine dans lequel nous avons mené notre étude n'est pas un domaine qui a fait l'objet de nombreuses décisions judiciaires. D'autre part, l'Autorité de Protection des Données Personnelles traite toutes ses décisions dans le cadre de la loi et publie de nombreux guides, annonces et vidéos pour rendre la loi compréhensible. Par conséquent, la source nous avons le plus profité dans notre étude est principalement constituée des ressources imprimées et numériques de l'Autorité de Protection des Données Personnelles.

En conclusion, nous avons essayé de répondre aux obligations des sociétés commerciales turques dans le cadre de la Loi sur la Protection des Données Personnelles, qui est très nouvelle pour notre pays, avec notre proposition de solution pratique à la lumière des explications théoriques, puis des avis du doctrine et enfin les décisions de la Commission de Protection des Données Personnelles.

ABSTRACT

The first law of general regulation regarding the protection of personal data in Turkey is the Law No. 6698 on the Protection of Personal Data. The law was published in the Official Gazette on 07.04.2016. In accordance with the system envisaged by the law, the Personal Data Protection Authority was established, and certain duties and power were granted to this authority. The decisions of the Personal Data Protection Authority have an impact on the widespread adoption of personal data protection law in our country. The revision of the Personal Data Protection Board decisions indicated that the data controller subject to administrative enforcement is usually a company. Besides certain foreign companies, the majority of the companies subjected to administrative enforcement are Turkish commercial companies. Therefore, we preferred to address the liabilities that a data controller must fulfill within the scope of the law on the protection of personal data with a special focus on Turkish commercial companies rather than discussing public institutions, individuals, and foreign companies to avoid diluting the topic. Consequently, we determined the subject of our thesis as "Obligations of Turkish Commercial Companies Pursuant to Law No. 6698 on the Protection of Personal Data." While we frequently use the concept of data controller in our study, we have attempted to provide the examples primarily based on a company. Likewise, in a significant portion of the decisions we discuss, we strive to use a company that has been subjected to sanctions as an example.

The introduction part of our study, deals with the historical background of personal data protection law, national and international sources. In particular, since different approaches have been adopted in the world in the field of personal data protection, we first addressed the emergence of personal data protection law, followed by its development in our country and other countries, and finally its development in international law.

The first part of our study deals with the fundamental concepts, basic principles and the personal data processing conditions under the law. We have tried to review the fundamental concepts comprehensively. Because we have identified that most of the defenses submitted by companies at risk of administrative fines under the Personal Data Protection Law were based on these fundamental concepts. For example, the company that is likely to be imposed a penalty may claim that it is not a data controller, that the action carried out to avoid the penalty did not involve processing personal data because there was no data recording system in place. Particularly, identity of the data controller and data processor has been addressed in many decisions, guidelines and announcements published by the Personal Data Protection Board. In some disputes, the very existence of personal data can be subject to debate. Therefore, a good understanding of the fundamental concepts in the field of personal data protection law is essential. A clear understanding of the fundamental concepts will also provide the answer to the questions of who will fulfill the obligations under the law and whether such obligations exist. For instance, when an action is not considered as a personal data processing activity, there is no need to rely on any data processing condition

specified in the law. Conversely, when there is a data processing activity, it would be necessary to rely on a data processing condition. Therefore, the first issue to be evaluated is whether the action performed will be considered as processing of personal data. Otherwise, when the Personal Data Protection Board intends to impose an administrative fine in a dispute that comes to its attention, the respondent is the data controller. Hence, the first thing that the Personal Data Protection Board needs to determine is the identity of the data controller. In certain cases, identifying the data controller can indeed be quite challenging. Therefore, unlike other laws, the fundamental concepts have a great importance in the context of the Personal Data Protection Law. Therefore, we have attempted to address these concepts in as much detail as possible.

The other topic addressed in the first section is the general principles. General principles have been the subject of many decisions of the Personal Data Protection Board and have caused many companies being subjected to administrative fines. One of the reasons for the importance of the subject is that, even if a data controller relies on a data processing condition specified in the law, if the data processing activity does not comply with the general principles, the data processing activity performed is unlawful. Moreover, since the general principles are required to be considered in every process within the scope of personal data processing activity, a data controller should constantly ask whether the transaction is in compliance with the general principles. In this section of the study, we have attempted to address the general principles, especially in the light of the decisions of the Personal Data Protection Board. Since the issue of principles is generally an abstract subject, many cases that have been the subject of many decisions have been discussed in this part of our study to make the study more concrete.

The final issue in the first section is the conditions for processing personal data. The legislator has regulated the conditions for the processing of personal data of general nature and the conditions for the processing of personal data of special nature separately by adopting a binary distinction. In this part of our study, we have addressed the issue based on the basic distinction made by the legislator. We have also attempted to present the issue with examples based on the decisions of the Personal Data Protection Board. In particular, in many decisions of the Personal Data Protection Board, we have observed that one of the most challenging issues for companies in practice is determining the correct personal data processing condition. The issues such as the data controller processing personal data without relying on any data processing conditions or processing personal data without obtaining explicit consent even when explicit consent should be obtained, are constantly repeated. In practice, I would like to point out that the questions I encounter both from the companies that I have had the opportunity to work with and from my colleagues who provide consultancy services on this issue often revolve around whether obtaining explicit consent is necessary or whether the data processing activity can be considered within the scope of legitimate interest. Therefore, a correct understanding of the conditions for personal data processing is the first step in determining the correct data processing condition. Accordingly, in this part of our study, we have attempted to proceed with examples as much as possible and to include the decisions of the Personal Data Protection Board.

In the second section of our thesis, we discussed the obligations of Turkish trading companies under Law No. 6698 on the Protection of Personal Data, which also constitutes the title of our thesis. In this section, we addressed the obligations related to the obligation to inform, VERBİS registration, obligations regarding data security, the obligation to respond to applications made by data subjects, the obligation to

comply with board decisions, and the obligation to destroy data. Finally, we evaluated these obligations in the light of Articles 1524, 64, 82, 55, 366, and 375 of the Turkish Commercial Code No. 6102.

One of the first obligations we addressed in this section is the obligation to prevent the unlawful processing of personal data.. The fundamental basis of the obligation to prevent the unlawful processing of personal data lies in the data controller's responsibility to correctly determine the data processing condition and conduct data processing activities based on that condition. In this respect, we have first explained the expectations of the legislator from Turkish commercial companies and the obligations that should be fulfilled, and then, we have addressed the cases in which this obligation is deemed to be violated based on the decisions of the Personal Data Protection Board. In addition, in this section, we have also comprehensively covered the obligation to prevent unauthorized access to personal data. In particular, this issue has been addressed by specifying the administrative and technical measures which may be adopted within the scope of the Law on the Protection of Personal Data, since the company is required to take certain administrative and technical measures. It should be noted that the Personal Data Protection Board imposes administrative fines on the grounds that this obligation is not fulfilled in any case if a personal data is accessed illegally. Therefore, we have attempted to determine what has been done incomplete in the cases subject to the decisions and to offer solutions. The Personal Data Protection Board often determines only the violation of the law, but does not provide a solution to the case. Generally, the points where the Board determines the violation of the law are the procedures and methods frequently employed by Turkish commercial companies. Consequently, in this section of our study, we have also included our recommendations for the fulfillment of the obligation.

Although the basis of our study focuses on the obligations, of course, it is an individual who is responsible for fulfilling this obligation in terms of Turkish commercial companies. In addition, the data controller is always the respondent of the administrative fine that may be imposed by the Personal Data Protection Board. Even if the violation is solely due to the fault of an employee, the company will be the respondent of the fine, and as a consequence, the issue of recourse is frequently encountered. In such circumstances, it is very clear that the company may seek recourse from the employee. Furthermore, the company may have not taken any action within the scope of compliance with the Law on the Protection of Personal Data even if there is no obvious data violation, a study may have been conducted but remained incomplete, or the most common scenario where compliance efforts have been made but remained on paper. We also attempted to address the issue of who would be responsible in this section of the study, without straying from the scope of the study. We endeavored to evaluate the issue in line with the dynamic structure of Turkish commercial companies and the requirements of business life. It should be noted that the possibility of non-compliance with the Law on the Protection of Personal Data is quite high within the scope of the law. It is relatively easy to determine when a violation results from an employee's fault, but it is relatively more challenging to determine who is responsible for negligence or deficiencies rather than a clear violation of the law. Therefore, at the end of this section, I also provided my own opinions to contribute, even if it's just a drop in the ocean compared to the knowledge of those dedicated to this field.

Throughout the study, we frequently referred to the guidelines published by the Personal Data Protection Board and the decisions of the Personal Data Protection Board. We have tried to do this in all sections. Because the law that constitutes the

subject of our study is a law with a history of only seven years. Considering the judicial decisions on the protection of personal data, it is understood that evaluations and determinations are often made in accordance with the general principles rather than the Law on the Protection of Personal Data No. 6698. Considering that the Law entered into force only seven years ago and the trial process takes a very long time in our country, the area we work in is not an area that has been the subject of many judicial decisions. On the other hand, the Personal Data Protection Authority considers all its decisions within the scope of the law and publishes many guides, announcements and videos to make the law understandable. As such, the source we used most in our study was the printed and digital resources of the Personal Data Protection Authority.

As a result, we have tried to deal with the obligations of Turkish commercial companies within the scope of the Personal Data Protection Law, which is very new for our country, with our practical solution proposal in the light of the theoretical explanations, then the opinions in the doctrine and finally the decisions of the Personal Data Protection Board.



ÖZET

Türkiye’de kişisel verilerin korunması alanındaki genel düzenleme niteliğini haiz olan ilk kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu’dur. Kanun 07.04.2016 tarihli Resmi Gazete’de yayımlanmıştır. Kanun ile öngörülen sistem uyarınca Kişisel Verileri Koruma Kurumu oluşturulmuş ve bazı görev ve yetkiler de bu kuruma tanınmıştır. Ülkemizde, kişisel verilerin korunması hukukunun yaygınlaşmasında Kişisel Verileri Koruma Kurumu’nun verdiği kararların etkisi büyüktür. Kişisel Verileri Koruma Kurulu kararları incelendiğinde, idari yaptırım uygulanan veri sorumlusu genellikle bir şirkettir. Özellikle de belirli bazı yabancı şirketler dışında yaptırıma maruz kalan kesimin çok büyük bir oranda Türk ticaret şirketleri olduğu dikkat çekmektedir. Bu nedenle, kişisel verilerin korunması hukuku kapsamında bir veri sorumlusunun yerine getirmesi gereken yükümlülükleri, Türk ticaret şirketleri özelinde ele almayı tercih ettik ve çalışmamızda kamu kurumlarını, gerçek kişileri, yabancı şirketleri ele alıp konuyu dağıtmak yerine Türk ticaret şirketlerine odaklandık. Bu yaklaşımın bir sonucu olarak tez çalışmamızın konusunu “6698 Sayılı Kişisel Verilerin Korunması Kanunu Uyarınca Türk Ticaret Şirketlerinin Yükümlülükleri” olarak belirledik. Çalışmamızda veri sorumlusu kavramını sıklıkla kullanmakla birlikte örneklerimizi mümkün mertebe bir şirket üzerinden verilmesine gayret gösterdik. Aynı şekilde ele aldığımız kararların büyük bir kısmında da örnek teşkil etmesi açısından yaptırım uygulanan veri sorumlusunun bir şirket olmasına gayret gösterdik.

Çalışmamızın giriş bölümünde kişisel verilerin korunması hukukunun tarihçesi, ulusal ve uluslararası kaynaklar konusunu ele ala aldık. Özellikle kişisel verilerin korunması alanında dünyada farklı yaklaşımlar benimsendiği için önce kişisel verilerin korunması hukukunun doğuşunu, akabinde ülkemizde ve diğer ülkelerdeki gelişimi ve en nihayetinde uluslararası hukuktaki gelişimi ele aldık.

Çalışmamızın birinci bölümünde kanuna ilişkin temel kavramlar, temel ilkeler ve kanunda yer alan kişisel veri işleme şartlarını ele aldık. Temel kavramları çok kapsamlı bir şekilde incelemeye gayret gösterdik. Zira Kişisel Verilerin Korunması Kanunu kapsamında idari para cezası yaptırımına maruz kalma riski taşıyan şirketler tarafından Kişisel Veriler Koruma Kurulu’na sunmuş olunan çoğu savunmanın temel kavramlar üzerine kurgulandığını tespit ettik. Örneğin yaptırıma maruz kalma ihtimali doğan şirket, veri sorumlusu olmadığını öne sürebilmekte ya da veri işleme faaliyetinin alenen cezayı gerektirdiği durumlarda cezadan kurtulma gayesi ile gerçekleştirilen eylemin kişisel veri işleme faaliyeti olmadığını zira ortada bir veri kayıt sistemi bulunmadığını ileri sürebilmektedir. Özellikle kimin veri sorumlusu olduğu kimin veri işleyen olduğu Kişisel Verileri Koruma Kurulu tarafından yayınlanan birçok kararda, rehberde ve duyuruda yer bulmuş bir konudur. Hatta bir adım daha geriye gidecek olursak bazı uyuşmazlıklarda ortada bir kişisel veri bulunup bulunmadığı dahi tartışabilmektedir. Dolayısıyla kişisel verilerin korunması hukuku alanında temel kavramların çok iyi idrak edilmesi gerekmektedir. Temel kavramların iyi anlaşılması aynı zamanda kanundaki yükümlülüklerin kim tarafından yerine getirileceği ve yükümlülüğün bulunup bulunmadığı sorularının da cevabını bizlere verecektir.

Örneğin bir eylemin kişisel veri işleme faaliyeti olarak tanımlanmaması durumunda kanunda belirtilen herhangi bir veri işleme şartına dayanmaya ihtiyaç bulunmayacaktır. Öte yandan eğer bir veri işleme faaliyeti söz konusuysa bunun bir veri işleme şartına dayanması gerekecektir. Öyleyse ilk değerlendirilmesi gereken husus, gerçekleştirilen eylemin kişisel verilerin işlenmesi olarak tanımlanıp tanımlanmayacağıdır. Ya da Kişisel Veriler Koruma Kurulu'nun, önüne gelen bir uyuşmazlıkta idari para cezası yaptırımını uygulamak istediği takdirde muhatabı, veri sorumlusudur. Bu nedenle Kişisel Verileri Koruma Kurulu'nun ilk tespit etmesi gereken veri sorumlusunun kim olduğudur. Bazı olaylarda veri sorumlusunun tespiti gerçekten de çok zor bir hal alabilmektedir. Dolayısıyla temel kavramlar, diğer kanunlardan farklı olarak Kişisel Verilerin Korunması Kanunu açısından çok büyük bir öneme sahiptir. Bu nedenle de mümkün olabilecek en detaylı şekilde ele alınmaya çalışılmıştır.

Birinci bölümde ele aldığımız bir diğer başlık ise genel ilkelerdir. Genel ilkeler, birçok Kişisel Verileri Koruma Kurulu kararına konu olmuş ve birçok şirketin idari yaptırıma maruz kalmasına sebebiyet teşkil etmiş önemli bir konudur. Konunun öneminin bir nedeni de veri sorumlusu tarafından kanunda belirtilen bir veri işleme şartına dayanılsa dahi eğer veri işleme faaliyeti genel ilkelere uygunluk teşkil etmiyorsa gerçekleştirilen veri işleme faaliyetinin kanuna aykırı olmasıdır. Ayrıca genel ilkeler, kişisel veri işleme faaliyeti kapsamında her süreçte göz önünde bulundurulması gereken ilkeler olduğundan aslında bir veri sorumlusu kendisine sürekli yaptığı işlemin genel ilkelere uygun olup olmadığını sormalıdır. Çalışmanın bu bölümünde genel ilkeler konusunu özellikle Kişisel Verileri Koruma Kurulu kararları ışığında ele almaya gayret gösterdik. Zira ilkeler konusu genel itibarıyla soyut bir konu olduğu için çalışmanın somutlaştırıcı olabilmesi adına birçok karara konu olay çalışmamızın bu bölümünde ele alınmıştır.

Birinci bölüm içerisinde son ele aldığımız konu ise kişisel verilerin işlenme şartlarıdır. Kanun koyucu, ikili bir ayrıma gitmek suretiyle genel nitelikteki kişisel verilerin işlenme şartları ile özel nitelikli kişisel verilerin işlenme şartlarını ayrı ayrı düzenlemiştir. Biz de çalışmamızın bu bölümünde kanun koyucunun yaptığı temel ayrımı esas alarak konuyu ele aldık. Ayrıca konuyu Kişisel Verileri Koruma Kurulu kararları ışığında örneklerle sunmaya gayret gösterdik. Özellikle Kişisel Verileri Koruma Kurulu'nun birçok kararında veri sorumlusunun hiçbir veri işleme şartına dayanmadan kişisel veri işlemesi ya da açık rıza alması gerektiği halde açık rıza almadan kişisel veri işlemesi gibi konular sürekli tekrar ettiğinden uygulamada da şirketleri en çok zorlayan konunun doğru kişisel veri işleme şartını tespit etmek olduğunu gözlemledik. Uygulamada, gerek birlikte çalışma fırsatı bulduğumuz şirketlerden gerekse bu konuda danışmanlık hizmeti sunan meslektaşlarımızdan aldığımız soruların özellikle açık rıza almak gerekip gerekmediği ya da veri işleme faaliyetinin meşru menfaat kapsamında ele alınıp alınamayacağı hususları olduğunu da belirtmek isteriz. Bu nedenle kişisel veri işleme şartlarının doğru anlaşılabilmesi, doğru veri işleme şartının tespitinin ilk basamağını oluşturmaktadır. Belirttiğimiz sebepler uyarınca çalışmamızın bu bölümünde mümkün mertebe örnekler üzerinden ilerlemeye ve Kişisel Verileri Koruma Kurulu kararlarına yer vermeye gayret gösterdik.

Çalışmamızın ikinci bölümünde, tezimizin de adını oluşturan Türk ticaret şirketlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki yükümlülüklerini ele aldık. İkinci bölümde aydınlatma yükümlülüğü, VERBİS kayıt yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından yapılan başvuruların cevaplanması yükümlülüğü, kurul kararlarının yerine getirilmesi

yükümlülüğü, imha yükümlülüğü konularını ele alıp en nihayetinde bu yükümlülükleri 6102 sayılı Türk Ticaret Kanunu m. 1524, m. 64, m. 82, m. 55, m. 366 ve 375 ışığında değerlendirdik.

Bu bölümde ele aldığımız ilk yükümlülüklerden birisi, kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğüdür. Kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünün temelinde veri sorumlusunun doğru veri işleme şartını tespit etmesi ve buna dayanarak veri işleme faaliyetini gerçekleştirmesi yer almaktadır. Biz de bu doğrultuda önce kanun koyucunun Türk ticaret şirketlerinden beklentisini, olması gerekeni açıkladıktan sonra Kişisel Verileri Koruma Kurulu kararları ışığında hangi hallerde bu yükümlülüğünün ihlal edildiğine dair kanaat getirildiği konularını ele aldık. Ayrıca bu bölümde kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğüne de kapsamlı bir şekilde yer verdik. Özellikle bu konuyu, şirket nezdinde belirli idari ve teknik tedbirleri almayı gerektirdiğinden Kişisel Verilerin Korunması Kanunu kapsamında alınabilecek idari ve teknik tedbirleri belirtmek suretiyle ele aldık. Hemen belirtmek gerekir ki bir kişisel veriye hukuka aykırı olarak erişim sağlandığı takdirde Kişisel Verileri Koruma Kurulu her halükarda bu yükümlülüğün yerine getirilmediğinden bahisle idari para cezası yaptırımını uyguladığı için kararlara konu olan olaylarda nelerin eksik yapıldığını tespit etmeye ve çözüm önerileri sunmaya gayret gösterdik. Zira Kişisel Verileri Koruma Kurulu, kararlarının büyük kısmında hukuka aykırılığı yalnızca tespit etmekle yetinmekte fakat olaya bir çözüm önerisi sunmamaktadır. Genellikle hukuka aykırılığı tespit ettiği noktalar da Türk ticaret şirketlerinin sıklıkla başvurduğu usul ve yöntemlerdir. Hal böyle olunca çalışmamızın bu bölümünde yükümlülüğün yerine getirilmesi için önerilerimize de yer verdik.

Çalışmamızın temelinde, yükümlülükler odaklanmakla birlikte elbette Türk ticaret şirketleri açısından bu yükümlülüğü yerine getirecek olan bir gerçek kişidir. Öte yandan, Kişisel Verileri Koruma Kurulu tarafından hükmedilebilecek idari para cezasının muhatabı her zaman veri sorumlusudur. İhlal, tamamen bir çalışanın kusurundan kaynaklansa dahi yaptırımın muhatabı şirket olacağı için bunun bir sonucu olarak rücu konusu sıklıkla karşımıza çıkmaktadır. Bu gibi durumlarda şirketin çalışanına rücu edebileceği çok açıktır. Öte yandan, şirket nezdinde bariz bir veri ihlali olmamakla birlikte Kişisel Verilerin Korunması Kanunu'na uyumluluk kapsamında hiçbir adım atılmamış olabilir, bir çalışma yapılmış fakat eksik kalmış olabilir ya da en sık karşılaşılan durum olan bir çalışma yapılmış fakat kağıt üzerinde kalmış olabilir. İşte bu gibi durumlarda sorumluluğun kimde olacağı konusunu da çalışmanın bu bölümünde ve çalışma kapsamı dışına çıkmadan genel hatlarıyla ele almaya çalıştık. Konuyu Türk ticaret şirketlerinin dinamik yapısına, ticaret hayatının gerekliliklerine uygun olarak değerlendirmeye gayret gösterdik. Belirtmek gerekir ki Kişisel Verilerin Korunması Kanunu kapsamında gerçekleştirilecek hukuka aykırılık ihtimali son derece fazladır. Hukuka aykırılığın bir çalışanın kusurundan kaynaklanması halinde bunu tespit etmek kolaydır. Fakat açıkça bir hukuka aykırılıktan ziyade ihmalden ya da eksiklikten kimin sorumlu olduğunu tespit etmek nispeten daha zordur. Bu nedenle bu alana gönül veren hukukçuların, onların bilgilerine oranla bilgimin okyanusta bir damla olduğu doktrine ufak da olsa bir katkı sağlamak amacıyla bu bölümün sonunda kendi kanaatlerimize de yer verdik.

Çalışmanın tamamında Kişisel Verileri Koruma Kurumu tarafından yayınlanan rehberlere, Kişisel Verileri Koruma Kurulu kararlarına sıklıkla atıfta bulunduk. Bunu bütün bölümlerde yapmaya gayret gösterdik. Zira çalışmamızın konusunu teşkil eden kanun, sadece yedi senelik geçmişi olan bir kanundur. Kişisel verilerin korunmasına yönelik yargı kararlarına bakıldığında, 6698 sayılı Kişisel Verilerin Korunması

Kanunu'ndan ziyade sıklıkla genel ilkeler uyarınca değerlendirme ve tespitlerde bulunulduğu anlaşılmaktadır. Kanunu'nun sadece yedi sene önce yayımlandığı, ülkemizde yargılama sürecinin de çok uzun sürdüğü göz önünde bulundurulduğunda çalışma yaptığımız alan çok fazla yargı kararına konu olmuş bir alan değildir. Öte yandan, Kişisel Verileri Koruma Kurumu bütün kararlarını kanun kapsamında ele almakta, kanunu anlaşılabilir kılmak için birçok rehber, duyuru ve video yayınlamaktadır. Hal böyle olunca çalışmamızda en çok istifade ettiğimiz kaynak Kişisel Verileri Koruma Kurumu'nun belirtilen basılı ve dijital kaynakları olmuştur.

Netice itibariyle ülkemiz için çok yeni olan Kişisel Verilerin Korunması Kanunu kapsamında Türk ticaret şirketlerinin yükümlülüklerini, önce teorik açıklamalar, akabinde doktrindeki görüşler ve en nihayetinde Kişisel Verileri Koruma Kurulu kararları ışığında uygulamaya yönelik çözüm önerimizle ele almaya gayret gösterdik.



GİRİŞ

I- Kişisel Verilerin Korunması Gereksinimi

İnsanoğlunun bilme ve öğrenme arzusu çok eskilere dayanmaktadır. Toplum nezdinde yaşanan gelişimler, iletişim kanallarının artması gibi faktörler bireyin birbirine daha fazla ihtiyaç duymasını beraberinde getirmiştir. Genel anlamıyla bilme ve öğrenme arzusunu taşıyan birey, aynı zamanda paylaşma eğilimi içindedir. Elbette öğrenilmek istenen veya paylaşılan unsurlar arasında kişisel veriler de yer almaktadır.

Zamanla toplumsal yapılar değişiklik göstermiş, ilkel toplumlar yerini modern yapılara bırakmıştır. Gelişimin bir ürünü olarak ortaya çıkan ilişkilerden birisi de birey-devlet ilişkisidir. Tarihsel akış içerisinde gerçekleşen birçok olay bireyin devlete bakış açısını, devletin de bireye davranışlarını şekillendirmiştir. Yakın tarihe gelindiğinde, 1939-1945 yılları arasında cereyan eden 2. Dünya Savaşı sürecinde, vatandaşlar tarafından devletin gözetleme ve baskı uygulayabilme konusunda ne kadar katı olabileceği tecrübe edilmiştir. İkinci dünya savaşı ile birçok insan, kendileri hakkında elde edilen birtakım kişisel verileri uyarınca ne dereceye kadar gözetlenebileceğini, baskı uygulanabileceğini, ayrımcılığa maruz kalabileceğini net bir şekilde görmüştür. Bu da kişisel verilerin korunmasının temelinde yatan endişe ve korkunun kaynağını göstermektedir.

Tarihsel akış içerisinde birçok olay gerçekleşirken teknoloji de değişimden nasibini almıştır. Özellikle ilk bilgisayarların üretilmesi adeta bir dönüm noktası olmuştur. Bilgisayarların hafızasının insan hafızasından daha kuvvetli olduğu, daha iyi kayıt tutabildiği, çok basit düzeyde de olsa veri tabanı tutabildiği anlaşılmıştır. Baskıcı, totaliter rejimlerin etkilerinden yeni yeni kurtulurken, hafızasının son derece kuvvetli olduğu bir aracın dünyaya tanıtılması insanlarda kişisel verilerinin kayıt altında tutulacağı, bilgilerinin her zaman erişime açık olacağı ve en nihayetinde devletlerin bu bilgileri aleyhlerine kullanacağı, bir baskı aracı haline getireceği düşüncesini oluşturmuştur. Daha basit bir anlatım ile kişisel verilerin işlenmesine ilişkin süreçler teknolojinin gelişmesiyle birlikte hız kazandığından, totaliter rejimlerin kişisel verileri çok daha rahat bir şekilde bireylerin üzerinde baskı unsuru olarak kullanacağı endişesi

artmıştır. Zira bilgisayarın olmadığı dönemde otomatik olmayan, eski metotlar ile yapılan işlemler artık bir araç vasıtası ile otomatik olarak yapılacaktır.

Gerek tarihsel gerek teknolojik gelişmeler neticesinde birey, kişisel verilerini mahrem alan içerisinde görmeye başlamıştır. Mahremiyet talebinin bir neticesi olarak da kişisel verilerin korunmasına yönelik bir yasal düzenlemeye ihtiyaç duyulmuştur.

Netice itibariyle, kişisel verilerin korunmasına yönelik bir kanuni düzenlemeye ihtiyaç duyulmasının temelinde kişisel veriye duyulan ihtiyacın artması, teknolojinin hızlı gelişimi, gelişmeler doğrultusunda kaygının artması¹ ve en nihayetinde mahremiyet talebi² yer almıştır.

Kişisel verilerin korunması, kişisel veriler ile yapılabilecek her türlü işlem açısından amaç, yöntem ve sınırların belirlenmesini ve sınırların ihlali halinde hangi hukuki yolların kullanılabileceğini ifade etmektedir.³

Günümüz itibariyle, kişisel verilerin korunması hukukuna yönelik hem uluslararası hem de ulusal birçok kaynak yer almaktadır. Bu kapsamda, bir sonraki başlıkta kişisel verilerin korunmasına yönelik uluslararası düzenlemeleri, takip eden başlıkta ise ulusal düzenlemeleri ele alacağız.

II-Uluslararası Düzenlemeler

Kişisel verilerin korunmasına yönelik ulusal düzenlemeler⁴, kişisel verilerin yurtdışına aktarımını kontrol altında tutmaya yönelik hükümler içermektedir. Bu eğilimin farkında olan bazı uluslararası kuruluşlar, kişisel verilerin yurtdışına aktarılması noktasında engeller olduğu takdirde uluslararası ticaretin zarar görme riski başta olmak üzere çeşitli çalışmalar yapmıştır.⁵ Yapılan çalışmaların temelinde belirli kriterleri sağlayan ülkelere veri aktarımının kolaylaştırılması ve uluslararası ticaretin

¹ Elif KÜZECİ, **Kişisel Verilerin Korunması**, İstanbul, On İki Levha Yayıncılık, 2021, s. 20

² Mesut Serdar ÇEKİN, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, İstanbul, On İki Levha Yayıncılık, 2020, s. 5, Paul B. LAMBERT, **Understanding the New European Data Protection Rules**, Florida: CRC Press, 2018, s. 25

³ Hüseyin Can AKSOY, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, 1. Bası, Ankara, Çakmak Yayınevi, 2010, s. 1

⁴ Ulusal düzenlemeler çalışmamızın 7-12. sayfaları arasında incelenmiştir

⁵ Murat DEVELİOĞLU, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayıncılık, İstanbul, 2017, s. 6

hız kaybetmemesi amaçlanmıştır. Bahsedilen düzenlemeleri sırasıyla OECD, Avrupa Konseyi, Birleşmiş Milletler ve Avrupa Birliği Düzenlemeleri şeklinde kategorize ederek ele alacağız.

Kişisel verilerin korunmasına yönelik ilk uluslararası adım OECD tarafından Özel Yaşamın Gizliliğinin ve Sınır Aşan Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri (“OECD Rehber İlkeleri”) ile atılmıştır.⁶ OECD Rehber İlkeleri, tavsiye niteliğinde olup sekiz temel ilkeyi ihtiva etmektedir. Bunlar veri toplamanın sınırlılığı ilkesi, veri kalitesi ilkesi, belirli amaç ilkesi, kullanımın sınırlılığı ilkesi, veri güvenliği ilkesi, açıklık ilkesi, bireyin katılımı ilkesi, hesap verilebilirlik ilkesi şeklindedir. Bu ilkeler, kişisel verilerin korunması alanındaki uluslararası birçok kaynağa temel teşkil etmiştir. Nitekim otuz altı yıl sonra yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda dahi benzer ilkeler ve izler görülmektedir.

Belirtmekte fayda var ki OECD Rehber İlkeleri 2013 yılında güncellenmiştir. Güncelleme ile hesap verilebilirlik, risk temelli yaklaşım, tasarımda mahremiyet gibi konuların ön planda çıktığı söylenebilir. Hesap verilebilirlik bağlamında kıyas yapıldığında eski metinde veri sorumlusunun sorumluluğuna odaklanılmışken güncel halinde veri sorumlusunun güncel otoritelere uyumluluğu ve ispat edilebilirlik üzerine odaklanıldığı görülmektedir.⁷ Özellikle, veri sorumlusu nezdinde kişisel verilerin korunmasına yönelik mahremiyetin yönetilmesi amacıyla bir program oluşturulmasının gerekliliği üzerinde durulmuş ve yapısal olarak programdan beklenenlerin çerçevesi çizilmiştir.

Kişisel verilerin korunmasına yönelik önemli bir diğer gelişme ise Avrupa Konseyi nezdinde gerçekleşmiştir. Uluslararası alanda kanaatimizce en etkili gelişme 108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi⁸ ile yaşanmıştır. Sözleşmenin amacı, kişisel verilerin otomatik yöntemler ile işlenmesine karşın özel hayatın gizliliğini güvence altına almaktır. 108 Sayılı Sözleşme, OECD ilkelerinden farklı olarak tavsiyede bulunmaktan ziyade

⁶ OECD, **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, 23 Eylül 1980.

⁷ Mehmet Bedii KAYA, **İstanbul Hukuk Mecmuası**, “Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verilebilirlik İlkesi”, 78 (4), 2020, (<https://doi.org/10.26650/mecmua.2020.78.4.0005>), (Erişim: 01.12.2023) s. 1866

⁸ Sözleşme 28 Ocak 1981 tarihinde Türkiye tarafından imzalanmış, 18 Şubat 2016 tarihli 29628 sayılı Resmi Gazete’de Onaya Uygun Bulma Kanunu yayımlanmış ve sözleşmenin Türkçesi 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete’de yayımlanmıştır. Sözleşme 1 Eylül 2016 tarihi itibarıyla ülkemizde yürürlüğe girmiştir.

yükümlülükler getiren bir sözleşmedir. Bunun en somut örneği sözleşmenin 4. maddesinde yer alan ve taraf devletlere yüklenen, sözleşmenin iç hukuka uyarlanması ve bu bağlamda gerekli düzenlemelerin yapılması yükümlülüğüdür.⁹ Türkiye bu sözleşmeyi imzaya açıldığı gün imzalamıştır.¹⁰

Sözleşme Türkiye açısından son derece önemlidir zira Türkiye Cumhuriyeti Anayasası'nın 90. maddesinin 5. fıkrası uyarınca usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası anlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümleri esas alınmaktadır. Bu nedenle, 108 Sayılı Sözleşme ülkemiz açısından normlar hiyerarşisinde önemli bir yere sahiptir.

Öte yandan, kişisel verilerin korunması alanının canlı bir alan olması, teknolojinin hızlı gelişimi ve alana özgü yeni problemlerin oluşması gibi hususlar 108 sayılı Sözleşme'yi bazı sorunları çözmede yetersiz hale getirmiştir.¹¹ Bu sebeple yeni çalışmalar yapılmış ve çalışmaların neticesinde Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Sözleşme¹² ("108+ sayılı Sözleşme") uluslararası hukuka kazandırılmıştır. Sözleşmede özellikle, kişisel verilerin adil ve şeffaf işlenmesi, şeffaflık ilkesi ve nasıl gerçekleştirileceği (8. madde), veri sorumlusuna getirilen ek yükümlülükler (10. madde) konuları ön plana çıkmıştır.

Avrupa Konseyi'nin yanı sıra Birleşmiş Milletler de kişisel verilerin korunması alanında çalışmalar yapmıştır. Uluslararası hukukta yaşanan birçok gelişmeyi, 14 Aralık 1990 tarihinde BM'nin Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin

⁹ Türkiye sözleşmeyi 28 Ocak 1981 tarihinde imzalamış ancak ülkemizde yürürlüğe girmesi 1 Eylül 2016'da gerçekleşmiştir. Bunun nedeni, 108 Sayılı Sözleşmede öngörülen, taraf devletlerin 108 Sayılı Sözleşmeyi onaylamadan önce iç hukukunda gerekli düzenlemeyi yapması yükümlülüğü ile alakalıdır. Nitekim Türkiye'de önce 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiş, ardından 108 Sayılı Sözleşme onaylanmıştır.

¹⁰ Sözleşmenin imzaya açıldığı gün olan 28 Ocak, Avrupa Konseyi tarafından Avrupa Veri Koruma Günü olarak ilan edilmiştir.

¹¹ KAYA, s. 1870

¹² Sözleşme, 10 Ekim 2018 tarihinde imzaya açılmış olup 46 ülke tarafından imzalanmıştır. (<https://www.coe.int/en/web/data-protection/convention108/modernised>) (Erişim Tarihi: 01.12.2023) ve (<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=223>) (Erişim Tarihi: 01.12.2023)

Rehber İlkeleri takip etmiştir.¹³ Belirtilen ilkelerin, yalnızca bilgisayar aracılığıyla işlem gören kişisel veriler açısından tatbik imkânı bulmaktadır.¹⁴

Kişisel verilerin korunması yönelik ele alacağımız son düzenlemeler ise Avrupa Birliği nezdinde gerçekleşen çalışmaların ürünleridir. 25 Ekim 1998 tarihinde ise 95/46EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi¹⁵ yayımlanmıştır. Türkiye de 6698 sayılı Kişisel Verilerin Korunması Kanunu’nu hazırlama sürecinde bu direktifi esas almıştır.

Direktif sadece Türkiye için değil aynı zamanda başta Avrupa ülkeleri olmak üzere birçok ülke için önem arz etmektedir. Direktifin hazırlanmasındaki temel maksat, bir bütün halinde pazar teşkil eden Avrupa Birliği’nin, sırf kişisel verilerin korunması yönünden ülkeler arasındaki farklılaşma nedeniyle bu statüsünün kaybedilmesinin önüne geçmektir. İkinci maksat ise bölge içerisinde kişisel veriler açısından serbest dolaşımın sağlanmasıdır.¹⁶

Daha sonrasında yerini GDPR (General Data Protection Regulation) olarak bilinen Avrupa Birliği Genel Veri Koruma Tüzüğü’ne¹⁷ bırakacak olan Direktif, veri kalitesine ilişkin prensipler, veri işlemenin hukuka uygun olmasını sağlayacak kriterler, özel nitelikli kişisel verilerin işlenmesi, ilgili kişinin verilerine erişim hakkı, ilgili kişinin itiraz hakkı gibi KVKK’dan alışık olduğumuz birçok konuyu düzenlemektedir. Belirtmekte fayda var ki amacı, Direktifin üye ülkeler arasında uyum ve aynı düzen içerisinde uygulanmasını sağlamak olan¹⁸ ve birçok konuda görüş ve tavsiyelerde bulunan Madde 29 Çalışma Gurubu da Direktif ile kurulmuştur.

¹³ Düzenlemenin orijinal ismi Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990 olup tam metin için: <https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac> (Erişim: 01.07.2023)

¹⁴ NİLGÜN BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yayınları, 2009, s. 24-25

¹⁵ Direktifin orijinal ismi “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data” olup tam metin için: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> (Erişim 27.07.2023)

¹⁶ Esra Tekil YILDIZ, **İnternet Üzerinde Kişisel Verilerin Korunması**, Prof. Dr. Fahiman Tekil’in Anısına Armağan, İstanbul, 2003, s. 795

¹⁷ Düzenlemenin orijinal ismi “Regulation of The European Parliament and of The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)” olup tam metin için: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1460910824051&uri=CONSIL:ST_5419_2016_INIT (Erişim: 01.07.2023)

¹⁸ DEVELİOĞLU, s. 11

Kişisel verilerin korunmasına yönelik en önemli ve güncel düzenlemelerden birisi olan GDPR 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. GDPR’a ihtiyaç duyulmasının nedeni, 95/46EC sayılı Direktif ile sağlanmak istenen amacın sağlanamamasıdır. Bu nedenle direktif ile GDPR arasında ciddi farklılıklar bulunmaktadır.

Bunlardan birincisi, GDPR bir direktif değil tüzüktür. Türk hukuk sisteminden farklı olarak AB Hukuku uyarınca tüzükler, tüm üye devletleri bağlayan ve doğrudan uygulanabilirliği bulunan hukuk kaynaklarıdır.¹⁹ Direktiflerde ise ulaşılması istenen bir sonuç belirtilmekte ancak bu sonuca nasıl ulaşılacağı konusunda yöntem tercihi ulusal otoritelere bırakılmaktadır. İşte tam da bu noktada Direktif ile istenen amaç sağlanamamıştır. Zira AB ülkeleri temelde aynı prensipte uzlaşabilmiş fakat uygulamada ayrılmıştır. Bu nedenle, yerleşik bir düzenin tesisi için²⁰ yeni düzenlemede bir tüzük tercih edilmiştir.

İlaveten direktif ile tüzük, muhatabının uyum sağlaması için göstermesi gereken efor anlamında da farklılık arz etmektedir. Örneğin direktife göre AB ülkelerinde faaliyet gösteren bir şirket hem direktife uyumlu olmalı hem de faaliyette bulunduğu her ülkede ayrı ayrı ulusal düzenlemelere uyum sağlamalıdır. Oysa aynı örnekteki şirket GDPR sayesinde sadece tüzüğe uyumlu olmaya çalışacaktır. Bu nedenle, bölgede faaliyet gösteren ticaret şirketleri açısından da temel bir çatı düzenleme ihtiyacı GDPR ile karşılanmıştır.

Netice itibarıyla, GDPR hem direktifle hedeflenin yerine getirilmesi hem de hem de kişisel verilerin korunması hukukuna yönelik en güncel kaynaklardan birisi olması sebebiyle son derece önemlidir.

III-Ulusal Düzenlemeler

Kişisel verilerin korunmasına yönelik ulusal düzenlemeler kronolojik akışa göre incelendiğinde, her dönemde getirilen düzenlemelerin arka planında farklı bir endişenin olduğu görülmektedir.

Kişisel verilerin korunmasına yönelik ilk düzenlemeler, 1970’li yıllarda yer bulmuştur. 1939-1945 yılları arasında cereyan eden 2. Dünya Savaşı sürecinde,

¹⁹ Sanem BAYKAL/ İlke, GÖÇMEN, “Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi”, Prof. Dr. Erdal Onar’a Armağan, Ankara, 2013, s. 325

²⁰ Nilgün BAŞALP, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, 2015, s. 82

vatandaşlar tarafından devletin gözetleme ve baskı uygulayabilme konusunda ne kadar katı olduğu tecrübe edilmiştir. Kişisel verilerin korunmasına yönelik ilk düzenlemeler ise savaştan 20-30 yıl sonra yer bulmuştur. Dolayısıyla ilk düzenlemelerin temelinde kişisel verilerin devletler tarafından kötüye kullanılabilme ihtimali, kişisel verilerin gözetleme aracı olarak kullanılabilmesi ve birey üzerinde baskının arttırılabilmesi korkusu ve endişesi yer almaktadır.²¹ Yine, her ne kadar ülkemize gelişi daha sonra olsa da bu dönemde ilk bilgisayarların üretilmesi, zaman içerisinde geliştirilmesi de korkunun bir diğer kaynağıdır. Zira bu dönemde bilgisayarların hafızasının insan hafızasından daha kuvvetli olduğu, daha iyi kayıt tutabildiği, çok basit düzeyde de olsa veri tabanı tutabildiği anlaşılmıştır. Baskıcı, totaliter rejimlerin etkilerinden yeni yeni kurtulurken, hafızasının son derece kuvvetli olduğu bir aracın dünyaya tanıtılması insanlarda kişisel verilerinin kayıt altında tutulacağı, bilgilerinin her zaman erişime açık olacağı ve en nihayetinde devletlerin bu bilgileri aleyhlerine kullanacağı, bir baskı aracı haline getireceği düşüncesini oluşturmuştur. Daha basit bir anlatım ile kişisel verilerin işlenmesine ilişkin süreçler teknolojinin gelişmesiyle birlikte hız kazandığından²², totaliter rejimlerin kişisel verileri çok daha rahat bir şekilde bireylerin üzerinde baskı unsuru olarak kullanacağı endişesi artmıştır. Zira bilgisayarın olmadığı dönemde otomatik olmayan, eski metotlar ile yapılan işlemler artık bir araç vasıtası ile otomatik olarak yapılacaktır.

Açıklanan gerekçelerle kişisel verilerin korunmasına yönelik ilk düzenlemelerin temelinde, genellikle kişisel verilerin kötüye kullanılması konusunda duyulan endişe, kişisel verilerin kişinin aleyhine sonuçlar doğuracak şekilde işlenmesi ve hatta bazı durumlarda Devletlerin dahi bu eylemi gerçekleştirebileceği endişesi yer almaktadır. Bu nedenle, ilk yasal düzenlemelerin temelinde bu endişeyi giderme amacıyla bir kontrol mekanizması oluşturulması ve denetlenebilirlik yer almaktadır.²³

Kişisel verilerin korunmasına ilişkin ilk ulusal düzenleme Almanya'nın Hessen eyaletinde doğan Hessen Veri Koruma Kanunu'dur. Kanunun temeline bakıldığında bilişim sistemleri aracı kılınmak suretiyle tapu kayıtlarına erişim sağlanmasında ve bu

²¹ Elif KÜZECİ: "Kişisel Verilerin Korunması Hakkı", iç. Kişisel Verilerin Korunmasına Akademik Bakış- **KVKK Akademi Derleme Çalışması** (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ankara, Ütopya Grafik, 2023, s. 29 vd.

²² Arthur R. MILLER, **The Assault on Privacy, Computers, Data Banks, and Dossiers**, ABD: The University of Michigan Press, 1971, s. 216 vd.

²³ KÜZECİ, a.g.e. s. 30

verilerin işlenmesinde uyulacak usul ve esasları belirlediği görülmektedir. Bu hukuki gelişmeleri 1973 tarihli İsveç Veri Yasası takip etmiştir. Ulusal bağlamda uygulanabilirlik açısından kişisel verilerin korunmasına yönelik ilk düzenleme, 1973 tarihli İsveç Veri Yasasıdır. Bu kanunun temelinde de vatandaşların kimlik numarası ile sağlanan bir entegrasyon neticesinde kişisel verilerinin işlenmesine yönelik risk ve tehditler yer almaktadır.²⁴ Nitekim İsveç'te bu tartışmaların öncesinde, bireye bir kimlik numarası tanımlanmasına, bu numara ile kişinin bazı bilgilerinin entegrasyonunun sağlanmasına şüphe ile yaklaşılmıştır. Bilgisayarların da bu dönemde daha popüler hale gelmesi ile bu endişeler alevlenmiş ve neticesinde de tam da bu konuya yönelik bir çerçeve çizme ihtiyacı hasıl olmuştur.

1973 tarihli İsveç Veri Yasası'nın bir diğer önemli özelliği ise, bir veri koruma otoritesinin (veri denetleme kurulu) kurulmasını düzenlemesidir. Buna göre, veri denetleme kurulu, makineler aracılığıyla veri tabanları oluşturulması konusunda izin ve onay makamı olarak belirlenmiş, aksi durumdaki uygulamalar da yasaklanmıştır. Pek tabi bu düzenlemeyi getirirken kanun koyucunun beklentisi, yasak dolayısıyla benzeri veri tabanları tutanların bu uygulamadan vazgeçeceği ve veri tabanlarının sınırlı bir bağlamda ve sadece kurulun onay vereceği gerçek ve tüzel kişilerce kullanılacağıdır. Oysa durum beklenenden farklı olmuş ve kanunda belirtilen şekilde veri tabanı kullanan ve bu bağlamda veri işleme faaliyeti yürüten kişilerin hepsi kurula onay almak için başvuruda bulunmuştur. Hatta bahsedilen onay süreci kurulun iş yükünü de ciddi anlamda arttırmıştır. Yeri gelmişken belirtmekte fayda var ki bu düzenlemenin bir benzeri de 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer almaktadır. Kapsamı tamamen farklı olsa da ilgili otoriteden izin alma süreci 6698 sayılı Kanunda da öngörülmüş bir süreçtir. İleride açıklanacak olmakla birlikte²⁵ kişisel verilerin yurt dışına aktarılmasını düzenleyen 9. maddede ilgili kişiden açık rıza almaksızın kişisel verilerin yurt dışına aktarılabilmesi için öngörülen bir yöntem de Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun izninin bulunmasıdır. Hemen belirtmek gerekir ki bahsedilen izin, çok detaylı ve kapsamlı bir çalışmanın ürünü olan taahhütnamelere verildiğinden İsveç Veri Denetleme Kurulu'nda olduğu gibi inanılmaz derecede bir iş yükü doğurmamıştır. Netice itibarıyla, bir örneği de

²⁴ Kişisel Verileri Koruma Kurumu, “**Kişisel Verilerin Korunması Kanunu ve Uygulaması**”, s.8 <https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf> (Erişim Tarihi: 02.07.2023)

²⁵ Bkz; s. 120 vd.

bizim kanunumuzda yer alan veri koruma otoritesinin kuruluşu ve hatta bazı durumlarda izin verme yetkisi bulunması ilk defa İsveç Veri Yasasında yer bulmuş ve birçok ülkenin veri koruma kanununa da bu bağlamda ilham kaynağı olmuştur.

İsveç Veri Yasası kısa süre içerisinde Avrupa’da yayılmış, birçok Avrupa ülkesi hızlı bir şekilde kendi veri koruma kanununu yayınlamıştır. Nitekim 1978 tarihli Fransa Veri Koruma Kanunu da bu şekildedir. Burada dikkat edilmesi gereken nokta, bahsedilen ilk yasaların odağında günümüzdeki kadar gelişmiş olmasa da veri tabanlarına yönelik usul ve esasların belirlenmesi hususu yer almaktadır. Tahmin edileceği üzere, kişisel verilerin korunmasını sadece veri tabanları ile sınırlı tutmak istenileni sağlamayacağından bunun yeterli olmadığı anlaşılmış ve zamanla birçok ulusal düzenlemede kapsam daha da genişletilmiştir.²⁶

Tarihsel gelişim ve ulusal kaynaklardan bahsederken Portekiz’in de üzerinde durmak gerekir. Zira Portekiz, kişisel verilerin korunmasına yönelik bir maddeye anayasasında yer veren ilk ülkedir. 1976 tarihli Portekiz Anayasası’nda yer alan madde, diğer düzenlemeler gibi veri tabanlarına ilişkin olmakla birlikte bahsedilen madde ile bilgi edinme hakkı tanınmış ve özel hayatın gizliliği vurgusu yapılmıştır. Portekiz’de yaşanan bu gelişmeyi bir yıl sonra İspanya ve ardından Avusturya takip etmiştir.

Genel hatlarıyla kişisel verilerin korunması hukukunun doğumu, gelişmesi ve bu alandaki ulusal düzenlemeler açıkladığımız şekilde olmakla birlikte farklı ülkelerde kişisel verilerin korunmasına yönelik yasalaştırma süreçlerinde farklı yaklaşımların benimsendiği görülmektedir. Örneğin, bazı ülkelerde kişisel verilerin korunması sadece yasalarla sağlanmaktayken bazı ülkelerde ise hem anayasa düzeyinde hem de farklı yasalar ile sağlanmakta; bazı ülkelerde ise toplu bir şekilde genel bir çatı kanun bulunmaktadır.

Bu yaklaşımlardan birincisi “*omnibus approach*” olarak tanımlanmaktadır. Bu yaklaşımın en somut ürünü GDPR’dır.²⁷ GDPR, en temel anlatımla çok geniş bir alanda uygulanma imkânı olan, kişisel verilerin korunmasına yönelik çatı bir yasadır. İlaveten, GDPR hem kamu hem de özel hukuk kişilerinin veri işleme faaliyetlerini

²⁶ KÜZECİ, a.g.e. s.32

²⁷ Orla LYNSKEY, **The Foundations of EU Data Protection Law**, Oxford University Press, 2015, s. 15

geniş bir perspektifte ele alan, sektör ayırt etmeyen bir kanundur. GDPR temelinde “*ombinus approach*” yaklaşımı bulunmaktadır. Burada kanun koyucu, sektörel bazdaki ihtiyaçları göz ardı etmek yerine genel bir çerçeve çizmekte, her ilgilinin kendi operasyonları doğrultusunda risk tabanlı bir yaklaşım ile kanuna uyumlu olmasını beklemektedir. Bu elbette konuyla ilgili hiçbir içtihat olmadığı, herkesin kanunu kendisine göre uygulayacağı anlamına gelmemektedir. İlgili veri koruma otoriteleri tarafından yayınlanan rehberler, kılavuzlar, mahkeme kararları, yerleşik uygulamalar uyum sürecinde ve otokontrol aşamasında referans alınacak kaynaklardır.²⁸

İkinci yaklaşım, sektörel bazda özel hayatın gizliliğine yönelik kanunlar çıkartılmasıdır. Bu yaklaşımı daha çok Anglo-Sakson ülkeleri benimsemiş olup yaklaşımın en somut örnekleri Amerika, Yeni Zelanda gibi ülkelerde görülmektedir. Örneğin ABD’de çocuklara yönelik mahremiyet yasası, sağlık sektörüne yönelik yasalar bulunmaktadır. Ancak tüm bunları genel anlamda düzenleyen kapsayıcı tek bir kanun bulunmamaktadır.²⁹ Dolayısıyla ABD sınırları içerisinde kişisel verilerin korunmasına yönelik yasalara uyumlu olmak isteyen bir şirket, hem federal yasalara hem eyalet yasalarına hem de sektörel olarak bir düzenleme mevcut ise bu düzenlemeye uyumlu olmak zorundadır. Burada kanun koyucunun yaklaşımı, her sektörün ihtiyacı farklılık arz edeceğinden çatı bir kanunun uygulanmasından ziyade sektörün ihtiyaçlarına uygun düşecek şekilde yasalaştırmaya gitmektir.

Üçüncü yaklaşım ise “*habeas data*” olarak adlandırılmaktadır. Habeas data aslında bir haktır. Bu hak uyarınca ilgili kişi, kendisine ait kişisel verilere erişebilme, düzeltme gibi birçok hakka sahiptir. Uygulanma yöntemi farklı olmakla birlikte KVKK m.11’de tanımlanmış olan ilgili kişinin hakları ile habeas data benzerlik göstermektedir. Bu yaklaşım daha çok Latin Amerika ülkelerinde benimsenmiştir. Örneğin Arjantin ve Peru, habeas data yaklaşımına sahip yasal düzenlemelere sahiptir. Habeas Data hakkı ilk defa Brezilya Anayasası’nda yer bulmuştur. Verilen bu hak uyarınca kişi, mahkemeye bir şikayet dilekçesi sunmak suretiyle herhangi bir veri kayıt sisteminde ne tür bilgilerin tutulduğunu öğrenme, verilerinin silinmesini ya da

²⁸ Christopher F. MONDSCHNEIN/ Casimo MONDA, “The EU’s General Data Protection Regulation (GDPR) in a Research Context”, **Fundamentals of Clinical Data Science** (Ed: Pieter Kubben · Michel Dumontier Andre Dekker), s. 57

²⁹ Paul M. SCHWARTZ/ Karl-Nikolaus PEIFER, “Transatlantic Data Privacy”, Kasım 2017, 106 **Georgetown Law Journal**, 2017;115. UC Berkeley Public Law Research Paper, s. 128

değiştirilmesini talep etme gibi haklara sahiptir.³⁰ Belirtilen hakkın anayasal düzlemde bir hak olarak kabul edildiği dönemin birkaç sene öncesinde, çoğu Latin Amerika ülkesinde baskıcı ve kuvvetli bir askeri güç bulunmaktaydı. Emniyet birimlerinin son derece yetkili olduğu da göz önünde bulundurulduğunda, bu dönemlerde asker tarafından veya kolluk kuvvetleri tarafından gözaltına alınan yada tutuklanan kişilerden bir daha haber alınamaması gibi durumlar ile karşılaşılırmaktaydı. Habeas data hakkının ortaya çıkmasının temelinde de tutukluken veya gözaltında iken kaybolan kişilerin ailesinin bu kişilere erişebilmesini sağlama arzusu yer almaktadır.³¹ Nitekim bu yola başvurulduğunda, kaybolan kişi hakkındaki en son kayıtlara ulaşılabilmekte ve fikir yürütülebilmektedir.

Görüldüğü üzere kişisel verilerin korunmasına yönelik üç farklı yaklaşım mevcut iken bazı ülkelerde ise karma yaklaşımlar söz konusudur. Karma yaklaşıma sahip olan ülkelerden birisi de Türkiye’dir. Nitekim kişisel verilerin korunması hakkı Türkiye’de hem anayasal düzeyde korunan bir haktır hem de 6698 sayılı KVKK uyarınca hususi bir düzenlemeye de sahiptir. Bununla birlikte sektör bazlı bir yasa mevcut değildir. Ayrıca habeas data yaklaşımının benzeri nitelikte bir anlayış KVKK m.11’de benimsenmiştir. Her ne kadar başvuru usul ve yöntemi farklı olsa da prensipte benzer hakları koruma altına almaktadır. Dolayısıyla Türkiye’deki yaklaşımın karma bir yaklaşım olduğu söylenebilir.

IV-Türk Hukukundaki Düzenlemeler

Türk hukuk sisteminde kişisel verilerin korunması, anayasal düzeyde tanınmış bir haktır. Kronolojik olarak ele alacak olursak ilk adım 12 Ekim 2004 tarihinde Resmi Gazete’de yayımlanan 5237 sayılı Türk Ceza Kanunu (TCK)³² ile başlamaktadır. Kişisel verilerin kaydedilmesi suçu TCK m. 135’te, verileri hukuka aykırı olarak verme veya ele geçirme suçu TCK m. 136’da, verileri yok etmeme suçu TCK m. 137’de düzenlenmiştir. Böylece, kişisel verilerin korunmasına yönelik Türk hukukundaki ilk yasal düzenleme TCK ile gerçekleştirilmiştir.

³⁰ Mutlu BİNARK, “Habeas Data Kavramı ve Kavramın Kişisel Verilerin Korunması Tartışmalarına Katkısı”, **Kültür ve İletişim Dergisi**, Eylül 2015- Şubat 2016, C. 18, S. 36, s. 196-207

³¹ Ünal YILDIZ., (2022). Habeas Data Kavramı ve Arjantin Örneği, **Kişisel Verileri Koruma Dergisi**, 4(1), s. 4

³² RG., 25611 S., 12.10.2004 T.

Bu gelişmeyi 2007 yılında, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun takip etmiştir.³³ Özellikle içerik sağlayıcılarının yükümlülüklerinin düzenlendiği 4. madde ve yer sağlayıcılarının yükümlülüklerinin düzenlendiği 5. madde, kişisel verilerin işlenmesi açısından önem arz eden düzenlenmelerdir. Zira bu maddelerde, internet ortamındaki trafik bilgilerinin işlenme süreleri, bütünlüğü ve gizliliğine yönelik düzenlemeler yer almaktadır.

2008 yılında ise, 5809 sayılı Elektronik Haberleşme Kanunu³⁴ ile kişisel verilerin korunmasına yönelik önemli gelişmeler yaşanmıştır. Özellikle, Bilgi Teknolojileri ve İletişim Kurumu'nun görev ve yetkilerinin yer aldığı “*Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.*” şeklindeki m. 6/ f. 1/ c bendi, m. 12/ f. 2/ d bendi, m. 43 ve m. 51 hükümleri, kişisel verilerin korunması açısından ön plana çıkan hükümler arasındadır.

12 Eylül 2010 tarihinde ise “*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*” şeklindeki madde, Türkiye Cumhuriyeti Anayasası'na³⁵ eklenmiştir. Bu düzenlemeyle birlikte kişisel verilerin korunması hakkı, Türkiye’de anayasal düzeyde korunan bir hak konuma erişmiştir. Anayasaya yapılan bu eklemeyen çok kısa bir süre sonra ise Türk Borçlar Kanunu’nun³⁶ 419. maddesinde “*İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.*” hükmüne yer verilmiştir.

Bir diğer önemli gelişme ise 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile yaşanmıştır.³⁷ Özellikle, ticari elektronik ileti gönderme

³³ RG., 26530 S., 23.05.2007 T.

³⁴ RG., 27050 S., 10.11.2008 T.

³⁵ RG., 17863 (Mükerrer) S., 09.11.1982 T.

³⁶ RG., 27836 S., 04.02.2011 T.

³⁷ RG., 29166 S., 05.11.2014 T.

şartlarının düzenlendiği 6. madde ve devamı hükümleri, kişisel verilerin işlenmesine yönelik önemli düzenlemelerdendir.

17 Mart 2016 tarihinde, 108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Türk hukukuna dahil edilmiştir.

7 Nisan 2016 tarihine gelindiğinde ise çalışmamızın da temelini teşkil eden 6698 sayılı Kişisel Verilerin Korunması Kanunu, 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Kanunun yürürlüğe girmesinin sadece bir ay sonrasında ise 181 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol Türk hukukuna dahil edilmiştir.

KVKK’nin yürürlüğe girmesini takiben 28 Ekim 2017 tarihinde ve 30224 sayılı Resmi Gazete’de Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik³⁸; 30 Aralık 2017 tarihinde ise 30286 sayılı Resmi Gazete’de Veri Sorumluları Sicili Hakkında Yönetmelik³⁹ yayımlanmıştır.

Son olarak Kanun kapsamında yayımlanmış iki adet tebliğ bulunmaktadır. Bunlar 10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete’de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ⁴⁰ ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ⁴¹’dir.

Yukarıda izah olunan yasal düzenlemelerin yanı sıra, Kişisel Verileri Koruma Kurumu tarafından yayınlanan birçok ilke karar, rehber, kılavuz ve yine yargı kararları bu alana ışık tutmaktadır.

V-Çalışmanın Amacı, Kapsamı ve İnceleme Planı

Zaman içerisinde toplumsal yapılar değişiklik göstermiş, bireyler birbirine daha fazla ihtiyaç duymaya başlamıştır. Bireylerin birbiriyle bilgi paylaşımı eğiliminde olması, devletlerin düzen tesis etme gayesiyle bilgiye düzenli olarak ihtiyaç

³⁸ RG., 30224 S., 28.10.2017 T.

³⁹ RG., 30286 S., 30.12.2017 T.

⁴⁰ RG., 30356 S., 10.03.2018 T.

⁴¹ RG., 30356 S., 10.03.2018 T.

duyması ve en nihayetinde teknolojinin de gelişmesiyle birlikte kişisel verilerin akışı hızlanmış, bununla birlikte bireyin kişisel verileri üzerindeki denetim mekanizması azalmaya başlamıştır.

Netice itibariyle teknolojik gelişmeler sadece bilgiye erişimi kolaylaştırmamış, bununla birlikte bireyin mahremiyet alanının ihlal edilmesini ve kişisel verilere erişilmesini daha kolay hale getirmiştir.

Dijital ortamda kişisel verilerin serbest dolaşım halinde olmasına karşın kişisel veriler üzerinde bireyin denetim imkanının sınırlı olması, bireyin mahremiyetine yönelik risklerin artış göstermesi yasal bir düzenlemeye duyulan ihtiyacı arttırmıştır.

Duyulan bu ihtiyaç neticesinde, başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve buna ilişkin uyulacak usul ve esasları düzenlemek amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu 07.04.2016 tarihinde yürürlüğe girmiştir.

Kanun kapsamında yer alan yükümlülükler temel itibariyle hem gerçek kişilere hem de tüzel kişilere yöneliktir. Dolayısıyla konunun öznesi bir gerçek kişi olabileceği gibi bir kamu kurumu veya bir anonim şirket de olabilir. Kişisel Verileri Koruma Kurumu tarafından yayımlanan kararlara bakıldığında ise ağırlıklı olarak uyumsuzluk konusu olaylarda bir Türk ticaret şirketinin olduğu görülmektedir. Bu nedenle çalışmamızın öznesi olarak Türk ticaret şirketleri seçilmiş, çalışma kapsamı da bu doğrultuda sınırlandırılmıştır.

Türk ticaret şirketleri, KVKK kapsamında belirli yükümlülükleri yerine getirmekle mükellef olduğu gibi 6102 sayılı Türk Ticaret Kanunu'nda öngörülen yükümlülükleri de yerine getirmekle yükümlüdür. Kişisel verilerin korunması kapsamında, TTK'de yer alan bazı düzenlemelerin KVKK kapsamındaki yükümlülüklerin yerine getirilmesi, sorumluluğun tespiti noktasında ayrı bir önem arz ettiği tespit edilmiştir. Bununla birlikte, literatürde KVKK kapsamındaki yükümlülüklerin TTK'de yer alan belirli hükümler uyarınca ele alındığı çalışma sayısı parmakla gösterilecek kadar azdır. Bu nedenle, hem konuyla ilgili çalışmaların sınırlı olması hem de bu konuda doktrine ve uygulayıcılara katkı sağlaması gayesiyle çalışmamız ele alınmıştır.

Bu çalışmanın temel amacı, Türk ticaret şirketlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında yükümlülüklerinin incelenmesidir.

Çalışmada, Türk ticaret şirketlerinin KVKK'ye uyumluluğunun sağlanabilmesi için yerine getirilmesi gereken temel yükümlülüklerin neler olduğu konusuna odaklanılmıştır. İlaveten, yerine getirilmesi gereken yükümlülüklerle ilişkin Türk Ticaret Kanunu'nda yer alan bazı düzenlemeler uyarınca oluşan özel durumlara yer verilmiştir. Çalışmanın kapsamı göz önüne alındığında özne olarak yalnızca Türk ticaret şirketlerine odaklanılmıştır. Çalışmanın boyutu itibariyle teknik tedbirler konusuna çok kısa bir şekilde yer verilmiş olup detaylı inceleme konusu yapılmamıştır. Ayrıca, çalışmanın kapsamını çok genişleteceğinden TTK'de yer alan bütün düzenlemelerden ziyade uygulamada sık karşılaşılan, öne çıkan ve özellik arz eden bazı maddelerin KVKK bağlamında incelemesi yapılmıştır. KVKK ile TTK kapsamında inceleme konusu yapılan alanlar, aydınlatma yükümlülüğünün TTK m. 1524 bağlamında değerlendirilmesi, kişisel verilerin işlenmesi ve imhası süreçlerinin TTK m. 64 ve TTK m. 82 bağlamında değerlendirilmesi, veri ihlal bildirim yükümlülüğünün TTK m. 82/ f. 7 bağlamında değerlendirilmesi, KVKK kapsamındaki yükümlülüklerin yerine getirilmemesinin TTK m. 55/f. 1, e bendi uyarınca haksız rekabet bağlamında incelenmesi ve son olarak KVKK kapsamındaki sorumluluğun tespitinde TTK m. 366/ f. 2 ve TTK m. 375 hükümlerinin etkisi şeklindedir. Netice itibariyle çalışmada, kişisel verilerin korunması hukuku kapsamında temel olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'na odaklanılmış, Türk Ticaret Kanunu'nun belirli hükümlerine yer verilmiş, Kişisel Verileri Koruma Kurumu kararları detaylıca irdelenmiş, doktrindeki görüşlere yer verilmiş, uygulamada sıklıkla karşılaşılan problemlere çözüm önerilerimiz sunulmuştur.

Çalışmada, kişisel verilerin işlenmesindeki temel ilkeler, kişisel verilerin işlenme şartları, aydınlatma yükümlülüğü, VERBİS kayıt yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından yapılan başvuruların cevaplanması yükümlülüğü, kurul kararlarının yerine getirilmesi yükümlülüğü, kişisel verilerin imha edilmesi yükümlülüğü konuları detaylıca ele alınacaktır. Nihai olarak, Türk ticaret şirketlerinin KVKK kapsamındaki yükümlülükleri, Türk Ticaret Kanunu'nda yer alan bazı düzenlemeler ışığında ele alınacaktır.

Çalışma iki bölümden oluşacak şekilde yapılandırılmıştır. Çalışmanın birinci bölümünde KVKK'ye ilişkin temel kavramlar, temel ilkeler ve KVKK'de yer alan kişisel verilerin işlenme şartları incelenecektir. Çalışmamızın bu bölümünde Kişisel Verileri Koruma Kurulu'nun temel ilkeleri ve veri işleme şartlarını nasıl ele aldığı,

doktrindeki görüşlerin neler olduğu, uygulamada karşılaşılan problemler ve çözüm önerileri üzerinde durulacaktır.

Çalışmanın ikinci bölümünde ise tezin temelini teşkil eden Türk ticaret şirketlerinin 6698 sayılı kişisel verilerin korunması kanunu kapsamındaki yükümlülükleri incelenecektir. Çalışmamızın bu bölümünde Türk ticaret şirketlerinin yükümlülükleri öncelikle genel itibariyle KVKK bağlamında ele alınacak, akabinde TTK’de yer alan bazı düzenlemeler uyarınca özellik arz eden çeşitli durumlar değerlendirilecektir. Belirtilen konular, Kişisel Verileri Koruma Kurulu kararları, doktrinde yer alan görüşler ve uygulamada karşılaşılan problem ışığında hem teorik hem de pratik olarak incelenecektir.



BİRİNCİ BÖLÜM

KANUNA İLİŞKİN TEMEL KAVRAMLAR, TEMEL İLKELER VE KANUNDA YER ALAN KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

I-TEMEL KAVRAMLAR

A-Kişisel Veri

Kişisel veri kavramı KVKK m. 3/ f. 1, d bendinde “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır. Tanımdan anlaşılacağı üzere kişisel veri kavramı üç temel unsurdan oluşmaktadır.⁴² Bunlar “bir verinin varlığı”, “verinin gerçek kişiye ilişkin olması”, “verinin kişiyi belirli kılması veya kişiyi belirlenebilir kılması” şeklindedir.

Kişisel veri dendiğinde akla ilk olarak bir gerçek kişinin adı soyadı, telefon numarası, evinin adresi gibi doğrudan bizi gerçek bir kişiye ulaştıran veriler gelmektedir. Bununla birlikte, verinin herhangi bir kayıt ile entegrasyonu sonucu kişiyi belirlenebilir kılması veya kişinin ekonomik, sosyal durumu gibi kimliğini ifade eden veriler de bu kapsam içerisinde yer almaktadır.⁴³ Kişisel veri kavramı hem çalışmamızın temelini teşkil ettiğinden hem de tespiti her zaman kolay olmadığından bu bölümde kavram, üç temel unsuru yönünden detaylıca izah edilecektir.

1-Kişisel Verinin Unsurları

a-Bir Verinin Varlığı

Kişisel veri kavramından bahsedebilmek için öncelikle elimizde bir veri bulunması gerekmektedir. Veri kavramı, her türlü bilgi şeklinde tanımlanmaktadır. Ancak genellikle veri kavramı ve bilgi kavramı birbirlerinin yerine kullanılmaktadır.

⁴² Madde 29 Veri Koruma Çalışma Grubu’nun 04.06.2007 tarihli ve 4/2007 sayılı görüşünde kriter sayısı dörttür. İlgili dokümanda “ilişkin olma” ve “gerçek kişi” şeklinde iki ayrı kriter bulunmakta olup çalışmamızda “gerçek kişiye ilişkin olma” şeklinde tek bir kriter yer verilmiştir. İçerik itibarıyla aynı doğrultudaki açıklamaları ihtiva etmektedir.

⁴³ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, 26. Yasama Dönemi, 1. Yasama Yılı, Sıra Sayısı: 117

Tanımından da anlaşılacağı üzere veri kavramı çok geniş bir kümeyi ifade etmektedir. Bilgi ise anlamlandırılmış veri bütününe verilen isimdir. Tanımlar arasındaki farkın temelinde anlam unsuru yer almaktadır.

Bir verinin, kişisel veri olup olmadığının tespitinde verinin doğru olup olmadığı, verinin aleni bir veri olup olmadığı yahut verinin ne formda olduğu gibi konular, kavramın tespiti açısından önem arz etmemektedir. Örneğin, bir sosyal medya platformunda herkese açık olacak şekilde paylaşılan fotoğraf, aleni bir şekilde paylaşıldığı için kişisel veri olma niteliğini kaybetmez. Yahut verinin muhakkak fiziki bir formatta bulunmasına da gerek yoktur.⁴⁴ Örneğin, gerçek bir kişiye ait ses kaydı veya video kaydı da bir kişisel veridir.

Son olarak, kişisel verinin tespitinde verinin doğru olup olmamasının da bir önemi yoktur. Eğer yanlış veri, ilgili kişiyi belirli veya belirlenebilir kılıyorsa yanlış dahi olsa bir kişisel veridir.⁴⁵ Aynı şekilde, Madde 29 Veri Koruma Çalışma Grubu'nun⁴⁶ görüşüne göre verinin doğruluğunun da kanıtlanmış olması gerekmez.⁴⁷ Nitekim ilgili kişinin haklarını düzenleyen KVKK m. 11/ f. 1, d bendinden açıkça anlaşılacağı üzere, ilgili kişiye yanlış olan bir kişisel veriyi düzeltmeyi talep hakkı tanınmıştır.

b-Verinin Gerçek Kişiye İlişkin Olması

Kanunda yer alan kişisel veri tanımı içerisinde “gerçek kişiye ilişkin” ibaresi yer almaktadır. KVKK uyarınca, koruma kapsamı içerisinde gerçek kişiye ilişkin veriler yer almaktadır.

Kişisel Verileri Koruma Kurulu da tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesine ilişkin bir kararında,⁴⁸ tüzel kişilerin verilerinin KVKK kapsamında bulunmadığını ifade etmiştir. Kişisel Verileri Koruma Kurumu'nun konuya yaklaşımını iyi anlayabilmek adına bahsedilen kararla

⁴⁴ Mesut Serdar ÇEKİN/ Ahmet Esad BERKTAŞ/ M. Furkan AKINCI, **Veri Hukuku**, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2023, s. 6

⁴⁵ Hüseyin Can AKSOY, **Kişisel Verilerin Korunması**, Yayınlanmış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2008, s. 18 vd. (Erişim: 05.07.2023)

⁴⁶ Orijinal ismi “Article 29 Data Protection Working Party” olan Madde 29 Veri Koruma Çalışma Grubu, Direktifin 29. maddesi uyarınca kurulmuş bir çalışma grubudur. Veri koruma ve veri gizliliği alanında bağımsız bir kuruluş olan grubun görevleri Direktifin 30. maddesinde ve 2002/58/EC. sayılı direktifin 15. maddesinde açıklanmıştır.

⁴⁷ Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 01248/07/EN, WP 136, s. 6

⁴⁸ Kişisel Verileri Koruma Kurulu, 2018/131 Sayılı ve 19.11.2018 Tarihli Kararı

birlikte 2022/103 sayılı kararın⁴⁹ da incelenmesi gerektiği kanaatindeyiz. Zira ilk karar tek başına incelendiğinde, kararın kaleme alınış biçimi sebebiyle bir veri tüzel kişiliğe ait ise her halükârda KVKK kapsamı dışındadır gibi bir yanlış anlaşılmaya sebebiyet verebilecek niteliktedir. Ancak Kurumun konuya yaklaşımı çok daha kademelidir.

2022/103 sayılı karar, unvanında ilgili kişinin adının geçtiği bir şirket hakkında başlatılan icra takibine ilişkin dosya içeriğinin sosyal medyada paylaşılması hakkındadır. Kararda önce Madde 29 Veri Koruma Çalışma Grubu'nun 04.06.2007 tarihli ve 4/2007 sayılı görüşüne atıf yapılmış, tüzel kişiler hakkındaki bilgilerin bazı durumlarda gerçek kişilerle ilişkili olabileceği, ticari unvan içerisinde gerçek kişi isimlerinin bulunması durumunda kişisel veriyi tespit edebilmek için belirli kriterlere bakılması gerektiği ve bu kriterlerin içerik, amaç ve sonuç olduğu belirtilmiştir. Somut olay özelinde yapılan eylemin gerçek kişinin şahsına yönelik olmadığı, hedeflenen eylemin şirkete yönelik olduğu, gerçek kişinin şahsı üzerinde hak ve menfaatleri açısından bir etkiye sebebiyet vermediği ve bu nedenle de kişisel veri kavramını tanımını karşılamadığı belirtilmiştir.

Bu doğrultuda içerik unsuru, verinin direkt ilgili kişi hakkında olmasını; amaç unsuru veriyi işleme amacının ilgili kişiye ilişkin olmasını; sonuç unsuru ise veri işleme faaliyeti sebebiyle ilgili kişinin menfaatinin etkilenip etkilenmediğini ifade etmektedir.⁵⁰ Belirtmekte fayda var ki bu kriterlerden sadece bir tanesinin sağlanması yeterlidir. Kişisel Verileri Koruma Kurulu da benzer nitelikteki talep ve şikayetlerde Madde 29 Veri Koruma Çalışma Grubu'nun 04.06.2007 tarihli ve 4/2007 sayılı görüşünü referans almakta, değerlendirmesini de görüşte belirtilen içerik, amaç ve sonuç kriterlerine göre yapmaktadır.

Bir diğer önemli husus ise verinin gerçek bir kişiye ait olmaması fakat gerçek bir kişiyle ilişkili olması durumudur. Tanımlama uyarınca verinin gerçek kişiye ilişkin olması yeterli olup gerçek kişiye ait olması zorunlu değildir.⁵¹

⁴⁹ Kişisel Verileri Koruma Kurulu, 2022/103 Sayılı ve 10.02.2022 Tarihli Kararı

⁵⁰ DÜLGER, a.g.e., s. 170

⁵¹ Aradaki farkı bir örnek ile açıklamak gerekirse, bir benzin istasyonunda her pompadan sorumlu sadece bir işçinin olduğunu, ilgili bölümde hangi saatte ne kadar litre benzin satışı gerçekleştiği gibi verilerin kayıt altına alındığını varsayalım. Burada ilk bakışta işçiye ait hiçbir veri yok gibi görünebilir. Gerçekten de kriter, gerçek kişiye ait olma şeklinde ele alındığında burada işçiye ilişkin bir veri yok gibi görünmektedir. Zira veri, istasyona ilişkin gibi görünmektedir. Öte yandan bu kayıtlar, işçinin fazla mesai yapıp yapmadığı, ulusal bayram ve genel tatil günlerinde çalışıp çalışmadığı gibi performansı ve çalışmasına ilişkin birçok veriyi bize sunmaktadır. Dolayısıyla buradaki kayıtlar gerçek bir kişi ile

Gerçek kişiye ilişkin olma kriteri bakımından bir diğer önemli konu, ilgili kişinin ölmesidir. 4721 sayılı Türk Medeni Kanunu⁵² m. 28 uyarınca kişilik ölümle sona ermektedir. Bu nedenle, ölmüş bir kişinin verileri “gerçek kişiye ilişkin olma” kriterini sağlamamaktadır. Nitekim Kişisel Verileri Koruma Kurulu bir kararında⁵³ ölmüş bir kişinin eşinin Kuruma yaptığı başvuruda, ölmüş kişinin sağlık verilerini sağlığında tedavi gördüğü klinikten talep ettiğini fakat kliniğin bu verileri paylaşmadığı iddiasını incelemiş ve verinin ölmüş kişiye ait olduğunu, talepte bulunanın ise sağ olan eş olduğunu, ölüm sebebiyle kişisel verisi işlenen bir gerçek kişi olmadığını karara bağlamıştır.

c-Verinin Kişiyi Belirli Kılması veya Verinin Kişiyi Belirlenebilir Kılması

Bir kişisel veriden bahsedebilmek için diğer kriterlerin varlığıyla birlikte gerçek bir kişiye ulaşma durumundan veya gerçek kişiye ulaşabilme ihtimalinden bahsetmek gerekir. Bazı durumlarda bunun tespiti çok kolaydır. Örneğin bir kişinin adı soyadı, telefon numarası, doğrudan ilgili kişiyi belirli kılan bir kişisel veridir.

Bazı durumlarda ise birkaç unsur birleşmek suretiyle, başka bilgilerin de değerlendirilmesiyle kişi belirlenebilir hale gelir. İşte bu durumda da yine diğer kriterlerin varlığıyla birlikte bir kişisel veriden bahsedebilmek mümkündür.

Daha farklı bir anlatım ile ilk bakışta kişinin direkt tespit edilmediği fakat bir bilgi kombinasyonu (özgün kombinasyon) ile belirlenebilir olduğu durumlarda da kişisel veriden bahsetmek mümkündür.⁵⁴

Belirli ve belirlenebilir kişiyi örnekler ile açıklayalım. Örneğin, sıklıkla online alışveriş sitelerinde ad soyad, telefon numarası, e-posta adresi, ev adresi gibi kişisel verilerimizi paylaşmaktayız. Ya da kamu kurumlarında işlemlerimizi gerçekleştirmek için TC kimlik numarası bilgisi paylaşmaktayız. Bu veriler şüphesiz kişisel verilerdir.

Bazı durumlarda ise dolaylı olarak kişi belirlenebilir durumdadır. Örneğin X otelinin tek sahibi, A bankası Altunizade şubesinin tek güvenlik görevlisi bu şekildedir.

ilişkilendirilebilir niteliktedir ve bu nedenle kişisel veri içermektedir. Sonuç itibarıyla, veri doğrudan gerçek bir kişiye ait olmasa bile verinin gerçek bir kişi ile ilişkilendirilebilme imkânı mevcut ise kişisel veriden söz edilebilme ihtimali vardır.

⁵² RG., 24607 S., 08.12.2001 T.

⁵³ Kişisel Verileri Koruma Kurulu, 2019/273 Sayılı ve 18.09.2019 Tarihli Kararı

⁵⁴ Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 01248/07/EN, WP 136, s. 13; LAMBERT, s. 62 ; Paul VOİGT ve Axel VON DEM BUSSCHE, **The EU General Data Protection Regulation (GDPR), A Practical Guide**, Cham: Springer, 2017, s. 11

Bazı hallerde ise bir veri kayıt sistemi üzerinden sorgulama yapılmak suretiyle ilgili kişiye ulaşmak mümkün olabilir. Örneğin herhangi bir vatandaş, araç plakasından araç sahibinin kim olduğunu öğrenme imkanına sahip değildir ve bu nedenle o kişi için araç plakası ilk bakışta kişisel veri gibi durmayabilir. Fakat Emniyet Genel Müdürlüğü tarafından araç plakasından aracın sahibinin kim olduğu sorgulanabilmektedir. Dolayısıyla harf ve rakam kombinasyonundan oluşan plaka aslında gerçek kişiyi belirlenebilir kıldığından bir kişisel veridir.

Kişinin belirlenebilir olması ihtimali akla bazı soruları getirmektedir. Örneğin çok büyük çabalar sonucu birçok veri birleştirilerek gerçek bir kişiye ulaşılabilmesi mümkünse yine kişisel veriden bahsedilebilir mi? Ya da çok az çabayla olmakla birlikte sadece üç kişi açısından kişinin belirlenebilir olduğu, bunun dışında kimsenin veriyi anlamlandıramadığı, kişiyi tespit edemediği durumlarda da kişisel veriden bahsetmek mümkün müdür?

Belirlenebilirlik kriterinin sağlanabilmesi için kişinin herkes tarafından belirlenebilir olmasına gerek yoktur. Küçük bir grubun kişiyi belirleyebilir nitelikte olması dahi yeterli görünmektedir.⁵⁵ Örneğin kan değerleri aşırı derecede kötü olan bir hastanın doktoru tarafından, sadece kan değerlerinin yazılı olduğu tahlil evrakına bakılarak tanınabilmesi bu şekildedir. O doktordan başka kimsenin tahlile bakarak sonucun kime ait olduğunu bilmesine imkân yoktur. Ancak tek bir doktor açısından dahi o kişi belirlenebilir bir kişidir. Bu nedenle de kişisel veriden bahsedebilmek mümkündür.

Öte yandan, belirlenebilirlik açısından harcanacak eforun ne seviyede olması gerektiği bir başka önemli sorudur. Belirlenebilirlik ihtimali, makul düzeyde bir çaba ile ortaya çıkabiliyorsa diğer kriterlerin varlığıyla birlikte bir kişisel veriden bahsedebilmek mümkündür. Nitekim GDPR gerekçesinde⁵⁶, veri sorumlusunun veya bir başka kişinin makul olarak kullanılabileceği bütün araçların göz önünde bulundurulması gerektiği belirtilmiştir. Buna göre “makul olma” derecesinin somut olayın özelliklerine göre değerlendirilmesi gerekmektedir.

⁵⁵ Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 01248/07/EN, WP 136, s. 15

⁵⁶ Avrupa Birliği Resmi Gazetesi, L 119 S., 04.05.2016 T.

Bazı durumlarda kişinin belirlenebilir hale gelmesi için bilirkişi düzeyinde teknik bir inceleme yapılması, raporlanması ve bu bilginin de başka bilgiler ile eşleştirilmesi gerekebilir. Kanaatimizce bilgiye ulaşabilmek için bu seviyede eforu gerektiren bir veri, kişisel veri değildir.⁵⁷

B-Özel Nitelikli Kişisel Veri

Özel nitelikli kişisel veri, KVKK m. 6'da *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"*⁵⁸ özel nitelikli kişisel veridir." demek suretiyle sınırlayıcı olarak tanımlanmıştır.

⁵⁷ Yüksek efor harcanmasını gerektiren bir örnek olarak GSM operatöründe çalışan bir işçinin bilmediği bir numaradan aranarak tehdit edildiğini ve çalışanın da bu kişinin kimliğini tespit etmek istediğini ele alalım. Bu ihtimalde çalışan, çalıştığı şirketin kullanımına sunduğu veri tabanından faydalanmak suretiyle kişinin adının Mustafa YILMAZ olduğunu, bir soruşturma dosyası kapsamında ilgili telefon sahibi hakkında savcılıktan müzekkere yazıldığını ve çalıştığı firma tarafından müzekkereye cevap verildiğini, soruşturma numarasının bu evrakta görüldüğünü ve ev adresinin ise mahalle, sokak, bina numarası, ilçe, il şeklinde olduğunu ve fakat kapı numarası içermediğini varsayalım. Bu durumda kapı numarası eksik olsa dahi eksik adres bilgisinin bir kişisel veri olup olmadığının incelenmesi gerekir. Kimliği tespit etme noktasında kararlı olan çalışan, elde ettiği adrese gider. Zillere baktığında apartmanda Mustafa YILMAZ adında iki farklı kişinin oturduğunu tespit eder. Her ne kadar elinde telefon numarası, ad soyad ve apartman bilgisi olsa da kendisini telefonda tehdit eden kişinin tam olarak kim olduğunu belirleyemez. Bu sebeple avukat olan bir arkadaşına ilgili kişi hakkındaki soruşturma numarasını vererek belirtilen dosyadaki şüphelinin adres bilgisini temin etmesini talep eder. Arkadaşı da bu talebi geri çevirmez ve bir şekilde soruşturma dosyasından kişinin adres bilgisini elde eder. Çalışan elindeki bütün verileri birleştirmek suretiyle kendisini tehdit eden kişiyi tespit eder. Bu örnekte eksik bir adres bilgisinin kişisel veri olabilmesi için önce bir GSM operatörünün veri tabanından faydalanılmış, fiziken belirtilen adrese gidilip apartman zilleri kontrol edilmiş, ardından avukat arkadaşı ile soruşturma numarası paylaşılmış ve en sonunda da eksiksiz adres bilgisi temin edilmiş ve kişi belirli hale gelmiştir. İşte burada harcanan efor çok yüksek bir efordur. Bu örnekte makul seviyenin çok üzerine çıkmıştır. Bu sebeple örneğin gerçekleşme şeklindeki eksik adres bilgisi bir kişisel veri değildir. Bir an için akla, ilgili kişinin eyleminin şikayet edilmesi suretiyle savcılık tarafından da rahatlıkla tespit edilebileceği ve bu kadar ciddi bir efora gerek olmadığı düşünülebilir. Fakat burada da kanaatimizce veriye savcılık, mahkeme gibi kanallar ile erişilebilmesi de makul bir düzeyin üzerinde çabayı gerektirmektedir. Nitekim savcılık da soruşturma sürecinde yine GSM operatöründen ilgili kişinin bilgilerini isteyecek, bu eksik bilgiler sebebiyle ilgili birime müzekkere yazılarak adres tespiti yapılması talep edilecek ve kişi bu sefer de polis marifetiyle tespit edilmiş olacaktır. Dolayısıyla ortada yine yüksek seviyede bir efor söz konusu olacaktır.

⁵⁸ KVKK her ne kadar *"genetik veri"* kavramına yer vermiş olsa da genetik veri kavramına tanım olarak yer vermemiştir. GDPR ise genetik veri kavramını *"bir kişinin kalıtsal ve edinilmiş genetik özelliklerine ilişkin kişisel veriler"* olarak tanımlamıştır. Bkz. Lee A. BYGRAVE, Luca TOSONI "Article 4(13) Genetic Data", iç. **The EU General Data Protection Regulation (GDPR), A Commentary** (Ed. Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY), Croydon : Oxford University Press, Nitekim 196. ve devamı sayfalarda (özellikle s. 202) bu tanımın teknolojik gelişmeler karşısında yetersiz kaldığını ve uygulanabilirliğinin azaldığını belirterek teknolojik gelişmelere daha uygun bir tanımın daha yerinde olacağını belirtmiştir.

Bahsi geçen verilerin ortak özelliği, öğrenilmesi halinde veri sahibi hakkında ayrımcılık yapılmasına sebebiyet verebilecek nitelikte olmasıdır.⁵⁹ Bu sebeple de KVKK, bu verilere özel bir önem atfetmektedir. Bu doğrultuda -ileride daha detaylı açıklanacağı üzere-⁶⁰ özel nitelikli kişisel verilerin işlenme şartları, kişisel verilerin işlenme şartlarından ayrılmıştır.

KVKK, özel nitelikli kişisel veriler bakımından büyük oranda diğer ulusal düzenlemeler ile aynı doğrultudadır. Örneğin GDPR, Direktif, 108 Sayılı Sözleşme gibi önemli kaynaklarda da özel nitelikli kişisel veri şeklinde ayrı bir kategori söz konusudur.

Öte yandan, kılık kıyafet şeklindeki özel nitelikli kişisel veri türü, Türkiye’ye özgü bir özel nitelikli kişisel veridir. Kılık kıyafet ile kastedilen kişi hakkında ayrımcılığa sebebiyet verebilecek şekilde bir veri tutulmasıdır. Örneğin çalışan adayı seçme ve yerleştirme süreçlerini yürüten bir şirketin insan kaynakları departman müdürünün çalışan adayları hakkında “türbanlı” veya “çok kısa bir etek giymişti” şeklindeki özgeçmiş üzerine aldığı notlar bu şekildedir.

Özel nitelikli kişisel veriler bazı durumlarda KVKK’de sayıldığı şekilde direkt karşımıza çıkmamaktadır. Bazı durumlarda simgeler, semboller de bir özel nitelikli kişisel veriye çağrışım yapabilecek niteliktedir. Örneğin bir veri sorumlusu, çalışan adayı seçme sürecinde çalışan adaylarından hangi siyasi partiyi desteklediğini sormayabilir. Fakat görüşme tutanaklarında adayın bıyık kesimi, sakalı ile ilgili notlar alabilir ki bu notları alırken kastı, siyasi düşüncesine yönelik kanaatini bildirmek olabilir. Kanaatimizce, KVKK’de sayıldığı şekilde direkt olarak özel nitelikli kişisel veri olmasa bile mevcut veri, ortalama zekaya sahip bir Türkiye Cumhuriyeti vatandaşı nezdinde kişinin siyasi, dini eğilimi gibi konularda bir fikir uyandıracak nitelikte ise özel nitelikli kişisel veridir. Dolayısıyla burada amaç unsurunun⁶¹ önem arz ettiğini belirtmek isteriz.⁶²

⁵⁹ Kişisel Verileri Koruma Kurumu, **Özel Nitelikli Kişisel Verilerin İşlenme Şartları Rehberi**, s. 1 www.kvkk.gov.tr, (Erişim Tarihi: 06.07.2023)

⁶⁰ Bkz: s. 85 vd.

⁶¹ Aynı görüşte DÜLGER, a.g.e, s. 179

⁶² Madde 29 Veri Koruma Çalışma Grubu da verilerin toplanma yöntemi ve toplanmaktaki amacının bu süreçte değerlendirilmesi gerektiği; bir verinin salt özel nitelikli kişisel veri olmamasının o veriyi özel nitelikli kişisel veri kapsamı dışına çıkarmayacağı görüşündedir.; Aynı doğrultuda Christian TINNEFIELD, Henrik HANSSEN, “Mobile Health in the EU (Part 2): **Personal Data and Sensitive Information in Health Businesses**”,

Bazı durumlarda ise özel nitelikli kişisel veri, veri sorumlusu istemediği halde dolaylı olarak kendisine gelmektedir. Örneğin başörtülü bir işçi adayı, iş başvuru formuna herhangi bir fotoğrafını eklediğinde ilk bakışta veri sorumlusu, kılık kıyafet verisi almış gibi görülebilir. Fakat burada veri sorumlusunun gayesi, kişinin kılık kıyafet verisini almak, dini eğilimlerini tespit etmek değildir. Dolayısıyla bu örnekte fotoğrafın özel nitelikli bir kişisel veri olarak değil bir kişisel veri olarak değerlendirilmesi gerekir.

C-Veri Kayıt Sistemi

Veri kayıt sistemi tanımı, birazdan açıklayacağımız⁶³ kişisel verilerin işlenmesi tanımının önemli bir ayağını oluşturmaktadır. Zira, kişisel verilerin işlenmesi KVKK m. 3/ f. 1, e bendinde *“Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.”* şeklinde tanımlanmıştır. Buradan hareketle bir kişisel veri işleme faaliyetinden bahsedilebilmesinin bir yolu da bir veri kayıt sistemi olması ve kişisel verilerin de otomatik olmayan yollar ile elde edilmesi, kaydedilmesi, depolanması gibi veri üzerinde bir işlemin gerçekleşmesidir. Öyleyse veri kayıt sistemi nedir?

Veri kayıt sistemi, KVKK m. 6/ f. 1, h bendinde *“Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi”* şeklinde tanımlanmıştır. Buradan hareketle veri kayıt sisteminden bahsedebilmek için belirli kriterlere göre kategorize edilmiş bir sistem gereklidir. Örneğin bir şirkette çalışanların yaş gruplarına göre sıralanması, performanslarına göre bir tabloda toplanması, bu kapsamda değerlendirilmektedir. Buna göre birinci örneğimizde yaş grubu çalışanlar açısından kriteri oluşturmaktayken ikinci örneğimizde performans verileri kriteri oluşturmaktadır. Dolayısıyla bu şekildeki bir çalışma, ister bir ajandaya not edilmiş olsun isterse dijital ortamda herhangi bir araç ile kayıt altında bulunuyor olsun her durumda veri kayıt sistemi bulunduğu söylenebilir.

<https://www.engage.hoganlovells.com/knowledgeservices/news/mobile-health-in-the-eu-part-2-personal-data-and-sensitive-information-in-mhealth-businesses> (Erişim: 07.07.2023)

⁶³ Bkz: s. 27

KVKK’de veri kayıt sistemine ilişkin yapılan tanımlamanın mefhum-u muhalifinden belli bir kriter olmaksızın rastgele kayıt altına alınan bilgilerin veri kayıt sistemi dışında tutulduğu söylenebilir. Örneğin bir şirketin satın alma departman müdürünün görüştüğü kişinin telefon numarasını ve e-posta adresini bir bloknota yazması ve kullandıktan sonra da bu bloknotu atması halinde bloknota rastgele yazılan bu bilgi⁶⁴ herhangi bir kritere göre oluşturulmadığından bir veri kayıt sisteminden bahsetmek mümkün değildir. Burada önemle altını çizmek gerekir ki verilen örnek, sadece veri kayıt sistemi olmamasına ilişkindir yoksa yine de bu bloknota alınan veriler kişisel veri teşkil etmektedir.

Öte yandan, kişisel veri kayıt sisteminden bahsederken tanım içerisinde yer alan “kriter” unsuru her zaman ve herkesçe çok rahatlıkla anlaşılamayabilecek bir unsur olabilir. Örneğin bir şirketteki çalışanların yaş grubuna göre sıralanması durumunda buradaki kriterin yaş grubu olduğu ilgili dokümandan veya dijital kayıttan çok rahatlıkla anlaşılabilecek niteliktedir.

Bazı durumlarda ise kriter unsuru herkesçe anlamlandırılmayabilir. Daha farklı bir anlatım ile ortalama zekaya sahip bir vatandaşın ilk görünüm itibarıyla kriterin ne olduğunu anlamlandıramaması söz konusu olabilir. Tam da bu noktada üç kaynak, sorunun cevabına ışık tutabilir.

Bunlardan birincisi “Durant v Financial Services Authority” isimli davadır.⁶⁵ Veri kayıt sisteminin ihtilaf konusu olduğu davaya bakan İngiliz Yüksek Mahkemesi, bir veri kayıt sisteminden bahsedebilmek için iki noktaya vurgu yapmaktadır. Bunlar “veriye kolay erişilebilirlik” ve “dosyalama sistemin yeterli derecede sofistike olması” şeklindedir. Buradan hareketle, veri kayıt sistemi olup olmadığı tartışma konusu olan bir sistem açısından ilk değerlendirme noktası, sistemin kişisel verilere kolay erişilebilirliği sağlayıp sağlamadığının tespit edilmesidir. Bunu değerlendirmenin en kolay yolu belirli referansların, indekslerin olup olmadığını belirlemektir. Örneğin kişinin yaşı, mesleği, maaş bilgisi gibi bir kriter referans noktası olabilir ve sistem

⁶⁴ Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, s.24; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, s. 29 (www.kvkk.gov.tr) (Erişim:07.07.2023)

⁶⁵ Michael John Durant v Financial Services Authority, Royal Courts of Justice, Case No: B2/2002/2636, 8 Aralık 2003 (<http://www.bailii.org/ew/cases/EWCA/Civ/2003/1746.html>) (Erişim: 07.07.2023)

bunun üzerine kurulmuş olabilir. Dolayısıyla burada kolay erişilebilirlikten söz edilebilir.

İkinci kaynağımız ise İngiltere Veri Koruma Otoritesi'nin (ICO) “Veri Kayıt Sistemi Sıkça Sorulanlar” isimli rehberidir.⁶⁶ Bu rehberde tavsiye edilen, bir sistemin veri kayıt sistemi olup olmadığı konusunda ihtilaf yaşanması halinde “Temp Test” adı verilen stajyer testinin uygulanmasıdır. Buna göre eğer stajyer pozisyonunda bulunan, özel bir yatkınlığı ve evrak aşinalığı olmayan⁶⁷ bir kişi, mevcut sistem içerisinde istenilen bilgiye kolayca erişebiliyor ise bir veri kayıt sisteminden, dosyalama sisteminden bahsedebilmek mümkündür.

Son olarak, bu konudaki en önemli referans kaynağımız Kişisel Verileri Koruma Kurumu'nun konuyla ilgili yayımladığı “100 Soruda Kişisel Verilerin Korunması” ve “Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulanlar” isimli iki rehberdir.⁶⁸ Buna göre veri kayıt sisteminden bahsedebilmek için temel nokta, “kişisel verilerin belirli kriterlere göre yapılandırılması” ve “elektronik veya fiziki olarak bir dosyalama sisteminin bulunması” şeklindedir.

Netice itibariyle bir sistemin veri kayıt sistemi olup olmadığı konusunda tereddüt yaşıyor ise öncelikle belirli kriterlere göre bir yapılandırma olup olmadığı kontrol edilmeli, dosyalamanın bu kriter referans alınarak mı yapıldığı incelenmeli, atıf yapılan mahkeme kararında olduğu gibi sistemin veriye erişimi kolaylığı hedefleyip hedeflemediği incelenmeli, kolaylık noktasında tereddüt yaşıyor ise de ICO tarafından öngörülen stajyer testi uygulanmalıdır. KVKK uyarınca ilk iki kriter yeterli görülmeyle birlikte gerek rehberlerde gerekse Kişisel Verileri Koruma Kurulu kararlarında konuyla ilgili çok detaylı bir açıklamaya yer verilmediği için kanaatimizce yukarıda bahsettiğimiz veriye kolay erişilebilirlik unsuru ve bu unsurun stajyer testi metodu ile analizi son derece önemlidir.

⁶⁶ Frequently Asked Questions and Answers About Relevant Filing Systems, Information Commissioners Office (ICO)

⁶⁷ DÜLGER, a.g.e., s. 186

⁶⁸ Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, s.24; Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, s. 29 (www.kvkk.gov.tr) (Erişim:07.07.2023)

Ç-Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, KVKK m. 3/ f. 1, e bendinde “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” şeklinde tanımlanmıştır.

Tanımın daha net anlaşılabilmesi için otomatik olan ve otomatik olmayan veri işleme faaliyetlerinin ayrılması gerekmektedir. Kanun, otomatik olan yollar ile kişisel verilere ilişkin her türlü faaliyeti kişisel verilerin işlenmesi olarak kabul etmiştir. Veri işleme faaliyeti ister tamamen otomatik olsun ister kısmen otomatik olsun bu kapsamda yer almaktadır. Peki kişisel verilerin otomatik yollar ile işlenmesi ne demektir?

Kişisel verilerin otomatik yollar ile işlenmesi, kişisel verilerin bilişim sistemleri kullanılmak suretiyle bir faaliyete konu edilmesini ifade etmektedir.⁶⁹ Bu yöntemde verinin işlenmesi esnasında bilgisayar, telefon gibi işlemci sahibi bir cihaz kullanılmakta veya insan müdahalesinin minimum seviyede olduğu bir algoritma aracı olmaktadır.⁷⁰

Bir kişisel verinin elde edilmesi, bir kişiye aktarılması, bir bilgisayarda arşivlenmesi, kişisel verilerin silinmesi gibi veri üzerinde gerçekleştirilen her türlü faaliyet, bir kişisel veri işleme faaliyetidir.⁷¹ Örnekleyci olarak sayılan bu faaliyetlerin, daha çok bilişim sistemleri aracı kılınmak suretiyle gerçekleştirilmesi halinde otomatik bir veri işleme faaliyetinden bahsedilecektir. Örneğin bir veri sorumlusu web sitesinde yer verdiği iletişim panelinde, iletişim konusu olarak talep, şikayet ve öneri olmak üzere üç ayrı başlığa yer vermiş olsun. İlgili kişiler tarafından bu panel kullanıldığında sistem bunu otomatik olarak talep konusuna göre ayırt ediyor,

⁶⁹ DÜLGER, a.g.e., s. 185

⁷⁰ Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, s. 22, (www.kvkk.gov.tr), (Erişim: 09.07.2023)

⁷¹ GDPR’da veri işleme “*processing*” kavramı ile ilgili daha detaylı bilgi için bkz. Luca TOSONİ, Lee A. BYGRAVE, “Article 4(2) Processing”, iç. **The EU General Data Protection Regulation (GDPR), A Commentary** (Ed. Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY), Croydon : Oxford University, 2020, s. 116

kişilerin adını soyadını, talep konusunu ve telefon numaralarını kategorize edebiliyorsa kişisel verilerin otomatik yolla işlenmesi söz konusudur.

Öte yandan bilişim sistemleri kullanımının minimuma indirildiği ve insan faktörünün ön plana çıktığı faaliyetler ise otomatik olmayan kişisel veri işleme olarak nitelendirilmektedir. Örneğin bir şirketteki insan kaynakları departman yetkilisinin görevlendirme süreçlerini yürütebilmek amacıyla bir A4 kağıdına kendi eliyle yıllık izne ayrılan personellerin adını soyadını, departmanını ve izne ayrıldığı tarihleri yazması halinde otomatik olmayan bir veri işleme faaliyetinden söz edilecektir. Yeri gelmişken hemen belirtmek gerekir ki otomatik olmayan yollar ile kişisel verilerin işlenmesinden bahsedebilmek için otomatik yollardan farklı olarak bir veri kayıt sisteminin bulunması gerekmektedir. Veri kayıt sisteminin ne olduğu bir önceki başlıkta açıklandığından burada tekrar edilmeyecektir.⁷²

Netice itibarıyla kişisel verilerin işlenmesinden bahsedebilmek için öncelikle bir faaliyet bulunması gerekmektedir. Bu faaliyet kişisel veriler üzerinde yapılan her türlü işlem olabilmektedir. Burada bir sınırlama söz konusu değildir.⁷³

Kişisel veri üzerinde gerçekleştirilen bir faaliyet varsa ikinci bakılması gereken şey bu faaliyetin otomatik yollar ile mi yapıldığı yoksa otomatik olmayan yollar ile mi yapıldığıdır. Şayet faaliyet tamamen veya kısmen otomatik yollar ile gerçekleştirilebiliyor ise kişisel verilerin işlenmesinden söz edilebilir.

Öte yandan faaliyet otomatik olmayan yollar ile gerçekleştiriliyor ise yani insan faktörü maksimum bilişim faktörü ise minimum seviyede ise burada ek olarak bir veri kayıt sisteminin de bulunması gerekmektedir. Buna göre, eğer kişisel veri üzerinde gerçekleştirilen faaliyet otomatik olmayan yollar ile gerçekleştiriliyor ancak bu faaliyet bir veri kayıt sistemine bağlı olarak yapılmıyor ise kişisel verilerin işlenmesinden söz edilemeyecektir.

D-İlgili Kişi

İlgili kişi, KVKK m. 3/ f. 1, ç bendinde “*Kişisel verisi işlenen gerçek kişi*” şeklinde tanımlanmıştır. Tanımdan da anlaşılacağı üzere ilgili kişiden bahsedebilmek için öncelikle bir gerçek kişi bulunması gerekmektedir. Verisi işlenen kişi, KVKK

⁷² Bkz: s. 24

⁷³ Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, s. 22, (www.kvkk.gov.tr), (Erişim: 09.07.2023)

uyarınca ilgili kişi olarak tanımlanmaktadır. Örneğin bir şirketin çalışanı, müşterisi, bir şirkete özgeçmiş bırakan çalışan aday gibi kişiler ilgili kişi olabilir.

Uygulamada genellikle ilgili kişi kavramının yerine veri sahibi kavramının da kullanıldığı görülmektedir. Bu kavramların birbirinin yerine kullanılmasında bir sakınca olmamakla birlikte KVKK’de veri sahibi yerine ilgili kişi kavramı tercih edildiği için bizler de çalışmalarımızda ilgili kişi kavramını tercih etmekteyiz.

İlgili kişi tanımıyla ilgili değinmek istediğimiz son nokta çocuklara ilişkindir. Tanımdan anlaşılabileceği üzere ilgili kişiden bahsedilebilmesi için bir gerçek kişinin bulunması ve verilerin de bu gerçek kişiye ait olması yeterli ve gereklidir. Bu nedenle verisi işlenen kişinin bir çocuk olması ile bir yetişkin olması arasında KVKK bakımından hiçbir farklılık bulunmamaktadır.⁷⁴ Bu nedenle çocuklar da ilgili kişi olabilmektedir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında⁷⁵ “ilgili kişi sıfatını haiz çocuk” kavramını kullanmıştır. Buradan da çocuğun ilgili kişi olabileceği rahatlıkla anlaşılabilmektedir.

E-Veri Sorumlusu

Veri sorumlusu, KVKK m. 3/ f. 1, 1 bendinde “*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” şeklinde tanımlanmıştır. Buna göre, ilgili kişiden farklı olarak veri sorumlusu tüzel kişi de olabilmektedir.

Kanunda yer alan tanımdan hareketle veri sorumlusundan bahsedebilmek için öncelikle gerçek veya bir tüzel kişi bulunmalıdır. Bu tüzel kişi ya da gerçek kişi, kişisel verilerin işleme amaçlarını belirlemeli, kişisel verilerin işleneceği araçları belirlemeli ve ilaveten, kişisel verilerin yer alacağı veri kayıt sisteminin kurulmasından ve yönetilmesinden de sorumlu olmalıdır. Dolayısıyla bir veri sorumlusundan bahsedebilmek için bu şartların tümünü bir arada sağlanması gerekmektedir.

⁷⁴ Mevzuatımızda her ne kadar çocuk bakımından ayrı bir değerlendirme yapılmasa da Article 29 Data Protection Working Party çocukların kişisel verilerinin korunmasına yönelik esasları Opinion 2/2009 adlı çalışmada açıklamıştır. Daha detaylı bilgi için bkz. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf (Erişim: 03.10.2023)

⁷⁵ Kişisel Verileri Koruma Kurulu’nun “İlgili kişi anne ve ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapıldığı iddiası” hakkında 02/12/2021 tarihli ve 2021/1217 sayılı karar özeti (www.kvkk.gov.tr) (Erişim: 10.07.2023)

Veri sorumlusu bir tüzel kişi olabileceği gibi gerçek kişi de olabilir. Nitekim Kişisel Verileri Koruma Kurulu bir kararında⁷⁶ bir avukatın veri sorumlusu olduğuna hükmetmiştir. Yine bir başka kararda⁷⁷ ise bir doktorun veri sorumlusu olduğu tespit edilmiştir. Dolayısıyla Kişisel Verileri Koruma Kurulu’nun gerçek kişiler adına da veri sorumlusu sıfatıyla idari para cezasına hükmedebildiği görülmektedir.

Veri sorumlusunu doğru bir şekilde tespit edebilmek KVKK açısından son derece önemlidir. Çünkü KVKK kapsamındaki yükümlülüklerin neredeyse tamamı, veri sorumlusu tarafından yerine getirilmesi gereken yükümlülüklerdendir. Bu nedenle de kanuna aykırılık halinde yaptırımların muhatabı olan kişi, veri sorumlusudur.

Yeri gelmişken belirtmekte fayda var ki veri sorumlusu uygulamada en çok veri işleyen ile karıştırılmaktadır. Veri işleyen tanımı çalışmamızın bu bölümünde açıklanacaktır⁷⁸ ancak çok detaya yer vermeden şunu belirtmek gerekir ki veri sorumlusu genellikle veri işleyene talimatta bulunan, emirler veren, veri işleyen üzerinde denetim yetkisine sahip olan, veri işleyen kişisel veriyle ne yapabileceğinin sınırlarını çizen, kontrol mekanizmasına sahip olan gerçek veya tüzel kişidir. Dolayısıyla veri sorumlusu kişisel verilerin yönetimi ve kontrolü bakımından adeta veri işleyenin amiri gibidir.

Veri sorumlusuyla ilgili bir diğer önemli konu ise veri sorumlusunun kendi bünyesindeki kişilerin KVKK kapsamındaki pozisyonunun ne olduğudur. Örneğin, sekiz departmanı olan bir şirkette insan kaynakları departmanı acaba veri sorumlusu mudur ya da hem şirket hem de bütün departmanlar ayrı ayrı veri sorumlusu olarak değerlendirilebilir mi? Hemen belirtmek gerekir ki bir şirketin departmanları şirketin işlediği kişisel veriler bakımından veri sorumlusu olamaz çünkü kişisel verilerin hangi amaçlar ile kullanılacağı, kişisel verilerin işlenmesinde hangi araçların kullanılacağı gibi karar ve kontrol mekanizması her zaman şirketin tüzel kişiliğine aittir.⁷⁹ Bu nedenle de bir şirketin herhangi bir departmanının ya da bir şirkette çalışan herhangi

⁷⁶ “Kişisel verilerin veri sorumlusu bir avukat tarafından kısa mesaj yoluyla üçüncü kişilere ifşa edilmesi hakkında” Kişisel Verileri Koruma Kurulu’nun 14.01.2020 Tarihli ve 2020/26 Sayılı Karar Özeti; Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen Rehberi, s. 8, (www.kvkk.gov.tr), (Erişim: 11.07.2023)

⁷⁷ “İlgili kişinin telefon numarasının hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/923 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 11.07.2023)

⁷⁸ Bkz: s. 32

⁷⁹ Kişisel Verileri Koruma Kurumu, **Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)**, s.18, (www.kvkk.gov.tr), (Erişim: 11.07.2023)

bir departman çalışanının veri sorumlusu olabilmesi mümkün değildir. Bu tespitin en önemli sonucu, bir şirkette herhangi bir departmanda meydana gelecek ve KVKK kapsamında hukuka aykırılık teşkil edecek eylemin sorumlusu, o departman veya o departmandaki ilgili kişi değil şirkettir.

Veri sorumlusuyla ilgili değinmek istediğimiz son husus ise tarafların aralarında tanzim edebileceği bir sözleşme ile bu sıfatı belirleyip belirleyemeyeceğidir. Uygulamada genellikle veri sorumlusu-veri sorumlusu veya veri sorumlusu-veri işleyen arasında kişisel veri aktarımına ilişkin sözleşmeler yapılmakta ve bu sözleşmeler uyarınca taraflardan hangisinin veri sorumlusu olduğu hangisinin veri işleyen olduğu tespit edilebilmektedir. Acaba taraflar, sözleşme yapmak suretiyle bir kişinin veri sorumlusu olduğunu düzenleyebilir mi?

Kişisel Verileri Koruma Kurulu bu konuya ilişkin vermiş olduğu bir kararında tarafların yapacağı nitelendirmenin bir öneminin bulunmadığını, önemli olan kriterlerin KVKK’de belirtildiğini, bu nedenle bir kişinin veri sorumlusu ya da veri işleyen sıfatının olup olmadığının değerlendirilmesinde KVKK’de belirtilen kriterlerin göz önünde bulundurulacağını belirtmiştir.⁸⁰

Netice itibarıyla veri sorumlusu tanımı, kanun kapsamındaki en önemli tanımlardan birisi olup KVKK kapsamındaki yükümlülüklerin kim tarafından yerine getirileceği, idari para cezalarının kim adına hükmedileceği, KVKK kapsamında gerçekleştirilecek başvuruların, talep ve şikayetlerin muhatabının kim olacağı hususlarının tespiti açısından son derece önemlidir.

⁸⁰ “İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/78 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 12.07.2023), kararın ilgili kısmı aynen “*Şikâyet konu olayda avukatlık ortaklığı tarafından sunulan savunmada veri sorumlusu müvekkileri ile aralarındaki sözleşme gereği veri sorumlusu sıfatını haiz olmadıkları belirtilmişse de veri sorumlusu sıfatını tayin etmede Kanun çerçevesinde yapılacak değerlendirme için bu sözleşmede yer alan nitelendirmenin esas alınamayacağı; bununla birlikte ilgili kişiye ilişkin kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan, ilgili kişinin ortağı olduğu şirkete ait iletişim numaralarını borcun tahsili amacı ile avukatlık ortaklığı ile paylaşan GSM operatörü şirketin, “veri sorumlusu”; veri sorumlusunun verdiği talimat çerçevesinde ilgili kişiye ait olduğu belirtilen iletişim numaralarına borcun tahsili amacıyla kısa mesaj gönderen avukatlık ortaklığının ise veri işleyen olarak tanımlanabileceği,*” şeklindedir.

F-Veri İşleyen

KVKK m. 3/ f. 1,  bendi uyarınca veri işleyen “*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak tanımlanmıştır. Maddeden anlaşılacağı üzere veri işleyen gerçek kişi olabileceği gibi tüzel kişi de olabilmektedir. Veri işleyen kavramıyla kastedilen, veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına bu verileri işleyen kişilerdir.

Örneğin toplu SMS hizmeti sunan B firması, A firması ile yaptığı sözleşme uyarınca A firmasının kendisine göndereceği telefon numaralarına, yine A firmasının belirleyeceği mesaj içeriğini hiçbir değişiklik yapmaksızın gönderecektir. Bu örnekte müşterilerin telefon numarasını toplayan, toplu SMS gönderme konusunda karar yetkisine sahip olan, bunu hangi firma ile çalışarak gerçekleştireceğini belirleme imkanına sahip olan, çalışacağı firmaya göndereceği bilgiler ile ne yapılacağını sınırını çizen A firması olduğu için A firması veri sorumlusu, A firmasından aldığı yetkiye dayanarak onun adına toplu SMS gönderen B firması ise veri işleyendir.

Her ne kadar veri sorumlusu ile veri işleyenler arasında bariz farklılıklar bulunsa da bazı durumlarda bir kişi hem veri sorumlusu hem de veri işleyen olabilir. Örneğin biraz önce açıklamış olduğumuz toplu SMS hizmeti sunan firma açısından verilen örnekte firmanın veri işleyen olduğunu belirtmiştik. Bununla birlikte ilgili firma, çalışanlarının verileri bakımından ise veri sorumlusudur. Dolayısıyla bir kişinin aynı zamanda hem veri sorumlusu hem de veri işleyen olabilmesi mümkündür. Veri sorumlusu ile veri işleyen arasında farklar bulunması bu duruma engel değildir.

Genellikle veri sorumlusu ile veri işleyen arasında bir yetki devri söz konusudur. Daha açık bir anlatım ile, veri sorumlusu kişisel verileri toplamakla birlikte bu verilerin farklı şekillerde kullanılmasını istediği süreçte şirket dışından destek alabilmekte ve aslında kendi gerçekleştirebileceği bir işlemi dışarıdan hizmet almak suretiyle temin etmektedir. Bazen de bu durum veri sorumlusunun teknik altyapısının işleme uygun olmaması ve bu nedenle dışarıdan bir hizmet alma konusunda zorunlu olması yani kendisinin gerçekleştirmek istediği işlemi kendi kendine yapamayacak olmasından kaynaklanmaktadır. Toplu SMS örneğinde veri sorumlusu, telefon numaralarına sahip olmakla birlikte bu kişilere toplu SMS gönderebilecek altyapıya sahip değildir. Dolayısıyla burada kendisinin gerçekleştirmeye yetkili bulunduğu bir işlemi dışarıdan bir şirkete yaptırmakta, yani yetkisini aslında veri işleyene

devretmektedir. Nitekim Kişisel Verileri Koruma Kurumu da bir rehberinde⁸¹ veri sorumlusunun veri işleyene bazı yetkilerini devredebileceğini belirtmiştir. Bu yetkilerin özellikle kişisel verilerin toplanması, saklanması, korunması, aktarılması ve imhasına yönelik olduğu söylenebilir.

Veri sorumlusunun veri işleyene bazı yetkilerini devredebilme imkanına sahip olması beraberinde bazı soruları getirmektedir. Acaba veri sorumlusu yetkiyi devretmekle birlikte sorumluluğu da veri işleyene devretmiş olacak mıdır? Hemen belirtmek gerekir ki veri işleyen, veri sorumlusundan aldığı emir ve talimatlar ile hareket etmekte, veri sorumlusunun kendisine çizdiği sınır içerisinde kişisel verileri işlemektedir. Bu nedenle veri sorumlusu bazı yetkileri veri işleyene devretmekle KVKK kapsamındaki sorumluluklarından kurtulmaz.

Öte yandan, veri güvenliğine yönelik ayrık bir durum söz konusudur. Veri güvenliğine ilişkin yükümlülüklerin düzenlendiği KVKK m. 12’de açık bir şekilde, kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi konusunda veri sorumlusu ile veri işleyenin müştereken sorumlu olduğu belirtilmiştir.

Netice itibarıyla veri sorumlusu ile veri işleyen arasında sorumluluğa yönelik bir değerlendirme yapılacağında konunun veri güvenliğine yönelik tedbirlerle mi ilgili olduğu yoksa kanunda düzenlenen diğer hususlarla mı ilgili olduğu tespit edilmeli; şayet veri güvenliğine ilişkin bir durum söz konusu ise müştereken sorumluluğun söz konusu olduğu, diğer durumlarda ise veri sorumlusunun sorumlu olduğu gözetilmelidir.

G-Açık Rıza

Açık rıza, KVKK m. 3/ f. 1, a bendinde “*Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” şeklinde tanımlanmıştır. Tanımdan anlaşılacağı üzere açık rızanın üç unsuru barındırması gereklidir. Açık rıza belirli bir konu özelinde alınmalı, ilgili kişi bu konu hakkında bilgilendirilmeli ve ilgili kişi hiçbir baskı altında kalmadan hür iradesi ile rıza göstermelidir. Açık rızanın unsurlarına detaylı bir şekilde yer vermeden önce tanımın terminolojisine de değinmek gerekmektedir.

⁸¹ Kişisel Verileri Koruma Kurumu, **Veri Sorumlusu ve Veri İşleyen**, s.3, (www.kvkk.gov.tr), (Erişim: 12.07.2023)

Öncelikle belirtmek gerekir ki KVKK’de sadece “açık rıza” kavramı tercih edilmiş olup rıza kavramına yer verilmemiştir. Yukarıda yer alan tanımdan da açıkça anlaşılacağı üzere açık rızadan bahsedebilmek için üç unsurun bir arada bulunması gerekmektedir. Öte yandan kanunun referans alındığı Direktifte ise açık rızanın bir unsuru olarak “tereddüte yer bırakmayacak açıklıkta” ibaresi yer almaktadır.

Bu unsurun KVKK’de belirtilmemesi sebebiyle doktrinde bir görüşün yaklaşımı, kanunda yer alan tanımlamada her ne kadar açık rıza yazsa da bunun açık rızanın değil rızanın tanımı olduğu, bu sebeple açık rıza konusunda örtülü bir boşluk olduğu ve bu boşluğun da TMK’nın 1. maddesi uyarınca hakim tarafından doldurulması gerektiği yönündedir.⁸² Kanaatimizce her ne kadar belirtilen unsura kanunda yer verilmemişse de Kişisel Verileri Koruma Kurumu’nun birçok kararında ve yayınladığı rehberlerde belirtilen şartı zaten aradığı göz önünde bulundurulduğunda aslında kanunda yer alan tanım ile Direktifte yer alan açık rıza tanımının yüksek oranda örtüştüğü kanaatindeyiz. Netice itibarıyla KVKK uyarınca bir açık rızadan bahsedebilmek için alınan açık rıza belirli bir konuya ilişkin olmalı, bilgilendirmeye dayalı olmalı ve en nihayetinde ilgili kişi özgür iradesiyle rızasını açıklamış olmalıdır.

1-Açık Rızanın Unsurları

a-Belirli Bir Konuya İlişkin Olma

Açık rızanın belirli bir konuya ilişkin olması şartı en basit anlatımla ilgili kişinin rıza vereceği alanın sınırlandırılmış olmasını ifade etmektedir. Bir başka anlatım ile genel ve muğlak ifadelerden ziyade açık rıza alınan sürecin tane tane, çok net ve basit bir şekilde ilgili kişinin bilgisine sunulması ve ilgili kişinin de kendisine sunulan çerçeve içerisinde bulunan alana rıza göstermesini ifade etmektedir.

Bu sebeple açık rıza alınacağı zaman, kişisel verinin işleneceği süreçlerin doğru bir şekilde tespit edilmesi ve bu hususların ilgili kişinin bilgisine sunulması gerekmektedir. Buna göre “*kişisel verilerimin işlenmesini onaylıyorum*” veya “*aydınlatma metnini okudum, kişisel verilerin işlenmesini kabul ediyorum*” şeklindeki genel ifadeler, kanunun aradığı açık rıza şartlarını taşımamaktadır.⁸³ Zira burada açık rıza alanının sınırları çizilmemekte aksine çok geniş ve muğlak ifadeler ile ileride oluşabilecek bütün ihtimallerde kişisel verilerin işlenmesinin yolu açılmaya

⁸² Cihan AVCI BRAUN, “**Kişisel Verilerin İşlenmesinde Rıza**”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S.1, 2018, s.19

⁸³ Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 5, (www.kvkk.gov.tr), (Erişim:13.07.2023)

çalışılmaktadır. Dolayısıyla içeriği belirli olmayan, anlaşılamayan, muğlak ifadelerin bulunduğu açık rıza metinleri hukuken geçerli metinler değildir.

Ayrıca Kişisel Verileri Koruma Kurumu tarafından yayınlanan karar ve rehberlerde de kurumun “battaniye rıza” kavramını kullandığı görülmektedir.⁸⁴ Battaniye rıza kavramı ile kastedilen yukarıdaki örnekte yer verdiğimiz şekilde açık rızaya ilişkin süreçlerin muğlak bırakıldığı, genel anlamıyla bütün süreçleri kapsayacak şekilde yuvarlak bir ifade ile rıza alınması işlemi ifade etmektedir. Kişisel Verileri Koruma Kurumu yayınlamış olduğu bir duyuruda da bu şekilde alınan rızaların geçerli olmadığını ifade etmiştir.⁸⁵ Bu noktada akla, birden fazla sürece ilişkin ilgili kişiden açık rıza alınmak isteniyorsa veri sorumlusunun bunu nasıl yapacağı sorusu gelebilir. Burada dikkat edilmesi gereken husus, her bir sürecin ayrı ayrı belirtilmesi ve her süreç özelinde ilgili kişinin kabul etme ve reddetme imkanına sahip olmasıdır.

Başka bir anlatım ile aynı metin içerisinde birden fazla sürecin yer alması ve süreç bazlı olarak ilgili kişinin kabul etme ve reddetme imkanlarına sahip olması halinde battaniye rızadan söz edilemez. Dolayısıyla burada önemli olan, açık rızanın tek bir evrakta talep edilip edilmemesinden ziyade süreç bazında ilgili kişinin kabul etme ve reddetme imkanlarına sahip olup olmadığıdır.

Belirli bir konuya ilişkin olma unsuru açısından akla gelebilecek bir başka soru, açık rıza alınırken süreçlerin belirli olması gerektiğinden acaba veri sorumlusu açık rıza aldığı süreçlerin dışında yeni bir süreçte de rızaya dayalı olarak veri işlemek istediğinde yeniden rıza almak zorunda mıdır? Bu durumda veri sorumlusunun yeniden açık rıza alması gerekecektir. Zira, veri sorumlusunun ilk başta almış olduğu açık rıza, veri sorumlusun yeni uygulayacağı süreci kapsamamaktadır. Dolayısıyla ilk başta çizdiği sınırın dışına çıkmak istediği için bu noktada yeniden açık rıza alması gerekecektir.

b-Bilgilendirmeye Dayalı Olma

KVKK uyarınca usulüne uygun alınmış bir açık rızadan bahsedebilmek için rızayı gösteren ilgili kişi, neye rıza verdiğini bilmelidir. Bunun için de veri

⁸⁴ “İşverenin, işçisine ait kişisel verileri ve özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Karar Özeti

⁸⁵ Kişisel Verileri Koruma Kurumu, **Açık Rıza Alınırken Dikkat Edilecek Hususlar**, (www.kvkk.gov.tr), (Erişim:14.07.2023)

sorumlusunun ilgili kişiyi, neden açık rıza aldığı ve aldığı açık rızayla ilgili kişinin kişisel verileriyle ne yapacağı hususlarında çok sade ve basit bir şekilde bilgilendirmesi gerekmektedir. Ancak bilgiye dayalı olarak verilen bir rıza, açık rıza olarak kabul edilebilecektir. Veri sorumlusu bu bilgilendirmeyi yaparken Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e⁸⁶ uygun hareket etmelidir.

Dikkat edilmesi gereken bir önemli nokta da bu bilgilendirmenin ne zaman yapılacağıdır. KVKK uyarınca geçerli bir bilgilendirmeden bahsedebilmek için bilgilendirme ya kişisel verilerin işlenmesinden önce yapılmalı ya da en geç kişisel verilerin işleneceği anda yapılmalıdır.⁸⁷

Son olarak belirtmek istediğimiz husus, ilgili kişinin sadece açık rıza vereceği konuyla ilgili bilgilendirilmesinin yeterli olmayacağı aynı zamanda ilgili kişinin rıza gösterdiği takdirde neler ile karşılaşacağı konusunda da bilgilendirilmesi gerektiğidir.⁸⁸ Zira rızanın sonuçları ilgili kişiye bildirilmezse sadece açık rızanın belirli bir konuya ilişkin olma şartı gerçekleştirilmiş olacak fakat bilgiye dayalı olma unsuru gerçekleşmemiş olacaktır. Bu da netice itibarıyla alınan açık rızayı sakatlayacaktır.

c-Özgür İradeyle Açıklanmış Olma

Özgür iradeyle açıklanmış olma unsuru, ilgili kişinin açık rıza vereceği husus konusunda veri sorumlusu tarafından bilgilendirilmesi ve neye açık rıza vereceğini öğrenmesi aşamalarından sonra kararını hiçbir baskı altında kalmadan hür iradesiyle vermiş olmasını ifade etmektedir. KVKK uyarınca geçerli bir açık rızadan bahsedebilmek için ilgili kişi, açık rıza beyanını özgür iradesiyle vermelidir. Buradan hareketle ilgili kişinin iradesinin sakatlanmasına sebebiyet verebilecek nitelikte tehdit, hile gibi davranışlar, açık rızayı hukuka aykırı hale getirebilecektir.⁸⁹ Burada gündeme gelebilecek farklı hukuka aykırılık ihtimalleri, her somut olayını özelliğine göre ayrıca değerlendirilmelidir.

Uygulamada çok sık karşılaşılan ve açık rızada özgür irade unsuruna ilişkin en önemli konu, açık rızanın hizmet sunma koşuluna bağlanmasıdır. Bazı veri

⁸⁶ RG., 30356 S., 10.03.2018 T.

⁸⁷ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.4

⁸⁸ Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 6, (www.kvkk.gov.tr), (Erişim:14.07.2023)

⁸⁹ Kişisel Verileri Koruma Kurumu, **Açık Rıza Rehberi**, s. 6, (www.kvkk.gov.tr), (Erişim:14.07.2023)

sorumluları tarafından ilgili kişiden açık rıza alınmakta fakat açık rıza alınırken ilgili kişi rıza göstermediği takdirde hizmetin ilgili kişiye sunulmayacağı yönünde bir izlenim oluşturulmakta ya da hizmet gerçekten de sunulmamaktadır.

Örneğin bir e-ticaret sitesinden alışveriş yapan tüketici, kişisel verilerinin yurtdışına aktarımına ilişkin açık rızaya ilişkin bir onay vermediği takdirde satın alma işlemini gerçekleştiremiyor ise burada açık rıza bir hizmet sunma ön koşuluna bağlanmıştır. Bu şekilde verilecek açık rıza kişinin özgür iradesinden ziyade satın alma işlemini tamamlama gayesi ile verildiğinden ve ilgili kişi üzerinde özgürlüğünü kaldırarak düzeyde bir baskı uygulandığından bu uygulama hukuk aykırıdır. Bu durumda geçerli bir açık rızadan bahsedilemeyecektir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında⁹⁰ açık rıza ile müşterilerinin avuç içi izi verilerini işleyen bir veri sorumlusu hakkında rıza gösterilmediği takdirde veri sorumlusu tarafından sunulan hizmetlerden yararlanamadıkları sebebiyle veri sorumlusu hakkında idari para cezası uygulanmasına karar vermiştir.⁹¹

Öte yandan, bazı durumlarda ise hizmetin açık rıza ile sunulması zorunlu olabilmektedir. Örneğin bir web sitesinin e-bülten aboneliği kısmından yararlanmak isteyen kişi açık rıza göstermek zorundadır. Şayet açık rıza göstermek istemiyor ise bu hizmetten yararlanmama hakkına da sahiptir. Bu gibi durumlarda açık rızanın hizmet şartına bağlanmasından söz edilemez ve ilgili kişi rıza göstermemenin sonucuna katlanması gerekir.⁹² Aksi durumda, veri sorumlusunun açık rıza göstermeyen kişiye de e-bülten aboneliği hizmeti sunması gerekir ki bu durumda da Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik⁹³ hükümlerine aykırılık gerçekleştirmiş olur.

Açık rıza konusuyla ilgili akla gelebilecek bir diğer konu ise çocukların açık rızasıdır. Hemen belirtelim ki KVKK’de bu konuyla ilgili özel bir düzenleme

⁹⁰ Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.07.2023)

⁹¹ Ayrıca spor salonu hizmetli sunan bir veri sorumlusu hakkında da yine Kişisel Verileri Koruma Kurulu tarafından benzer gerekçeyle bir veri sorumlusu hakkında idari para cezası uygulanmasına karar verilmiştir. “Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.07.2023)

⁹² Sinan Sami AKKURT, “Açık Rıza”, iç. Kişisel Verilerin Korunmasına Akademik Bakış – **KVKK Akademi Derleme Çalışması** (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik; Ankara, 2023, s.171

⁹³ RG., 29417 S., 15.07.2015 T.

bulunmamaktadır. Ancak çocukların kişisel verileri çok hassas ve özellik arz eden bir alan olduğu için ve aynı zamanda çocuklar, hukuki ilişkilerin risk ve sonuçlarını tam anlamıyla idrak edemeyeceği için kanunda bu konuyla ilgili özel bir düzenleme yapılması gerektiği kanaatindeyiz.

Açık rıza ve çocuklar arasındaki sorular temel iki noktada toplanmaktadır. Bunlardan birincisi açık rızanın unsurlarından olan bilgilendirmeye dayalı olma unsurunun gerçekleştirilebilmesi amacıyla veri sorumlusunun kimi aydınlatacağına nasıl tespit edileceğidir. Daha basit bir ifade ile veri sorumlusu sadece çocuğu aydınlatmak ile hukuki yükümlülüğünü yerine getirmiş olacak mıdır yoksa veli ya da vasinin de aydınlatılması gerekir mi? Bir diğer nokta ise KVKK'de açıkça düzenlenmediği için açık rızayı verme yetkisinin kime ait olduğu problemidir.

Yukarıda da belirttiğimiz üzere çocuğun kişisel verilerinin işlenmesi KVKK'de özel olarak düzenlenmediğinden çocuğun rızasına ilişkin sorulara cevap verebilmek adına genel hüküm olan TMK hükümlerine bakmak gerekir.

İlk değerlendirilmesi gereken husus, kişisel verilerin işlenmesine açık rıza gösterilmesinin hukuki durumudur. Açık rıza gösterilmesi, kişiye sıkı sıkıya bağlı olan bir hakkın kullanılmasıdır. Kanunumuzda kişiye sıkı sıkıya bağlı hakların bir listesi yer almamakla birlikte bu kategoride yer alan hakların tespiti açısından iki önemli kriter bulunmaktadır. Bunlar, hakkın sahibinden ayrılmaz olması ve hakkın malvarlığına ilişkin olmamasıdır. Açık rıza gösterilmesi de kural olarak yalnızca ilgili kişi tarafından kullanılabilecek bir hak olduğundan ve malvarlığına ilişkin olmadığından şahsa sıkı sıkıya bağlı bir haktır. Buradan hareketle, aşağıda yer vereceğimiz bütün açıklamalar, açık rızanın şahsa sıkı sıkıya bağlı hak olmasının sonuçları üzerinden şahsi ve doktrinsel değerlendirmelerimizi içermektedir. Yeri gelmişken belirtmekte fayda var ki Kişisel Verileri Koruma Kurumu da bir kamuoyu duyurusunda⁹⁴ açık rıza verilmesinin kişiye sıkı sıkıya bağlı bir hak olduğunu ifade etmiştir.

Şahsa sıkı sıkıya bağlı hakları farklı açılardan çeşitlere ayırmak mümkündür. Bunlardan birisi de mutlak anlamda kişiye sıkı sıkıya bağlı haklar ve nispi anlamda kişiye sıkı sıkıya bağlı haklardır. Mutlak anlamda şahsa sıkı sıkıya bağlı olan hakların

⁹⁴ Kişisel Verileri Koruma Kurumu, Whatsapp Uygulaması Hakkında Kamuoyu Duyurusu, (www.kvkk.gov.tr), (Erişim: 15.07.2023)

temsilci tarafından kullanılması mümkün değildir ancak hak sahibi bu hakkı kullanabilmektedir. Öte yandan yasal temsil veya iradi temsil yoluyla kullanılabilen haklar ise nispi anlamda kişiye sıkı sıkıya bağlı haklardır.⁹⁵

Hareket noktamız olan iki soruya cevap verebilmek için önce küçüğün ehliyet durumunun tespiti gerekir. TMK m. 14 aynen “*Ayırt etme gücü bulunmayanların, küçüklerin ve kısıtlıların fiil ehliyeti yoktur.*” şeklindedir. Küçükler, fiil ehliyetine göre kategorilere ayrıldığında şayet ayırt etme gücüne sahipse sınırlı ehliyetsiz, ayırt etme gücü yok ise tam ehliyetsizdir.

Ardından, ayırt etme gücünü tespit etmek gerekmektedir. Zira TMK bu tespiti bir sonuç bağlamaktadır. TMK m. 16 aynen “*Ayırt etme gücüne sahip küçükler ve kısıtlılar, yasal temsilcilerinin rızası olmadıkça, kendi işlemleriyle borç altına giremezler. Karşılıksız kazanmada ve kişiye sıkı sıkıya bağlı hakları kullanmada bu rıza gerekli değildir.*” şeklindedir. Buna göre ayırt etme gücüne sahip küçük, kişiye sıkı sıkıya bağlı haklarından birisini kullanmak istediğinde yasal temsilcisinin rızasına ihtiyaç duymamaktadır. Yani en basit anlatım ile açık rıza gösterecek olan çocuk eğer ayırt etme gücüne sahipse tek başına vereceği açık rıza geçerlidir. Hemen belirtmek gerekir ki çocuğun ayırt etme gücüne sahip olup olmadığı, her somut olayın özelliğine göre rızanın önem seviyesi, çocuğun yaşı, çocuğun gelişim durumu gibi kriterler uyarınca ayrıca değerlendirilmelidir.⁹⁶ Kanaatimizce bu değerlendirmede, çocuk neye rıza gösterdiğini anlayabilecek durumda olmalı, çocuk açık rıza göstermesi halinde ne gibi sonuçlar ile karşılaşabileceğini idrak edebilmeli, çocuk rıza göstermesi halinde oluşabilecek riskleri en azından kafasında tasarlayabilecek kadar yetişkinlik düzeyine ulaşmış durumda olmalıdır.

Netice itibariyle çocuğun ayırt etme gücüne sahip olduğu durumlarda sorunun cevabı son derece basittir. Çocuğun tek başına aydınlatılması yeterlidir ve çocuğun tek başına göstereceği açık rıza, diğer koşulları sağlamak kaydıyla geçerlidir. Asıl problemli nokta ayırt etme gücüne sahip olmayan küçüğün rızası hususudur. Burada da tam ehliyetsizlerin kişiye sıkı sıkıya bağlı olan haklar bakımından temsili sorunu gündeme gelmektedir.

⁹⁵ M. Kemal OĞUZMAN-Özer SELİÇİ-Saibe OKTAY ÖZDEMİR, **Kişiler Hukuku**, 14. Bası, İstanbul, Filiz Kitabevi, Ekim 2014, s. 98

⁹⁶ Mustafa DURAL, Tufan ÖĞÜZ, **Türk Özel Hukuku**, C. II, Kişiler Hukuku, 12. Bası, İstanbul, 2012, s. 60; OĞUZMAN/SELİÇİ/OKTAY-ÖZDEMİR, a.g.e., s. 55

Tam ehliyetsizlerin kişiye sıkı sıkıya bağlı olan haklar açısından temsil edilmesi durumu özellik arz eden bir husustur. Kural olarak, kişiye sıkı sıkıya bağlı olan hakların bizzat hak sahibi tarafından kullanılması gerektiği ve bu nedenle de yasal temsilcinin kişiye sıkı sıkıya bağlı olan bir hakkı kullanmasının mümkün olmadığı kabul edilmektedir.⁹⁷

Öte yandan doktrinde, bu kuralın mutlak suretle uygulanması halinde tam ehliyetsizin saygınlığının zedelenebileceği veya korunma ihtiyacının karşılanamayabileceği belirtilmektedir.⁹⁸ Hatta doktrinde, mutlak anlamda kişiye sıkı sıkıya bağlı hakların çok geniş bir çerçevede ele alınması tam ehliyetsizi neredeyse hak ehliyetinden yoksun duruma düşüreceğinden, aksine hüküm olmadıkça kişiye sıkı sıkıya bağlı hakların yasal temsilci tarafından kullanılabilmesi ifade edilmektedir.⁹⁹ Bu sebeple de mutlak anlamda kişiye sıkı sıkıya bağlı haklar ve nispi anlamda kişiye sıkı sıkıya bağlı haklar olarak ikili bir ayrıma gidilmektedir. Buradan hareketle kanaatimizce, ayırt etme gücüne sahip olmayan bir çocuğun yasal temsilcisi, çocuğun üstün yararına ve menfaatlerine aykırı düşmediği müddetçe çocuk adına açık rıza verme yetkisine sahiptir.¹⁰⁰ Zira aksinin kabulü halinde çocuğun üstün yararına dahi olsa yasal temsilcinin rıza gösteremeyeceğinin kabulü gerekir ki hukukumuzda temel olan çocuğun gelişimi, çocuğun üstün yararının gözetilmesine ilkeleri ile bu yaklaşım örtüşmemektedir.

İlaveten, ayırt etme gücüne sahip olmayan çocuk açısından açık rıza verme yetkisi kanaatimizce yasal temsilci tarafından kullanılabilmesinden aydınlatmanın da çocuk adına ve fakat yasal temsilciye yapılması gerekli ve yeterlidir. Çocuk zaten ayırt etme gücüne sahip olmadığından ayrıca aydınlatılmasına gerek bulunmadığı

⁹⁷ M. Kemal OĞUZMAN, Nami BARLAS, **Medeni Hukuk Dersleri**, İstanbul, 2011, s. 161 vd.

⁹⁸ Ergun ÖZSUNAY, **Gerçek Kişilerin Hukuki Durumu**, İstanbul, 1979, s. 59; DURAL/ÖĞÜZ, a.g.e., s.79; OĞUZMAN/SELİÇİ/OKTAY-ÖZDEMİR, a.g.e., s. 83

⁹⁹ Abdulkadir ARPACI, **Kişiler Hukuku (Gerçek Kişiler)**, 2. Bası, İstanbul, 2000, s. 52-54; Jale G. AKİPEK/ Turgut AKINTÜRK, Derya ATEŞ KARAMAN, **Türk Medeni Hukuku, Başlangıç Hükümleri, Kişiler Hukuku**, C. I, 8. Bası, İstanbul, 2011, s. 316 vd.; Aydın ZEVKLİLER/ Mehmet Beşir ACABEY/ K. Emre GÖKYAYLA, **Medeni Hukuk (Giriş-Başlangıç Hükümleri-Kişiler Hukuku-Aile Hukuku)**, Ankara, 2000, s. 327

¹⁰⁰ Konuya ilişkin farklı yaklaşımlar söz konusudur. Çocuk ve yasal temsilcinin birlikte rıza göstermesi gerektiğine ilişkin görüş için: Erdoğan, C. (2019). Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında). **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, 21(Özel Sayı); Yasal temsilcinin çocuk hakkında tek başına rıza göstermeye yetkili olduğu, öte yandan veri sorumlusunun hem çocuğu hem de yasal temsilciyi aydınlatması gerektiğine ilişkin görüş için: Murat UÇAK., **Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası, Kişisel Verileri Koruma Dergisi**, 2020, 3. Cilt, 1. Sayı; aynı doğrultuda DÜLGER, a.g.e., s. 232

kanaatindeyiz. Nitekim bir bölge adliye mahkemesi kararında¹⁰¹ 2 yaşındaki bir kız çocuğunun fotoğraflarının paylaşılabilmesi için anneanneden alınan iznin geçersiz olduğu ve anne babadan izin alınması gerektiği belirtilmiştir.

Son olarak belirtmek gerekir ki açık rıza, çalışmamız kapsamında bir hukuka uygunluk nedeni de olduğundan açık rızanın geri alınması,¹⁰² açık rıza karşılığında ek avantaj sunulup sunulamayacağı¹⁰³ ve gerekmediği halde açık rıza alınması¹⁰⁴ durumunda ne olacağı, çalışmamızın ilgili kısımlarında detaylıca ele alınacaktır.

H-Veri Sorumluları Sicili (VERBİS)

Veri sorumluları siciline ilişkin bir tanım KVKK'de yer almamaktadır. Bununla birlikte, “*Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.*” şeklindeki KVKK m. 16/ f. 1 hükmü ile Kişisel Verileri Koruma Kurulu tarafından bir sicil tutulacağı düzenlenmiş ve aynı maddenin beşinci fıkrasında yer alan “*Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.*” hükmü ile sicile ilişkin detayların yönetmelikte yer alacağı ifade edilmiştir.

Bu kapsamda, Veri Sorumluları Sicili Hakkında Yönetmelik, 30286 sayılı ve 30.12.2017 tarihli Resmi Gazete’de yayımlanmıştır. Yönetmeliğin tanımlar üst başlığını taşıyan 4. maddesinin birinci fıkrasının o bendinde VERBİS, “*Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi*” şeklinde tanımlanmıştır.

VERBİS, kural olarak tüm veri sorumlularının veri işleme faaliyetine başlamadan önce kaydolması gereken, kamuya açık olan, dijital ortamda tutulan bir sicildir. Çalışmamızın yazım tarihi itibarıyla VERBİS’te yedi kategori bulunmaktadır. Bunlar veri sorumlusunun hangi kişisel veriler kategorisinde veri işlediği bilgisi, kişisel verilerin işleme amaçları, kişisel verilerin aktarımında alıcı grupları, kişisel verilerin ne kadar süre ile işlendiği, kimlerin kişisel verilerinin işlendiği, yurtdışına veri aktarımı yapılıp yapılmadığı ve kişisel verilerin güvenliği için hangi idari ve teknik tedbirlerin alındığı bilgisidir. Sicilin dijital ortamda kamuya açık bir şekilde

¹⁰¹ Antalya BAM, 11. HD., 2017/224 E., 2017/237 K., 23.03.2017 T.

¹⁰² Bkz: s. 59

¹⁰³ Bkz: s. 62

¹⁰⁴ Bkz: s. 60

tutulması sayesinde verisi işlenen ilgili kişi, veri sorumlusunun KVKK kapsamındaki faaliyetlerini yukarıda yer alan yedi kategori kapsamında inceleyebilme imkanına sahiptir.¹⁰⁵

VERBİS'e kayıt yükümlülüğü, veri sorumlusunun yükümlülüklerinden birisi olduğundan bu bölümde sadece tanım ile yetineceğiz. Kayıt yükümlülüğü ve konuya ilişkin eleştirilerimize ilgili başlık altında¹⁰⁶ yer verilecektir.

I-Kişisel Verilerin İmhası

Kişisel verilerin imhasına ilişkin bir tanım KVKK'de yer almamaktadır. Öte yandan, 30224 sayılı ve 28.10.2017 tarihli Resmi Gazete'de yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 4/ f. 1/ c bendinde imhanın tanımı "*Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi*" şeklinde yapılmıştır.

Maddeden açıkça anlaşılacağı üzere belirtilen faaliyetlerin her biri, kişisel verilerin imhası için sunulmuş bir yöntemdir. Başka bir anlatımla, bir veri sorumlusu kişisel veri imha etmek istediğinde bunu imha etmek istediği veriyi anonimleştirerek yapabilir, yok ederek yapabilir veya silerek yapabilir. Tercih hakkı veri sorumlusuna aittir.

1-Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, KVKK m. 3/ f. 1/ b bendinde ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 10/ f. 1'de "*Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*" şeklinde tanımlanmıştır.

Bir kişisel verinin anonim hale getirildiğinden bahsedebilmek için kimliği belirli veya belirlenebilir bir kişiye ulaşılamaması gerekmektedir. Bu kapsamda veri sorumlusu ve veri sorumlusunun veriyi aktardığı alıcı grupları, veriyi geri döndürmeye çalışsa bile, farklı yöntemler deneseler ve hatta veriyi, ellerindeki başka veriler ile

¹⁰⁵ Kişisel Verileri Koruma Kurumu, **Veri Sorumluları Sicili Rehberi**, s. 7 (www.kvkk.gov.tr), (Erişim: 16.07.2023)

¹⁰⁶ Bkz: s. 105 vd.

eşleştirmeyi deneseler bile kimliği belirli veya belirlenebilir bir kişiye ulaşamamalıdır.¹⁰⁷

Kişisel verilerin anonim hale getirilmesi bir veri imha yöntemi olduğundan ve kişisel verilerin imhası da veri sorumlusunun yükümlülükleri arasında yer aldığından veri sorumlusunun anonim hale getirme işlemini nasıl yapması gerektiği çalışmanın ilerleyen kısımlarında¹⁰⁸ detaylıca açıklanacaktır.

2-Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 8/ f. 1’de aynen “Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.” şeklinde tanımlanmıştır.

Kişisel verilerin silinmesinden bahsedebilmek için öncelikle kişisel verinin erişilemez ve tekrar kullanılamaz hale getirilmesi gerekir. Tekrar kullanılamaz ve erişilemez olma olgusunun ilgili kullanıcılar açısından gerçekleşmesi gerekmektedir. Zira birazdan açıklayacağımız üzere¹⁰⁹ bu olgunun ilgili kullanıcı değil de herkes tarafından gerçekleşmesi halinde silinmeden değil yok etmeden bahsedilir. Bu nedenle kişisel verilerin silinmesi için ilgili kullanıcı veriye hiçbir şekilde erişememeli ve veriyi tekrar kullanamamalıdır.

Kişisel verilerin silinmesine yönelik hangi yöntemin tercih edileceği veri sorumlusunun takdirindedir. Belirtmekte fayda var ki silinecek olan kişisel verinin dijital ortamda bulunması ile fiziki ortamda bulunması farklılık arz ettiğinden silme yöntemi de farklılık arz edecektir.¹¹⁰ Kişisel verilerin silinmesi bir veri imha yöntemi olduğundan ve kişisel verilerin imhası da veri sorumlusunun yükümlülükleri arasında yer aldığından veri sorumlusunun silme işlemini nasıl yapması gerektiği çalışmanın ilerleyen kısımlarında detaylıca¹¹¹ açıklanacaktır.

¹⁰⁷ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 10/ f. 2 aynen “Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.” şeklindedir.

¹⁰⁸ Bkz: s. 148 vd.

¹⁰⁹ Bkz: s. 44

¹¹⁰ CANBAY, s. 321

¹¹¹ Bkz: s. 147 vd.

3-Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 9/ f. 1’de aynen “*Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.*” şeklinde tanımlanmıştır.

Kişisel verilerin yok edilmesinden bahsedebilmek için öncelikle kişisel verinin erişilemez ve tekrar kullanılamaz hale getirilmesi gerekir. Tekrar kullanılamaz ve erişilemez olma olgusunun yukarıda anlattığımız silmeden farklı olarak yalnız ilgili kişi nezdinde değil herkes tarafından gerçekleşmesi gerekmektedir.

Kanun koyucu, kişisel verilerin yok edilmesi için herhangi bir yöntem zorunluluğu getirmemiştir. Kişisel verilerin nasıl yok edileceğinin takdiri veri sorumlusuna aittir. Nitekim Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 9/ f. 2 aynen “*Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*” şeklindedir.

Kişisel verilerin yok edilmesi, bir veri imha yöntemi olduğundan ve kişisel verilerin imhası da veri sorumlusunun yükümlülükleri arasında yer aldığından veri sorumlusunun yok etme işlemini nasıl yapması gerektiği çalışmanın ilerleyen kısımlarında¹¹² detaylıca açıklanacaktır.

II-KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

Kişisel verilerin işlenmesine ilişkin temel ilkeler, kişisel verilerin korunması hukukunu düzenleyen birçok kaynakta yer alan bir husustur.¹¹³ Bu ilkelerin KVKK’de düzenlenmiş olması bizler için son derece önemlidir. Zira, birazdan detaylıca anlatılacak olan ilkeler hem kanun koyucunun kişisel verilerin korunması hukukuna bakış açısını göstermekte hem de Kişisel Verileri Koruma Kurumu’na, önüne gelen uyumsuzluklarda temel kontrol noktalarını göstermektedir.

¹¹² Bkz: s. 148

¹¹³ 108 Sayılı Sözleşmenin “Verilerin Niteliği” üst başlığını taşıyan 5. maddesi; Direktifin “Veri Kalitesine İlişkin Prensipler” üst başlığını taşıyan 6. maddesi ve en GDPR’ın “Kişisel Verilerin İşlenmesine İlişkin İlkeler” üst başlığını taşıyan 5. maddesi kişisel verilerin korunmasına ilişkin uyulması zorunlu olan temel ilkeleri düzenlemektedir.

KVKK kapsamında, genel ilkeler üst başlığını taşıyan dördüncü maddede, beş adet ilkeye yer verilmiştir. Bunlar hukuka ve dürüstlük kurallarına uygun olma; doğru ve gerektiğinde güncel olma; belirli, açık ve meşru amaçlar için işlenme; işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkeleridir. Çalışmamızın bu bölümünde, belirtilen ilkeleri detaylıca izah edeceğiz.

A-Hukuka ve Dürüstlük Kuralına Uygun Olma

Hukuka ve dürüstlük kuralına uygun olma ilkesi çok geniş kapsamlı bir ilkedir. İlke neredeyse KVKK’de sayılan diğer ilkeleri de içine alacak niteliktedir. Çoğu durumda diğer ilkelerden birisine aykırılık söz konusu ise hukuka ve dürüstlük kuralına uygun olma ilkesine de aykırılık olma ihtimali muhtemeldir.

Kişisel verilerin işlenmesinde hukuka uygunluk olarak kastedilen, öncelikle konuyla ilgili özel düzenleme olan KVKK’de yer alan genel ilkelere uygun hareket edilmesi ve KVKK’de düzenlenen kişisel verilerin işlenme şartlarına dayanılmasıdır. Bununla birlikte diğer kanunlarda da kişisel verilerin işlenmesiyle ilgili bazı düzenlemeler yer aldığından, bu düzenlemelere de riayet edilmesi gerekmektedir. Dolayısıyla hukuka uygunluğu salt KVKK ile sınırlandırmamak gerekir.

Dürüstlük kuralına uygun olma ilkesi ise temelinde veri sorumlusunun, ilgili kişinin çıkarlarına uygun olacak şekilde ve yine ilgili kişinin makul beklentilerini karşılayacak şekilde faaliyetlerini yürütmesini ifade etmektedir.¹¹⁴ Burada özellikle dürüstlük ilkesi ile şeffaflık arasında bir bağlantı söz konusudur.¹¹⁵ Zira kanun koyucu veri sorumlusundan, kişisel verileri işleyeceği süreçte başta ilgili kişiye karşı olmak üzere şeffaf davranmasını, açık olmasını, dürüst davranmasını beklemektedir.¹¹⁶ Bu ilkeye aykırılık özellikle veri sorumlusunun bazı kişisel veri işlediği süreçleri ilgili kişiden saklaması şeklinde karşımıza çıkabilir. Örneğin kişisel verilerin yurt dışına aktarılmasında, konunun barındırdığı risk nedeniyle veri sorumlusunun yurt dışına veri

¹¹⁴ Nafiye YÜCEDAĞ “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, iç. Kişisel Verilerin Korunmasına Akademik Bakış – **KVKK Akademi Derleme Çalışması** (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik; Ankara, 2023, s.138; Mesut Serdar ÇEKİN, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, İstanbul, On İki Levha Yayıncılık, 2020, s. 70; Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları No 1, Ankara, Aralık 2019, s. 64, (www.kvkk.gov.tr), (Erişim: 05.08.2023)

¹¹⁵ DEVELİOĞLU, s. 45

¹¹⁶ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları No 1, Ankara, Aralık 2019, s. 64, (www.kvkk.gov.tr), (Erişim: 16.07.2023)

aktardığı halde aydınlatma metinlerinde buna yer vermemesi bu kapsamda değerlendirilebilir.

Doktrinde dürüstlük kuralına uygun davranma ilkesinin kapsamına ilişkin farklı görüşler söz konusudur. Doktrinde, Kişisel Verileri Koruma Kurumu'nun da esas aldığı¹¹⁷ hâkim fikir, ilgili ilkenin TMK m. 2'de düzenlenen dürüstlük kuralının farklı bir görünümü olduğu şeklindedir.¹¹⁸

Bir başka görüşe göre ise ilgili ilkeyle kastedilenin hâkim olan görüş ile tam anlamıyla aynı manaya gelmediği, burada kastedilenin veri sorumlusunun KVKK'den doğan haklarını adil bir şekilde kullanması gerektiği yönündedir.¹¹⁹

Bir başka görüş ise ilgili ilkenin adil olma kavramından da geniş bir alanı kapsadığı yönündedir.¹²⁰ Biz de hâkim olan görüşe katılmaktayız. Kanaatimizce KVKK'de yer alan dürüstlük kuralının temelinde veri sorumlusunun ilgili kişiyi yanıltmaması, veri sorumlusunun KVKK'de yer alan haklarını kötüye kullanmaması ve en nihayetinde veri sorumlusunun ilgili kişinin çıkarlarını gözeterek ve makul beklentilerini karşılayacak şekilde hareket etmesi yer almaktadır. TMK m. 2'nin görünümü ise hakların kullanılırken kötüye kullanılmaması, borçlar ifa edilirken dürüst davranılması, hukuki işlemlerde ise tarafların karşılıklı makul beklentilerinin karşılanması ve tarafların birbirini aldatmaması şeklinde karşımıza çıkmaktadır. Bu nedenle KVKK'de yer alan dürüstlük ilkesiyle TMK m. 2'de düzenlenen dürüst davranma ilkesinin örtüştüğü, ilgili ilkenin KVKK'ye yansımaları olduğu ayrıca, *“Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.”* şeklindeki KVKK m. 4/ f. 1 hükmü gereğince bağlamın sadece KVKK ile sınırlı tutulmaması gerektiği, nitekim KVKK'de bile diğer kanunlarda öngörülen usul ve esaslara atıfta bulunulduğu gerekçesiyle daha kapsayıcı olacak şekilde alınması gerektiği kanaatindeyiz.

¹¹⁷ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019, Ankara, s. 14, (www.kvkk.gov.tr), (Erişim: 16.07.2023)

¹¹⁸ Hayrunnisa ÖZDEMİR, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara: Seçkin, 2009, s. 138; Furkan Güven TAŞTAN, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, İstanbul, On İki Levha Yayıncılık, s. 48; DÜLGER, a.g.e., s. 111; YÜCEDAĞ, a.g.e., s. 137

¹¹⁹ ÇEKİN, a.g.e., s. 70; YÜCEDAĞ, a.g.e., s. 137

¹²⁰ BAŞALP, a.g.e., s. 37

B-Doğru ve Gerekliğinde Güncel Olma

Doğru ve gerektiğinde güncel olma ilkesi aslında iki ayrı unsuru ihtiva etmektedir. Veri sorumlusu tarafından işlenen kişisel veriler doğru olmalıdır. Aynı zamanda bu kişisel veriler şayet gerekli ise güncel olmalıdır. Bu ilkenin daha iyi anlaşılabilmesi için doğru verinin ve güncel verinin ne olduğunun açıklanması gerekmektedir.

Doğru veri, gerçek duruma uygun olan veri olarak tanımlanabilir. Buradan hareketle doğru olma ilkesi ile kanun koyucunun düzenlemek istediği husus, veri sorumlusu tarafından kişisel verilerin elde edilmesinden başlanarak gerçekleşen süreçte kişisel verinin gerçek duruma uygun olmasıdır.

Kişisel Verileri Koruma Kurulu vermiş olduğu güncel tarihli bir kararında veri sorumlusu olan GSM operatörünün, müşterisi olan ilgili kişinin ortağı olduğu şirketin kurumsal telefon numaralarını, ilgili kişinin bireysel iletişim numaralarıymış gibi işleme faaliyetini, doğru ve gerektiğinde güncel olma ilkesine aykırılık olarak değerlendirmiştir.¹²¹

Doktrinde, kural olarak veri sorumlusunun veriyi sürekli olarak güncel ve doğru tutma yükümlülüğü altında bulunmadığı ve bu nedenle de gerekmediği sürece veri sorumlusunun düzenli bir şekilde ilgili kişinin verilerinin güncel durum ile farklılık arz edip arz etmediğini araştırması şeklinde bir yükümlülüğü olmadığı ifade edilmektedir.¹²² Bununla birlikte, veri sorumlusunun ilk defa kişisel veri elde ettiği anda, ilgili verinin doğruluğunu teyit amacıyla farklı yöntemler belirlemesinin ve gerekli tedbirleri almasının ilkeye uygunluk açısından faydalı olacağı kanaatindeyiz.

¹²¹ “İlgili kişinin borç bilgisinin ortağı olduğu şirketin kurumsal numaralarına kısa mesaj olarak gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/78 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 17.07.2023), Kararın ilgili kısmı aynen “İlgili kişinin ortağı olduğu Şirkete ait kurumsal iletişim numaralarının, veri sorumlusu ile arasındaki bireysel sözleşmelerde de iletişim numarası olarak kullanılmasının veri sorumlusu tarafından Kanun’un 4’üncü maddesinde yer alan Genel İlkelerden “doğru ve gerektiğinde güncel” olma ilkesine aykırılık teşkil ettiği anlaşılmış olup, bu hukuka aykırı veri işleme faaliyeti nedeniyle avukatlık ortaklığı tarafından ilgili kişiye ilişkin kişisel verileri içeren kısa mesajların şirkete ait iletişim numaralarına gönderilmesi neticesinde, borca konu işlemle ilgisi olmayan üçüncü kişi şirket çalışanları ile ilgili kişiye ilişkin kişisel veri olan borç bilgisinin Kanun’un 5’inci maddesinde yer alan herhangi bir işleme şartı bulunmaksızın paylaşıldığı gözetildiğinde; Kanun’un 12’nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülüklerini yerine getirmediği kanaatine varılan veri sorumlusu hakkında Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 85.000 TL idari para cezası uygulanmasına” şeklindedir.

¹²² Selen UNCULAR, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Ankara, Seçkin Yayıncılık, 2014, s. 63; KÜZECİ, s. 21; YÜCEDAĞ, a.g.e., s. 141

Son olarak belirtmek gerekir ki uygulamada sıklıkla veri sorumlusunun, ilgili kişilerin verilerini sehven veya özensizlikten doğru olmayan kişiyle paylaşması durumuyla karşılaşılmaktadır. Veri sorumlularının bu durumu özellikle kontrol etmesi gerekmekte ve işlediği kişisel verileri, veriye teması olmaması gereken kişiler ile paylaşmaması veya onların erişimine sunmaması gerekmektedir. Nitekim Kişisel Verileri Koruma Kurulu konuyla ilgili bir kararında üçüncü bir kişiye ait faturanın, fatura sahibi olmayan başka bir kişiye e-posta gönderilmesi olayında, ilgili kişinin e-posta adresinin işlenmesinin doğru ve gerektiğinde güncel olma ilkesine aykırılık teşkil ettiğini ifade etmiştir.¹²³

C-Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Kişisel verilerin işlenmesinde uyulması gereken zorunlu ilkelerden birisi olan belirli, açık ve meşru amaçlar için işlenme ilkesi bünyesinde üç unsuru ihtiva etmektedir.

Bunlardan birincisi, kişisel verilerin belirli amaçlar için işlenmesi gerektiğidir. Belirli amaç ibaresi ile hedeflenen, veri sorumlusu tarafından gerçekleştirilecek olan veri işleme faaliyetinin sınırının çizilmesini sağlamaktır.

Bir başka anlatımla, bu ilkeye uyan veri sorumlusu aslında kişisel verileri ne gerekçe ile işleyeceğinin bir çerçevesini çizmektedir. Çizdiği çerçevenin, gerçekleştirdiği veri işleme faaliyetine uygunluğu ise aynı zamanda kişisel verilerin hukuka ve dürüstlük kuralına uygun olmasıyla da ilgilidir. Zira veri sorumlusu şayet belirlediği amaçların dışına çıkarsa hem belirli açık ve meşru amaçları için işlenme ilkesine aykırı hareket etmiş olur çünkü kendi çizdiği sınırın dışına çıkmaktadır hem de dürüstlük ilkesine aykırı hareket etmiş olur zira ilgili kişi bu işleme faaliyeti ile ilgili bilgi sahibi değildir ve aslında daha dar bir kapsamda verisinin işleneceğini düşünmektedir. Nitekim Kişisel Verileri Koruma Kurulu vermiş olduğu bir kararda, veri sorumlusunun aydınlatma metninde karara konu faaliyetiyle ilgili, ilgili kişiyi

¹²³ “İlgili kişinin e-posta adresine başka abonelere ait e-faturaların gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/925 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.07.2023) Kararın ilgili kısmı aynen “İlgili kişinin e-posta adresinin üçüncü kişilere ait faturanın iletilmesi suretiyle işlenmesi ve bu durumun Kanun’un 4 üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer alan “doğru ve gerektiğinde güncel olma” ilkesine aykırılık teşkil etmesi sebebiyle Kanun’un 12’nci maddesinin (1) numaralı fıkrasındaki yükümlülükleri yerine getirmede kanaatine varılan veri sorumlusu hakkında, daha önce verilen Kurul Kararında abonelerin kişisel verilerinin güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınması hususunda talimatlandırıldığı da dikkate alınarak, Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına,” şeklindedir.

bilgilendirmemesini, asıl amacının ne olduğunu açıklamamasını, öncelikle hukuka ve dürüstlük kuralına uygun olma ilkesine akabinde belirli açık meşru amaçla işleme ilkesine aykırılık olarak değerlendirmiştir.¹²⁴

İlkede yer alan bir diğer unsur ise meşru amaçlar unsurudur. Meşru amaç unsuru ile kastedilen en yalın anlatım ile hukuka uygunluktur. Yani veri işleme faaliyeti KVKK’de belirtilen kişisel verilerin işlenmesi şartlarından birisine dayanmalı ve aynı zamanda KVKK dışındaki diğer mevzuatla da uyumlu olmalıdır.

Üçüncü unsur ise açık amaçlar unsurudur. Açık amaçlar ibaresi ile hedeflenen, veri sorumlusunun gerçekleştireceği veri işleme faaliyetine gerekçe teşkil eden konunun yuvarlak ve muğlak olmayan ifadeler ile son derece açık, basit ve anlaşılabilir bir dille başta ilgili kişinin aydınlatılmasını sağlamak, akabinde veri koruma otoriteleri, veri işleyen gibi üçüncü kişilerin de veri işlemenin amacını rahatlıkla anlamasını sağlamaktır.

Uygulamada sıklıkla gördüğümüz üzere veri sorumluları tarafından hazırlanan aydınlatma metinlerinde veri işleme faaliyetine gerekçe teşkil eden süreçler anlatılırken bazı cümlelerin sonunda “gibi süreçler” veya “insan kaynakları süreçleri” gibi ifadeler yer verildiği görülmektedir. Anılan ilke uyarınca kişisel verilerin işlenmesinde veri sorumlusu tarafından bir çerçeve çizilmesi gerektiği, bu çerçevenin ilgili kişi tarafından açık bir şekilde anlaşılabilir olması gerektiği ve veri işleme faaliyetinin de bir meşru dayanağının olması gerektiği için örnekte yer verilen yuvarlak ifadelerin kullanılması veya detay verilmeden muğlak bir şekilde atıf yapılması, anılan ilke ile örtüşmemektedir.¹²⁵

¹²⁴ “Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler hakkında” Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/65 sayılı karar özetinin ilgili kısmı aynen “*Bu durumda, müşterilerin puanlanmasına dayanan veri işleme faaliyetinin Kanunun 4 maddesinde belirtilen kişisel verilerin işlenmesine ilişkin genel ilkelerden ilk olarak “Hukuka ve Dürüstlük Kurallarına Uygun Olma” ilkesine aykırılık teşkil ettiği, zira veri sorumlusunun sözü geçen kişisel veri işleme faaliyetine ilişkin olarak ilgili kişi ile hiçbir bilgi paylaşmadığı, konu “Belirli, Açık ve Meşru Amaçlar İçin İşlenme” ilkesi bakımından değerlendirildiğinde, veri sorumlusunun aydınlatma metninde ve kullanım koşullarına ilişkin metinde belirtilen amaçların müşterilerin puanlanmasına dayanan kişisel veri işleme faaliyetinin asıl amacının ne olduğunu açıklayamadığı*” şeklindedir.

¹²⁵ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 9, (www.kvkk.gov.tr), (Erişim: 20.07.2023)

Son olarak ilkeyle ilgili değinmek istediğimiz husus ise veri sorumlusu tarafından kişisel verinin elde edilmesi anındaki amaç ile daha sonrasında verinin işlenmesi sürecinde amacın ve sürecin değişiklik göstermesi durumudur.

Veri sorumlusu tarafından bir kişisel verinin ilk elde edilmesi anındaki gayesi, toplama amacıdır.¹²⁶ Veri, veri sorumlusu tarafından elde edildikten sonra, veri sorumlusunun veri üzerinde gerçekleştirdiği her türlü faaliyet ise sonraki işleme amacıdır.¹²⁷ Konuyla ilgili Kişisel Verileri Koruma Kurulu’nun bir kararı da son derece aydınlatıcıdır.¹²⁸ Kararda, veri sorumlusunun veriyi ilk elde ettiğinden farklı bir amaçla işlemek istediği takdirde ortaya yeni bir veri işleme faaliyeti çıktığı, bu nedenle de bu faaliyetin genel ilkelere ve veri işleme şartlarına uygun olması gerektiği ve bu noktada ilgili kişiye aydınlatma yapılması gerektiği ifade edilmiştir. Aksi durumda veri sorumlusu, diğer ihlallerle birlikte kişisel verilerin belirli, meşru ve açık amaçlarla işlenme ilkesini de ihlal etmiş olacaktır. Zira yeni süreçle ilgili hem ilgili kişi aydınlatılmamaktadır yani ilk başta belirlenen çerçevenin dışına çıkmıştır hem de KVKK’de sayılan veri işleme şartlarından birisine dayanılmamıştır.

Netice itibariyle veri sorumlularının kişisel veri işlemekteki amaçları ve süreçleri değiştiğinde buna ilişkin gerekli adımları atması gerekmektedir.¹²⁹ Her veri sorumlusunun veriyi ilk elde ettiği andaki amacıyla sonraki amacı arasında fark

¹²⁶ Article 29 Data Protection Working Party, No 203 (2013), Opinion 03/2013 on purpose limitation, s. 230

¹²⁷ YÜCEDAĞ, a.g.e., s. 145

¹²⁸ “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulu’nun 25/03/2019 tarihli ve 2019/78 Sayılı Karara konu olayda veri sorumlusu, petrol piyasasında dağıtıcı lisansı kapsamında faaliyet gösteren bir şirkettir. Veri sorumlusu, Enerji Piyasası Düzenleme Kurulu (EPDK) tarafından alınan bir karar ile kendilerine pompa satış hareketlerini plaka, akaryakıt türü, miktar, fiyat, zaman (saat, dakika ve saniye) bilgilerini almaları gerektiği yönünde bir yükümlülük yüklendiğini ve kendilerinin de bir otomasyon sistemi kurduklarını ve bu sistemi de EPDK’nın erişimine açtıklarını belirtmiştir. Veri sorumlusu, bu verileri yasal yükümlülüğünü yerine getirmek için aldığını ancak bu verileri daha farklı bir süreçte de kullanmak istediğini, hatalı akaryakıt dolumlarının önüne geçebilmek için araç tanıma projesi geliştirdiğini ve ellerindeki mevcut veriyi bu projede kullanmak istediklerini, ve bu kullanımın KVKK’de yer alan meşru menfaat veri işleme dayandırılıp dayandırılmayacağını Kişisel Verileri Koruma Kurumu’na sormuştur. Kişisel Verileri Koruma Kurulu kararında, veri sorumlusunun veriyi ilk aldığı anda KVKK m.5’te sayılan hallerden veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması unsurunun gündeme geldiğini, bununla birlikte veriyi ilk elde etme anındaki amaç ile projede güdülen amacın farklılık arz ettiğini, bu nedenle ikincil amacın genel ilkelere ve KVKK’de yer alan işleme şartlarına uygun olması gerektiğini, mevcut verilerin belirtilen projede kullanılmasının yeni bir veri işleme faaliyeti olduğunu, bu faaliyetin meşru menfaat veri işleme şartı kapsamında değerlendirilebileceğini, ancak veri sorumlusunun bu konuda erişilebilir ve görülebilir bir aydınlatma yapması gerektiğini ifade etmiştir.

¹²⁹ Süreç veya faaliyet bazlı olarak aynı kişisel verinin farklı amaçlarla işlenebileceğine ilişkin: Kişisel Verileri Koruma Kurumu, **Kişisel Veri İşleme Envanteri Hazırlama Rehberi**, KVKK Yayınları No: 30, s. 31, (www.kvkk.gov.tr), (Erişim: 22.07.2023)

bulunuyor ise izah olunan adımları atması gerekecektir. Kişisel Verileri Koruma Kurulu'nun 08.09.2022 tarihli güncel kararı da açıklamalarımız ile aynı doğrultuda olup veri işleme amacı değiştiği takdirde ilk kez veri işleniyor gibi aydınlatılma yapılması gerektiği ve KVKK'de belirlenen veri işleme şartlarından birisine dayanılması gerektiği şeklindedir.¹³⁰

Ç-İşlendikleri Amaçla Bağlantılı, Ölçülü ve Sınırlı Olma

İlke bünyesinde üç unsuru ihtiva etmektedir. Öncelikle kişisel veri işlendiği amaçla bağlantılı olmalıdır. İkinci aşamada kişisel veri işlendiği amaçla sınırlı olmalıdır. Son aşamada ise -ki kanaatimizce bu en önemli olanıdır- kişisel veri işlendiği amaçla ölçülü olmalıdır. Bu ilke GDPR'da veri minimizasyonu ilkesi olarak belirtilmektedir.¹³¹

İlke ile hedeflenen, veri sorumlusunun faaliyetini gerçekleştirebilmek için ihtiyaç duyduğu minimum veriyi kullanması ve kullandığı bu verinin de amacıyla bağlantılı ve sınırlı olmasıdır. Belirtmekte fayda var ki burada kastedilen veri sorumlusunun bütün süreçlerinde tamamen aynı şekilde sınırlı bir veri grubunu elde etmesi değil aksine süreç bazında, faaliyet bazında ihtiyaç duyulan minimum veriyi toplaması şeklindedir.¹³² Bu ihtiyacın da veri sorumlusunun faaliyet gösterdiği sektör ile, kişisel verilerin işleneceği süreç ile son derece bağlantılı olduğuna dikkat etmek gerekir. Örneğin bir veri sorumlusunun çok kritik ve ciddi bir operasyonu için sekiz farklı kişisel veriyi işlemesi ölçülü olabilecekken çok daha basit bir sürecinde dört adet kişisel veriyi işlemesi ölçülülük ilkesine aykırılık teşkil edebilir. Dolayısıyla ölçülülüğün, her somut olayın özelliğine göre ayrıca ele alınması gerekmektedir.

İlke içerisinde yer alan ilk unsur, kişisel verilerin işleme amacıyla bağlantılı olmasıdır. Burada kastedilen, veri sorumlusunun kişisel veriyi işleyeceği süreçle ilişkin veriyi toplaması ve işlemek istediği veriyle faaliyetinin amaçsal olarak bir bağı

¹³⁰ “İlgili kişinin telefon numarasının hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/923 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 20.07.2023), Kararın ilgili kısmı aynen “*Veri sorumlusu doktor tarafından telefon numarasının ilgili kişinin kendisinden alındığının beyan edildiği bu çerçevede söz konusu iletişim verisinin hasta doktor ilişkisi çerçevesinde muayene/televizyon süreçlerine ilişkin bilgilendirme amacıyla temin edildiğinin anlaşıldığı ancak daha sonra doktor tarafından reklam içerikli SMS göndermek amacıyla ilgili kişinin telefon numarasının işlendiği dikkate alındığında söz konusu kişisel veri işleme faaliyetinin Kanun’un 5’inci maddesinde yer alan herhangi bir işleme şartına dayanmadığına, bu kapsamda Kanun’un 12’nci maddesine aykırı uygulamada bulunan gerçek kişi veri sorumlusu doktor hakkında Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına*” şeklindedir.

¹³¹ GDPR m.5 / f. 1, c bendi

¹³² DÜLGER, a.g.e., s. 287

barındırmasıdır. Dolayısıyla amaçla bağlantılı olmayan bir işleme faaliyeti belirtilen ilkeye aykırılık teşkil edecektir.

İlke içerisinde yer alan bir diğer unsur, kişisel verilerin işlendikleri amaçla sınırlı olmasıdır. Bu unsur aslında, kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi ilkesi ile benzer doğrultudadır. Zira kanun koyucu öncelikle kişisel verilerin işlenirken belirli amaçlara ilişkin olması gerektiğini ifade etmekte akabinde bu ilke ile kişisel verilerin işlendikleri amaçla sınırlı olması gerektiğini belirtmektedir. Buradan hareketle kanun koyucunun veri sorumlusundan beklentisi, veri sorumlusunun kişisel veri işleme faaliyetine yönelik bir çerçeve çizmesini sağlamak ve bu doğrultuda veri sorumlusunun veri işleme amacını sınırlandırmasını sağlamaktır. Bir önceki başlıkta yaptığımız veri sorumlusunun kişisel veriyi toplama amacı ile sonraki işlemi amacı konusunu ilişkin açıklamalarımız¹³³ ve ilgili Kurul kararı,¹³⁴ bu bölüm için de geçerlidir.

Son olarak değinmek istediğimiz unsur ise kişisel verilerin işlendikleri amaçla ölçülü olması ilkesidir. Ölçülülük ilkesi olarak da anılan bu unsur, esasında veri sorumlusunun işlediği kişisel verinin miktarına yönelik bir düzenlemeyi içermektedir.¹³⁵ Bu ilke ile kanun koyucu, veri sorumlusunun adeta bir veri diyeti yapmasını, sadece faaliyetlerini yürütebilecek kadar veri işlemesini ancak daha fazlasını işlememesini hedeflemektedir.

Belirtmekte fayda var ki uygulamada en çok karıştırılan konulardan birisi şayet veri işleme faaliyeti, KVKK’de belirtilen veri işleme şartlarından herhangi birisine dayanıyorsa ve bu veri işleme şartı da veri sorumlusu tarafından doğru tespit edilmişse genel ilkelere riayet edilmese bile gerçekleştirilen veri işleme faaliyetinin doğru olduğu düşüncesidir. Bunu bir örnek ile açıklayalım.

Bir veri sorumlusunun gerçekleştirmek istediği operasyon için ölçülü olmayacak nitelikte kişisel veri talep ettiğini ancak ilgili kişinin de açık rıza göstermek suretiyle talep edilen verileri, veri sorumlusu ile paylaştığını varsayalım. Bu örneğimizde kişisel verilerin işlenmesi açısından veri işleme şartlarından bir tanesine dayanıldığı için veri işleme şartı özelinde herhangi bir problem bulunmamaktadır. Öte

¹³³ Bkz: s. 50 vd.

¹³⁴ Bkz: s. 50

¹³⁵ YÜCEDAĞ, a.g.e., s. 147; DÜLGER, a.g.e., s.288

yandan veri sorumlusu, dayanağı açık rıza olsa bile operasyonu için çok ciddi bir veri elde etmiştir. Bu durumda veri sorumlusu ölçülülük ilkesine aykırı hareket etmiştir. Netice itibariyle daha önceki yayınlarımızda da belirttiğimiz üzere sadece açık rıza almak veri sorumlusunu genel ilkelere riayet yükümlülüğünden kurtarmaz.¹³⁶ Veri sorumlusunun genel ilkelere riayet etme yükümlülüğü devam eder. Bu nedenle de açık rıza alınsa bile ilgili verinin ölçülülük ilkesine de uygun olması gerekir.¹³⁷

Ölçülülük ilkesi, her veri sorumlusunun faaliyet gösterdiği sektör, kişisel veriyi işlemek istediği süreç, işlemek istediği kişisel veri ile faaliyeti arasındaki orantılılık, amaç doğrultusunda ilgili kişisel verilerin işlenmesinin gerekliliği gözetilerek kontrol edileceğinden Kişisel Verileri Koruma Kurulu’nun bu ilkeye yaklaşımını, farklı senelerde vermiş olduğu kararları ele alarak izah edeceğiz.

Kişisel Verileri Koruma Kurulu’nun 02.08.2018 tarihli kararına¹³⁸ konu olayda, mahkeme tarafından veri sorumlusuna müzekkere yazılmış ve dava dosyasına bazı bilgileri sunması talep edilmiştir. Veri sorumlusu da müzekkereye cevap vermiş, ancak mahkemenin istediği veriden daha fazlasını sunmuştur. Bu olay netice itibariyle Kişisel Verileri Koruma Kurulu’nun önüne gelmiş ve karara bağlanmıştır. Karara göre, veri sorumlusunun kendisinden talep edilenden daha fazla kişisel veriyi yargılama sürecinde dahi olsa paylaşmasının, kişisel verilerin işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiği belirtilmiş ve veri sorumlusu hakkında idari yaptırım uygulanmasına karar verilmiştir.

Kişisel Verileri Koruma Kurulu’nun 25.03.2019 tarihli kararına konu olayda¹³⁹ veri sorumlusu, spor salonu hizmeti sunan bir şirkettir. Spor salonu, üyelerinin giriş-çıkış kontrolünde el-avuç okutma sistemi kullanmaktadır. Bu uygulama, ilgili kişiler tarafından yürütülen hukuki süreç nezdinde Kişisel Verileri Koruma Kurulu’nun önüne gelmiş ve karara bağlanmıştır. Karara göre, spor salonu

¹³⁶ Yasin ÜSTÜN/ Ayşe Nida GÜNAL, “İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi”, **Kişisel Verileri Koruma Dergisi**, Cilt 2, Sayı: 2, s. 65

¹³⁷ Ayşe Nida GÜNAL/ Yasin ÜSTÜN, “İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak “Meşru Menfaat”, **Kişisel Verileri Koruma Dergisi**, Cilt:4, Sayı: 2, 2022, s. 15

¹³⁸ İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık) ile ilgili Kişisel Verileri Koruma Kurulunun 02.08.2018 Tarihli Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.07.2023)

¹³⁹ Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.07.2023)

hizmetinden faydalanabilmek için el-avuç okutma sisteminin kullanılmasının, alternatif yollar mevcut iken özel nitelikli kişisel verilerin tercih edildiği ve bu tercihin de “minimum düzeyde veri talep etme ilkesi”ne aykırı olduğu tespit edilmiştir. Karar, Kişisel Verileri Koruma Kurulu’nun, ilgili ilkeyi en geniş ele aldığı ve açıkladığı kararlardandır. Bu nedenle Kurulun ilkeye yaklaşımı, karardan rahatlıkla anlaşılmaktadır. Özellikle veri sorumlusunun mevcut operasyonunu daha az kişisel veri işleyerek gerçekleştirmesinin mümkün olup olmadığı, veri işleme faaliyeti ile veri işleme amacı arasında bir dengesizlik olup olmadığı, minimum düzeyde verinin kullanılıp kullanılmadığı kararda irdelenmiştir.

Ayrıca belirtmek gerekir ki, veri sorumlusunun açık rızaya istinaden ilgili kişisel verileri işlediği savunması ise açık rızanın sınırsız bir veri işleme faaliyetinin kapılarını açmayacağı gerekçesiyle itibar görmemiştir.

Kişisel Verileri Koruma Kurulu’nun 06.08.2020 tarihli kararına konu olayda¹⁴⁰ veri sorumlusu, fiziksel mekan güvenliği sağlamak ve acil durum süreçlerini yürütebilmek konularını gerekçe göstererek bütün çalışanlarının parmak izini almış, çalışanlardan bu süreçte açık rıza almamış ve çalışanlarını aydınlatmamıştır. Kurul tarafından fiziksel mekan güvenliğinin temini için alternatif yolların mevcut olduğu, örneğin manyetik doğrulama, SMS doğrulama, barkodlu sistemler gibi yöntemler ile daha az kişisel veri işlenerek sürecin veri sorumlusu tarafından yürütülebileceği, bunun mümkün olmasına rağmen veri sorumlusu tarafından özel nitelikli kişisel verinin tercih edildiği, bu durumda amaç ile işlenen kişisel veri arasında bir dengesizlik olduğu tespit edilmiş ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı davranıldığından bahisle veri sorumlusu hakkında idari yaptırım uygulanmıştır.

Kişisel Verileri Koruma Kurulu’nun 19.01.2023 tarihli kararında¹⁴¹ ilgili kişi, veri sorumlusu olan çalıştığı şirketin kendisine tahsis ettiği kurumsal e-posta adresinde gerçekleştirdiği faaliyetinin izlendiğini, kontrol edildiğini ve bu faaliyetin ölçülülük ilkesine aykırılık teşkil ettiğini iddia etmiştir. Veri sorumlusu savunmasında özetle,

¹⁴⁰ “İşverenin, işçisine ait kişisel verileri ve özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.07.2023)

¹⁴¹ “Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/86 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 01.08.2023)

ilgili kişinin pazarlama ve iç iletişim yöneticisi olduğunu, ilgili kişinin şirketin ticari bilgilerini kendi şahsi e-posta adresine ilettiğini, başka bir çalışan ile gerçekleştirdiği telefon görüşmesini gizlice kayıt altına aldığını ve yine bu kaydı kendi şahsi e-posta adresine ilettiğini, ayrıca bu kaydı üçüncü bir kişiye de ilettiğini, bu bilgilere şirket içi denetim esnasında erişildiğini, ilgili kişinin görevleri arasında şirket içerisinde şüpheli paylaşımın tespiti halinde veri sorumlusunu bilgilendirmek görevinin yer aldığını, veri sorumlusu tarafından tüm çalışanların e-posta adreslerinin denetlenebileceği hususunda aydınlatıldığını, denetimlerde sadece anahtar kelimeler ve ekler uyarınca bir inceleme yapıldığını ve yalnızca şüpheli olanların tetkik edildiğini ifade etmiştir. Kurul öncelikle, incelediği dokümanlar uyarınca veri sorumlusunun ilgili kişiyi e-posta adresinin denetlenebileceği konusunda aydınlattığını tespit etmiştir. Akabinde, iletişim akışının incelenmesi ve iletişim içeriğinin denetlenmesi arasında fark bulunduğunu, veri sorumlusunun öncelikle aldırıldığı bir denetim raporu ile ilgili kişinin iletişim akışında şüpheyi tespit ettiğini, ardından şüpheyi istinaden ikinci aşamada içerik denetimi yaptığını, veri sorumlusunun herhangi bir ihlalin gerçekleşip gerçekleşmediğini yalnızca içerik denetimi yaparak tespit edebileceğini, bu doğrultuda kapsamın ilgili personel ile sınırlı tutulduğunu ve yine kişisel veri işleme faaliyetinin asıl amaç olan denetim amacıyla sınırlı tutulduğunu gözeterek ilkenin ihlal edilmediğine karar vermiştir.

Kurul, denetimin kademeli gerçekleştirilmesi, bütün işçilerin içerik denetimine maruz kalmasından ziyade önce rapor aldırılmak suretiyle eylemleri şüpheli işçilerin tespit edilerek kapsamın daraltılması, yalnızca denetim amacıyla sınırlı olarak içerik denetimi yapılması kriterlerini göz önünde bulundurmıştır. Bu kararda veri sorumlusunun takip ettiği kademeli süreç, e-posta içeriği denetlemek isteyen veri sorumluları için iyi bir örnek teşkil etmektedir.

Yeri gelmişken belirtmekte fayda var ki Anayasa Mahkemesi'nin 17.09.2020 tarihli kararı da işçinin e-posta içeriğinin kontrolü açısından çok önemlidir.¹⁴² Kararda,

¹⁴² Anayasa Mahkemesi, Başvuru Numarası: 2016/13010, Karar Tarihi: 17.09.2020, kararın ilgili kısmı aynen “Öncelikle e-posta hesabı üzerinden yapılan iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hâllerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmalıdır. Buradan hareketle çalışana açık bir bilgilendirmenin yapılmadığı hâllerde hak ve özgürlüklerine bir müdahalede bulunulmayacağı hususunda çalışanların makul bir beklenti içinde olacaklarının kabul edilmesi, temel hak ve özgürlüklerin sağladığı güvencelerden yararlandırılması gerektiği söylenebilir. Somut olayda başvurusunun yazılı olmayan iş sözleşmesi kapsamında görev yaptığı, yargılama sürecinde işverenin kurumsal e-postayı inceleme yetkisi ile kapsamını gösteren bir

e-posta hesabının iletişimin akışına ve içeriğine erişilecek şekilde kullanılmasının meşru menfaat kapsamında değerlendirilebileceği fakat ilgili kişinin bu denetim mekanizması hakkında bilgi sahibi olması gerektiği, aksi takdirde çalışan tarafından hak ve özgürlüklerine bir müdahalede bulunulmayacağı şeklinde makul bir beklentinin oluşacağı tespitlerine yer verilmiştir.

D-İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi diğer ilkelerin mantıksal bir sonucudur.¹⁴³ Zira kanun koyucu veri sorumlusundan, amacı belirlemesini, çerçeveyi daraltmasını ve yalnızca bu amaçla kişisel veri işlemesini beklemektedir. Bunun sonucunda da veri sorumlusunun amacı gerçekleşmiş ise veya amacı ortadan kalkmışsa artık o veriyi işlememesi gerekmektedir.¹⁴⁴ Bu durumda veri işleme faaliyetine son vermesi beklenmektedir.

İlke uyarınca her veri sorumlusunun işlediği kişisel verinin bir ömrü vardır. Her veriye ömür tayin etmek ve bunu doğru bir şekilde yapabilmek ise son derece meşakkatli bir iştir. Zira bir veri sorumlusunun bu ilkeye tam manasıyla uygun hareket edebilmesi için işlediği bütün kişisel veriyi bilmesi, bütün süreçlerini bilmesi, bütün amaçlarını bilmesi ve faaliyet gösterdiği sektörde süre yönünden özel bir düzenleme olup olmadığını bilmesi gerekir.

İlke, içerisinde iki unsuru ihtiva etmektedir. Bunlardan birincisi ilgili mevzuatta öngörülen süre kadar muhafaza edilme ilkesidir. Buna göre bir veri sorumlusunun işlediği kişisel veriler açısından mevzuatta düzenleme mevcut ise bu süre kadar kişisel verinin muhafaza edilmesi gerekmektedir.¹⁴⁵

bildirimin başvuruca yapıldığına ilişkin bilgi ve belge sunmadığı hususları gözetildiğinde işveren tarafından kurumsal e-posta hesabı üzerinden yapılan iletişimin izlenebileceği ve denetlenebileceği yönünde açık bir bilgilendirme yapılmadığı anlaşılmaktadır. Öte yandan e-posta iletişim içerikleri gerekçe gösterilerek başvurunun iş akdi feshedilmiştir. Ancak işveren davalı taraf olarak yargılama sürecinde kişisel verilerin işlenmesinin hukuki dayanağı ve işlemenin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemenin sonuçları ve verilerin muhtemel yararlanıcılarını gösterir bir bilgilendirme yapıldığını ortaya koyamamıştır. Bu bağlamda yargılama sürecinde feshin temel sebebini oluşturan e-posta iletişimine yönelik olarak böyle bir bilgilendirmenin yapıp yapılmadığı derece mahkemelerince tartışılmamış, başvurunun kendisi alenileştirmedeği hâlde onun rızası alınmadan ve önceden bir bilgilendirme yapılmadan e-posta içeriklerine erişildiği yönündeki esaslı iddialarının karşılanmadığı anlaşılmıştır.” şeklinde.

¹⁴³ DÜLGER, a.g.e., s. 300

¹⁴⁴ Kişisel Verileri Koruma Kurumu, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No: 29, Ankara, Haziran 2019, s. 9, (www.kvkk.gov.tr), (Erişim: 22.07.2023)

¹⁴⁵ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları No:1, Ankara, Aralık 2019, s. 69, (www.kvkk.gov.tr), (Erişim: 22.07.2023)

Kişisel Verileri Koruma Kurulu da bir kararında¹⁴⁶ veri sorumlusu olan bankanın 5411 sayılı Bankacılık Kanunu'na tabi olduğu, ilgili kanunun 42. maddesine göre ilgili kişinin kişisel verilerinin işlenmesi için bankalara bir süre belirtildiği, buradan hareketle ilgili kişinin mevzuatta öngörülen süreden önce kendisine ait kişisel verilerin silinmesi talebi ve şikayeti açısından yapılacak bir işlem olmadığına karar vermiştir. Dolayısıyla veri sorumlusu, şayet mevzuatta öngörülen bir süreye dayanarak veri işleme faaliyetini gerçekleştiriyor ve ilgili kişi de bu süreden önce işleme faaliyetine son verilmesini talep ediyor ise veri sorumlusu ilgili kişinin talebini reddetmelidir.

Birinci unsurun tespiti, çalışma alanı belirlendikten sonra son derece kolaydır. Çünkü kişisel verilerin işleneceği süre açısından mevzuatta bir düzenleme olup olmadığı ihtilafa konu olacak bir husus değildir. Önemli olan iyi bir mevzuat taraması ile hiçbir yasal düzenlemeyi atlamamaktır.

Öte yandan, her zaman veri sorumlusunun bir kişisel veriyi ne kadar süre ile işlemesi gerektiği açıkça yazmayabilir. Çoğunlukla da böyle bir süre mevzuatta yer almaz. Bu durumda ilke içerisinde yer alan ikinci unsur gündeme gelmektedir. Bu halde, kişisel veri işlendikleri amaç için gerekli olan süre kadar muhafaza edilecektir. Peki veri sorumlusu, kişisel verinin işlenmesi için gerekli olan süreyi neye göre tayin edecektir? Örneğin bir çalışan adayının özgeçmişinin 6 ay saklaması ile 12 ay saklanması arasında bir fark var mıdır? Belirtmek gerekir ki bu sorular açısından kesin bir cevap vermek mümkün değildir.

Kanun koyucu bu noktada süre tayin etme yetkisini veri sorumlusuna bırakmıştır. Zira her veri sorumlusunun bir kişisel veriyi işlemekte amacı aynı olmayacağı için veya her veri sorumlusunun faaliyet gösterdiği sektör aynı olmayacağı için bu konuda tüm veri sorumluları adına genel bir süre tayin etmek mümkün değildir. Bu durumda veri sorumlusu, kişisel veriyi hangi süreçte işleyeceğini belirlemeli, bu veriye neden ihtiyaç duyduğunu belirlemeli ve en nihayetinde de veriye ihtiyacının ne zaman ortadan kalktığını belirlemelidir.¹⁴⁷ Sorumuz üzerinden ilerleyecek olursak bir

¹⁴⁶ “İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi gereğince kişisel verilerin silinmemesi hakkında” Kişisel Verileri Koruma Kurulunun 05/12/2018 tarihli ve 2018/142 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 22.07.2023)

¹⁴⁷ Kişisel verinin gelecekte kullanılma ihtimaline istinaden işlenemeyeceği hakkında: Kişisel Verileri Koruma Kurumu, Örneklerle Kişisel Verilerin Korunması, KVKK Yayınları No: 29, Ankara, Haziran 2019, s. 9, (www.kvkk.gov.tr), (Erişim: 22.07.2023); Makul sürenin tayininde “bir verinin daha fazla saklanması için geçerli bir sebebinin kalmaması” kriteri hakkında: Kişisel Verileri Koruma Kurumu,

çalışan adayının özgeçmişinin altı ay ya da on iki ay saklanması açısından kanaatimizce bir farklılık yoktur. Öte yandan bir çalışan adayı özgeçmişinin beş yıl saklanması da kanaatimizce makul kabul edilemez. Çünkü hiçbir sektörde bir çalışan adayının başvurusuna beş yıl sonra geri dönüş yapılması makul karşılanmaz. Bu nedenle kişisel verinin bu denli uzun bir süre veri sorumlusu bünyesinde kalması ilkeye aykırılık teşkil edecek niteliktedir.

Netice itibariyle veri sorumlusu öncelikle bir kişisel veriyi işlemesi için mevzuatta bir süre öngörülüp öngörülmediğini araştırmalı, şayet bir süre var ise kişisel veriyi o süre kadar işlemeli, şayet bir süre öngörülmemiş ise kişisel veriyi işlediği süreç, amaç ve kişisel veriye olan ihtiyacının ne kadar sürede ortadan kalkacağını belirlemeli ve makul bir süre tayin etmelidir.

III- KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

A-KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

1-Açık Rıza

Açık rıza hem kişisel verilerin hem de özel nitelikli kişisel verilerin işlenmesi şartlarından birisidir.¹⁴⁸ Özel nitelikli kişisel verilerin işlenme şartları, birazdan anlatılacağından¹⁴⁹ bu bölümde genel anlamda kişisel verilerin işlenme şartı olan açık rıza ele alınacaktır.

Açık rızanın tanımı, açık rızanın şartları, battaniye rıza gibi kavramlar ve Kişisel Verileri Koruma Kurulu’nun açık rıza konulu kararları, çalışmanın tanımlar bölümünde anlatıldığından¹⁵⁰ bu başlık altında ağırlıklı olarak açık rızaya ilişkin özellik arz eden durumlar, açık rızanın geri alınması, açık rızanın gösterilme şekli ve gerekmediği halde açık rıza alınması durumunda konunun nasıl ele alınacağı anlatılacaktır.

Açık rızaya ilişkin ilk ele alacağımız konu, açık rızanın diğer veri işleme şartlarından üstün olup olmadığı konusudur. KVKK m. 5/ f. 1 hükmü incelendiğinde, kişisel verilerin işlenmesinde açık rıza alınmasının kural olduğu, ikinci fıkrada anılan

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları No:1, Ankara, Aralık 2019, s. 70, (www.kvkk.gov.tr), (Erişim: 23.07.2023)

¹⁴⁸ KVKK m. 5/ f. 1 hükmü aynen “*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.*”, KVKK m. 6/ f. 2 hükmü aynen “*Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.*” ve KVKK m. 8/ f. 1 hükmü aynen “*Kişisel veriler; ilgili kişinin açık rızası olmaksızın aktarılamaz.*” şeklindedir.

¹⁴⁹ Bkz: s. 85 vd.

¹⁵⁰ Detaylı bilgi için: s. 37-46.

işleme şartlarının ise istisna teşkil ettiği izlenimi oluşabilir. Ancak kişisel verilerin işlenme şartları olarak belirtilen ve KVKK m.5'te sayılan hiçbir veri işleme şartı birbirinden üstün durumda değildir. Bütün veri işleme şartları eş değer seviyededir.

Açık rızanın diğer veri işleme şartlarından tek farkı, veri işleme şartının tespiti anında değerlendirmeye alınacak son veri işleme şartı olmasıdır. Nitekim Kişisel Verileri Koruma Kurumu da yayınladığı bir rehberde¹⁵¹, önce KVKK m.5'te sayılan bir veri işleme şartının uygulama imkanının olup olmadığının kontrol edilmesi gerektiğini, şayet KVKK m. 5 /f. 2'de sayılan hiçbir veri işleme şartına dayanılamıyor ise o zaman açık rıza alınması gerektiğini ifade etmektedir. Netice itibariyle açık rıza, diğer veri işleme şartları ile eşdeğer seviyede bulunan, diğer veri işleme şartlarına bir üstünlüğü bulunmayan ancak en son ele alınması gereken bir veri işleme şartıdır.

Açık rızaya ilişkin değinilmesi gereken önemli konulardan birisi de açık rızanın geri alınabilirliğidir. KVKK'de açık rızanın geri alınabilirliği hakkında herhangi bir düzenleme bulunmamaktadır.¹⁵² Ancak, ilgili kişiler, kişisel verilerinin geleceğini belirleme hakkına sahiptir. Bu hak aynı zamanda kişilik hakkının da bir neticesidir.¹⁵³ Kişinin rızasına dayalı olarak yürütülen bir sürecin, kişinin rızası ortadan kalktığında yürütülmemesi gerekmektedir. Zira dayanak ortadan kalkmıştır. Dolayısıyla açık rızanın geri alınabilirliği de bu durumun en doğal sonucudur. Verilen rızanın istenilen her durumda geri alınması mümkündür.¹⁵⁴

Açık rızanın geri alınması, ileriye yönelik netice doğuracak bir işlemidir. Burada esas olan nokta, açık rızanın geri alınmasına yönelik beyanın veri sorumlusuna tebliğ edildiği andır.

Veri sorumlusu, ilgili kişinin bu iradesini öğrendiğinde artık talebi doğrultusunda hareket etmeli ve o an itibariyle derhal açık rızaya istinaden yürüttüğü veri işleme faaliyetine son vermelidir.¹⁵⁵ Kural bu olmakla birlikte bazı somut olaylar

¹⁵¹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 5, (www.kvkk.gov.tr), (Erişim: 24.07.2023)

¹⁵² TAŞTAN, a.g.e., s. 165'te KVKK m. 11/ f. 1, e bendinin dolaylı da olsa açık rızanın geri alınabilirliğini düzenlediği görüşündedir.

¹⁵³ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, s.11, (www.kvkk.gov.tr), (Erişim: 25.07.2023)

¹⁵⁴ AVCI BRAUN, a.g.e., s. 17; TAŞTAN, a.g.e., s 165

¹⁵⁵ Konuya ilişkin Kişisel Verileri Koruma Kurumu tarafından yayınlanan duyuru için: www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar, (Erişim: 25.07.2023); Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, s. 26, (www.kvkk.gov.tr), (Erişim: 25.07.2023)

açısından özel durumlar söz konusu olabilir. Örneğin, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik¹⁵⁶ m. 10 hükmü aynen “*Hizmet sağlayıcı, alıcının ticari elektronik iletiyi almayı reddettiğine ilişkin talebinin kendisine ulaşmasını müteakip üç iş günü içinde alıcıya ticari elektronik ileti göndermeyi durdurur.*” şeklindedir. Açıkça anlaşılacağı üzere bu maddeye göre hizmet sağlayıcısına veri işleme faaliyeti için 3 iş günü daha süre tanınmıştır.

Açık rızayla ilgili uygulamada yapılan en büyük hatalardan birisi, açık rıza gerekmediği halde veri işleme faaliyetinin ilgili kişiden açık rıza almak suretiyle yürütülmesidir. Bu durumda iki sorun gündeme gelmektedir. Birincisi, veri sorumlusu ilk etapta yanlış bir veri işleme şartı tercih etmiş ve aydınlatma metnine de açık rıza gerekmediği halde ilgili kişisel veriyi açık rızaya istinaden işlediğini yazmıştır. Acaba veri sorumlusunun bu yanlış tercihi tek başına bir sorun teşkil etmekte midir? İkinci ve en önemli soru ise eğer ilgili kişi verdiği açık rızayı geri alır ise ve veri sorumlusu da veri işlemeye devam ederse ne olacaktır?

Kişisel Verileri Koruma Kurumu’na göre açık rıza gerekmediği halde açık rıza alan bir veri sorumlusu, ilgili kişiyi yanıltmakta, aldatıcı davranmakta ve hakkını kötüye kullanmaktadır.¹⁵⁷ Veri sorumlusu bu hareketiyle, ilgili kişi nezdinde adeta rıza geri alındığında veri işleme sürecine son verileceği izlenimini uyandırmaktadır.

Örneğin bir şirketin, işçisinin özlük dosyasını oluşturma ve arşivleme süreçleri için gerekmediği halde işçisinden açık rıza aldığını ve işçisinin kişisel verilerini açık rızaya istinaden işlediğini, işçinin de çalışması devam ederken açık rızasını geri aldığını varsayalım. Bu örnekte veri sorumlusu, işçi nezdinde, şayet rızasını geri

¹⁵⁶ RG., 29417 S., 15.07.2015 T.

¹⁵⁷ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları, s. 2-3, (www.kvkk.gov.tr), (Erişim: 25.07.2023); “Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbar” ile ilgili olarak Kişisel Verileri Koruma Kurulu’nun 20/04/2021 tarihli ve 2021/389 sayılı Karar Özeti’nin ilgili kısmı aynen “*Ayrıca söz konusu kişisel veri işleme faaliyeti, Kanunda yer alan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı ve bu durumun ise Kanunun 4 üncü maddesinin ikinci fıkrasının (a) bendinde düzenlenen “hukuka ve dürüstlük kurallarına uygun olma” ilkesine aykırılık teşkil ettiği*” şeklindedir. Ayrıca Kişisel Verileri Koruma Kurulu’nun “Hizmetin Açık Rıza Şartına Bağlanması” isimli kararının da ilgili kısmı aynen “*Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği*” şeklindedir.(www.kvkk.gov.tr/Icerik/5412/Acik-Rizanın-Hizmet-Sartina-Baglanması), (Erişim: 25.07.2023)

çekerse özlük verisi tutmayacağı, özlük dosyası sürecindeki kişisel verileri işlemeyeceği izlenimini uyandırmaktadır.

Öte yandan, veri sorumlusunun özlük dosyası tutması ve bu bağlamda özlük verilerini işlemesi kanuni bir yükümlülüğüdür. Bu durumda veri sorumlusu ya açık rıza geri alındığı için veri işleme faaliyetine son verecek ve fakat özlük sürecine ilişkin yasal yükümlülüklerini yerine getirmeyecektir ya da veri sorumlusu, işçisi açık rızasını geri alsa bile yine de veri işlemeye devam edecektir.

İşte ikinci durum Kişisel Verileri Koruma Kurumu tarafından, hukuka ve dürüstlük kuralına uygun olma ilkesine aykırılık olarak değerlendirilmektedir.¹⁵⁸ Netice itibariyle Kurum, yukarıda ele aldığımız ilk davranışı aldattıcı, ilgili kişiyi yanıltıcı bir tutum olarak nitelendirmekte ve veri sorumlusunun hakkını kötüye kullandığını ifade etmektedir. İkinci hatalı eylemi ise hukuka ve dürüstlük kuralına uygun olma ilkesine aykırılık olarak değerlendirmektedir.

Doktrinde de gerekmediği halde açık rıza alınarak gerçekleştirilen bir veri işleme faaliyetinde, ilgili kişinin açık rızasını geri aldığı durumlarda veri sorumlusunun yine de diğer veri işleme şartlarına dayanarak veri işleme faaliyetine devam etmesi durumu, yanlış bir izlenime yol açan, aldattıcı bir eylem olarak nitelendirilip veri sorumlusu tarafından hakkın kötüye kullanımı olarak değerlendirilmekte ve bu sebeple de hukuka ve dürüstlük kuralına uygun olma ilkesine aykırılık teşkil ettiği ifade edilmektedir.¹⁵⁹

Bir başka görüşe göre ise burada süreç ikiye ayrılarak ele alınmalı, veri sorumlusunun başka bir sebebe dayanmak yerine açık rıza alması tek başına bir hukuka aykırılık olarak değerlendirilmemeli, öte yandan ilgili kişi açık rızasını geri çeker ve veri sorumlusu da başka bir veri işleme şartına dayanarak veri işleme faaliyetine devam ederse bu eylem hukuka ve dürüstlük kuralına uygun olma ilkesine aykırı kabul edilmelidir.¹⁶⁰

Kanaatimizce açık rıza alınması gerekmediği halde açık rıza alınması ve ilgili kişinin de açık rızasını geri çektiği halde veri sorumlusunun veri işleme faaliyetine

¹⁵⁸ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 3, (www.kvkk.gov.tr), (Erişim: 25.07.2023)

¹⁵⁹ DÜLGER, a.g.e., s. 390; KÜZECİ, s. 395; Oğulcan ÖZKAN, **Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2020, s. 106

¹⁶⁰ ÇEKİN, a.g.e., s. 103

devam etmesi, ilgili kişiyi aldatıcı nitelikte olup hakkın kötüye kullanımı teşkil etmektedir. Aksinin kabulü halinde bir veri sorumlusu, hem açık rıza dışındaki şartlardan birini veya birkaçını veri işleme faaliyetinin gerekçesi olarak gösterebilir hem de garanti olması açısından açık rıza almak suretiyle açık rızaya da dayanabilir. Bu tutum, veri sorumlusunun en azından bir doğru veri işleme şartını gerekçe gösterebilme gayesiyle ilgilidir. Kanaatimizce buna imkân tanıyan bir yaklaşımın kabulü isabetli değildir.

Bu yaklaşımın bir müeyyidesi olmaz ise açık rızanın içi boşaltılmış olur. Zira ilgili kişi, açık rızasını geri çekse de bir anlam ifade etmeyecektir. Bu nedenle belirtilen durumun hakkın kötüye kullanımı olduğu yönündeki Kişisel Verileri Koruma Kurumu'nun da iştirak ettiği, doktrinde belirtilen ilk görüşe, biz de belirttiğimiz gerekçeler ile iştirak etmekteyiz.

Ayrıca, açık rıza almak için veri sorumlusunun ek bir avantaj teklif edip edemeyeceğinin de incelenmesi gerekmektedir. Burada, açık rızanın bir hizmet şartına bağlanması ile açık rıza karşılığı ek bir avantaj teklif edilmesini karıştırmamak gerekir. Açık rızanın hizmet şartına bağlanması durumunda veri sorumlusu ilgili kişiye adeta “ya açık rıza göster ya da hizmeti alma” demektir. Dolayısıyla ortada bir baskı unsuru söz konusudur. Bu da açık rızayı sakatlamaktadır.

Ek avantaj durumunda ise veri sorumlusu, ilgili kişiye cezbedici bir teklifle gelmektedir. Bu durumda veri sorumlusu baskı uygulamaktan ziyade teşvik edici davranış sergilemektedir. Bu durumu bir örnekle açıklayalım.

Bir market zincirinin, sadakat programı kapsamında bir kart çıkardığını, bu kartı alan müşterilerine kaydolurken belirttikleri telefon numarasına düzenli olarak ticari elektronik ileti gönderdiğini, her hafta pazartesi günü ise bir SMS gönderdiğini ve bu SMS ile müşterilerin %8 indirimli alışveriş yapabileceğini varsayalım. Bu örneğimizde veri sorumlusu, açık rıza almak için ilgili kişiye %8 oranında bir indirim vadetmektedir. Bu durumda, ilgili kişinin bir baskı altında olduğu söylenemez. Zira burada baskı değil teşvik söz konusudur.

Öte yandan, açık rızanın hizmet şartına bağlandığı da söylenemez zira veri sorumlusu açık rıza göstermeyen müşterilerine de aynı ürünleri satmaya devam etmekte, hizmetini kesmemektedir. İşte bu durumda, ek avantaj karşılığı alınan açık

rızalar, diğer şartları sağlaması koşuluyla geçerlidir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında ek avantaj karşılığı açık rıza alınabilmesinin önünde bir engel bulunmadığını belirtmiştir.¹⁶¹

Veri sorumluları açısından önem arz eden bir diğer konu ise açık rızanın alınma şeklidir. KVKK’de açık rızanın nasıl alınacağı konusunda bir düzenleme yer almamaktadır. Bununla birlikte açık rıza alındığına ilişkin ispat yükümlülüğü veri sorumlusunun üzerindedir.¹⁶² Bu sebeple veri sorumlusu, ileride doğabilecek uyuşmazlıklara karşı ispat edilebilir bir yol tercih etmelidir.

Uygulamada ispat kolaylığı sağlaması açısından ilgili kişi aydınlatıldıktan sonra açık rızaya ilişkin bir metin imzalatılmakta ve bu metin veri sorumlusu tarafından arşivlenmektedir. Genel yaklaşım bu olmakla birlikte açık rıza muhakkak yazılı alınmak zorunda değildir. Bu kapsamda açık rızanın sözlü olarak alınması mümkün olduğu gibi dijital bir yolla alınması da mümkündür. Örneğin ilgili kişi, veri sorumlusunun web sitesinde bir kutucuğu işaretlemek suretiyle açık rıza gösterebilir.

Öte yandan, diğer koşulları sağlamak şartıyla açık rıza, ilgili kişinin aktif bir davranışıyla da alınabilir.¹⁶³ Örneğin Kişisel Verileri Koruma Kurumu’nun düzenlediği konferanslarda uyguladığı “kokart uygulaması” bu şekildedir.¹⁶⁴ Bu uygulamada ilgili kişi bir yaka kartı tercih etmek suretiyle aktif bir davranış sergilemekte ve açık rızasını bu şekilde göstermektedir. Dolayısıyla veri sorumlusu, açık rızaya ilişkin izah olunan bütün şartları sağlamak koşuluyla ilgili kişiden açık

¹⁶¹ “Bir market zincirinin sadakat kart uygulamasına ilişkin ihbar ve şikayetler hakkında” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/82 sayılı Karar Özeti’nin ilgili kısmı aynen “Müşterinin Sadakat Kart Programına üye olmadığı durumda Şirketin sunduğu ürüne ve kişiye özel fırsat dünyasından faydalanamadığı ancak bu durumun hiçbir şekilde herhangi bir müşterinin Şirketin sunduğu alışveriş ortamından faydalanmasını engellemediği dolayısıyla, veri sorumlusu Şirket tarafından hizmet sunumu kapsamında Sadakat Kart Programına katılımın müşteriler açısından zorunlu tutulmadığı, söz konusu Programa üye olmayan müşterilere hizmet sunulmaması gibi bir durum ortaya çıkmadığı dikkate alındığında, Sadakat Kart Programına üye olunması sırasında kişilerin açık rızalarına başvurulması aksi takdirde söz konusu programdan yararlanılmaması hususunda Şikayetçinin Şirket tarafından bir hizmet veya ürün sunulmasının açık rıza şartına bağlandığı iddiası ile ilgili Kurumca yapılacak bir işlem bulunmadığına” şeklindedir.

¹⁶² Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 28, (www.kvkk.gov.tr), (Erişim: 25.07.2023)

¹⁶³ Leyla KESER BERBER/ Ayça ATABEY/ Melis MERT, E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı: 2, 2019, s. 70,

¹⁶⁴ Kokart uygulamasına göre, etkinliğe katılan ziyaretçiler fotoğraf çekilen alana girmeden önce şayet fotoğraflarının çekilmesini ve paylaşılmasını istiyorlar ise yeşil yaka kartı, fotoğraflarının çekilmesini ve paylaşılmasını istemiyorlar ise kırmızı yaka kartı takmaktadır. Detaylı bilgi için Kişisel Verileri Koruma Kurumu, 2019 Faaliyet Raporu, s. 78

rızayı istediği şekilde alabilmektedir. Şekil açısından önem arz eden tek husus ispatlanabilir olmasıdır.

Ayrıca belirtmekte fayda var ki susma, eylem göstermeme halleri, ilgili kişinin açık rıza göstermesi olarak yorumlanamaz çünkü ortada aktif bir davranış bulunmamaktadır.¹⁶⁵ Başka bir anlatım ile, açık rızaya ilişkin veri sorumlusunun ilgili kişiye yönelik “rızası olmasaydı itiraz ederdi” şeklindeki savunmasına itibar edilmeyecek aksine “rızası olsa açıkça gösterirdi” yaklaşımı kabul edilecektir.

Son olarak değinmek istediğimiz husus, bazı durumlarda veri işleme faaliyetinin açık rızaya dayanarak gerçekleştirilmesinin mümkün olmamasıdır. Örneğin bir kişisel veri, veri sorumlusu tarafından reklam amaçlı işlenmek isteniyor ve fakat veri sorumlusunun bulunduğu sektör itibarıyla reklam yasağı mevcutsa, ilgili kişi açık rıza vermiş olsa dahi veri sorumlusu bu veriyi açık rızaya istinaden işleyemeyecektir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında özel hastaneler açısından reklam yasağı bulunduğunu, özel hastane tarafından hastalarından açık rıza alınmış olsa bile hastalarının tedavi süreçlerine ilişkin reklam yapılmasının yasak olduğunu ve bu nedenle de açık rıza veri işleme şartına dayanılamayacağını belirtmiştir.¹⁶⁶

2-Kanunlarda Açıkça Öngörülmesi

Kişisel verilerin işlenmesi, kanunlarda açıkça öngörülmüş ise veri sorumlusu, KVKK m. 5/ f. 2, a bendi uyarınca ilgili kişinin açık rızasına ihtiyaç duymadan kişisel

¹⁶⁵ Nafiye YÜCEDAĞ, Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt 75 Sayı 2, s. 775; Hale AKDAĞ, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Adalet Yayınevi, Ankara, 2013, s. 113-114; AVCI BRAUN, a.g.e., s. 29;

¹⁶⁶ “Bir hastanenin reklam ve tanıtım faaliyetleri kapsamında sağlık verileri de dahil kişisel verilerin işlenmesine ilişkin olarak hastalardan açık rıza almasının hukuka aykırı olduğuna yönelik ihbar hakkında” Kişisel Verileri Koruma Kurulunun 11/05/2023 tarihli ve 2023/787 sayılı Kararı, (www.kvkk.gov.tr), (Erişim: 26.07.2023), Kararın ilgili kısmı aynen “*Veri sorumlusu tarafından ilgili kişilerin hastalıkları ve tedavi süreciyle ilgili video çekimlerinin yapılması ve sosyal medya hesaplarından paylaşılması suretiyle özel nitelikli kişisel veri olan sağlık verilerinin işlenmekte olduğu ve bu hususta reklam, pazarlama ve tanıtım amacıyla kişisel verilerin işlenmesine yönelik Kanun’un 6’ncı maddesinin 2’nci fıkrası uyarınca ilgili kişilerin “açık rızasının” bulunduğu, ancak her ne kadar ilgili kişilerin açık rızası bulunsada sektörel düzenlemeler uyarınca özel hastanelerin talep yaratmaya yönelik tanıtım yapmalarının yasak olduğu, ayrıca Özel Hastaneler Yönetmeliği’nin 60’ıncı maddesinde yer alan yasaklayıcı hüküm dikkate alındığında somut olayda açık rızanın bir veri işleme şartı olarak ileri sürülemeyeceği ve dolayısıyla söz konusu veri işleme faaliyetinin Kanun’un 6’ncı maddesi kapsamında herhangi bir dayanağının bulunmadığı, bu doğrultuda Kanun’un 12’nci maddesinin 1’inci fıkrasının (a) bendi kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli tedbirleri almayan veri sorumlusu hakkında Kanun’un 18’inci maddesinin 1’inci fıkrasının (b) bendi gereğince 250.000 TL idari para cezası uygulanmasına” şeklindedir.*

verileri işleyebilecektir. Hemen belirtmek gerekir ki bu veri işleme şartına dayanılabilmesi için dayanağın, ya bir kanun maddesi olması gerekir ya da kanunun açık bir şekilde yönlendirme yaptığı ikincil bir düzenleme olması gerekir.

Doktrinde bu konuda bir görüşe göre yönetmeliklerin bu veri işleme şartına esas alınamayacağı ifade edilmektedir.¹⁶⁷ Bu görüşe katılmamaktayız çünkü kanun koyucu her zaman düzenlemelerini kanunda açık bir şekilde yapmayabilir ki genellikle daha detay düzenlemelere yönetmeliklerde yer verilir. Kanunda da bu konuların yönetmelikte düzenleneceği ayrıca belirtilir. Yönetmeliklerde de hangi kanunun hangi maddesine dayanılarak yönetmeliğin oluşturulduğu açıkça yazar. Hal böyle olunca kanunun açıkça yönetmeliği işaret ettiği durumlarda ilgili veri işleme faaliyetinin bir yönetmelik maddesine de dayanmak suretiyle gerçekleştirilmesi mümkündür. Nitekim Kişisel Veriler Koruma Kurumu da yayınlamış olduğu bir rehberde,¹⁶⁸ kanundaki açık hüküm ile ikincil bir mevzuata atıf yapılmasını “kanunlarda açıkça öngörülme” veri işleme şartı kapsamında ele alacağını belirtmiştir.

Ayrıca Kişisel Verileri Koruma Kurulu bir kararında da Devlet Arşivleri Hizmetleri Hakkında Yönetmelik m. 3 hükmünü bu kapsamda ele almıştır.¹⁶⁹ Yine Kişisel Verileri Koruma Kurulu’nun 25.06.2020 tarihli bir başka kararında da kanunlarda açıkça öngörülme veri işleme şartına dayanak olarak Bilgi Teknolojileri ve İletişim Kurulu’nun 2016/DK – YED/517 sayılı kararı ile onaylanan “Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar” düzenlemesi esas alınmıştır.¹⁷⁰

¹⁶⁷ DÜLGER, a.g.e., s. 392

¹⁶⁸ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 6, (www.kvkk.gov.tr), (Erişim: 26.07.2023)

¹⁶⁹ “Sicil dosyalarındaki kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkmaması sebebiyle, imha edilmemesi gerektiği hakkında” Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Karar Özeti

¹⁷⁰ “İlgili kişinin bir kargo şirketine karşı açtığı işe iade davasında, kişisel verisi olan kamera görüntülerinin kargo şirketi tarafından mahkemeye sunulması” hakkında Kişisel Verileri Koruma Kurulunun 25/06/2020 tarihli ve 2020/494 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 26.07.2023), Kararın ilgili kısmı aynen “İlgili kişinin veri sorumlusu kargo şirketi tarafından açık rızası alınmaksızın kamera kaydının alındığı iddiası karşısında; veri sorumlusunun daha önceden, ilgili kişinin imzaladığı kişisel veriler hakkında bilgilendirme metni gereğince aktarma merkezinde kamera kaydı alındığına ilişkin olarak ilgili kişiye bilgilendirme yapıldığı, ilgili kişinin imzaladığı bu aydınlatma bildirimine göre veri sorumlusunca kamera kayıtlarının hukuken geçerli sebeplere dayanılarak işlendiği” beyanı çerçevesinde değerlendirme yapıldığında; veri sorumlusunun ilgili kişinin açık rızasının alındığını tevsik edici belgeyi sunmadığı, ancak veri sorumlusunun kargo şirketi olduğu göz önüne alındığında; Bilgi Teknolojileri ve İletişim Kurulunun 2016/DK – YED/517 sayılı kararı ile onaylanan “Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar” düzenlemesinin “Posta gönderilerinin görüntüleme cihazları ile kontrolü” başlıklı 6 ncı maddesinin ikinci fıkrasında yer alan,

Netice itibariyle, bu veri işleme şartının temelinde veri sorumlusunun, kanun koyucunun kendisine yüklediği bir görevi yerine getirmek amacıyla ilgili kişisel veriyi işlemek zorunda olması yer almaktadır. Kanun koyucunun da kişisel verilerin işlenmesine yönelik düzenlemeyi her zaman kanun seviyesinde yapmayabileceği, açık bir atıf yapmak suretiyle bu alanın detaylarını bir yönetmelikte belirleyebileceği gerekçeleriyle ikincil mevzuatın da “kanunlarda açıkça öngörülme” şartı kapsamında ele alınabileceği kanaatindeyiz. İzah olunan rehber ve karar uyarınca da anlaşıldığı üzere Kişisel Verileri Koruma Kurumu’nun yaklaşımı da bu doğrultudadır.

Bu veri işleme şartına ilişkin uygulamada en sık yapılan hatalardan birisi, bazı kamu kurumlarının yayınladığı duyurular doğrultusunda veya kamu kurumlarının veri sorumlusundan bizzat talepleri doğrultusunda gerçekleştirilen veri işleme faaliyetlerinin bu veri işleme şartına dayandırılmasıdır. Örneği verilen bu durumlarda, “kanunlarda açıkça öngörülme” veri işleme şartına dayanılmaz, zira anılan düzenlemeler kanun olmayıp kanunla eş değer seviyede görülen bir düzenleme veya kanunun açıkça atıf yaptığı ikincil bir mevzuat da değildir.

Bu veri işleme şartı açısından en çok verilen örnek Bankacılık Kanunu’nun¹⁷¹ 42. maddesidir.¹⁷² Maddede açıkça ilgili kişinin kişisel verilerinin 10 yıl süreyle saklanması gerektiği düzenlenmektedir. Yine özlük dosyaları açısından “işçi özlük dosyaları” üst başlığını taşıyan İş Kanunu’nun 75. maddesi¹⁷³ bu şekildedir. Maddeye göre işçinin özlük dosyası kapsamında yer alması gereken bilgilerden birisi de işçinin kimlik bilgileridir. Dolayısıyla özlük dosyasında işçisinin kimlik bilgisini işleyen bir veri sorumlusunun “kanunlarda açıkça öngörülme” ilkesine dayanması mümkündür.

“Hizmet sağlayıcılarının posta gönderilerini kabul merkezlerinde kamera sistemi kurularak kayıtlar; gerektiğinde ilgili mercilere sunulmak üzere en az bir (1) ay süreyle saklanır.” hükmü gereğince veri sorumlusu kargo şirketinin, Kanunun 5 inci maddesinin ikinci fıkrasının (a) bendinde yer alan; “Kanunlarda açıkça öngörülmesi” hukuki sebebine uygun olarak işleme yaptığı” şeklindedir.

¹⁷¹ RG., 25983 S., 01.11.2005 T.

¹⁷² Madde aynen “Alınan yazılar ve faaliyetler ile ilgili belgelerin asılları veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyaları ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretleri, usûlleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanır. Bu belgelerin mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkündür. Bu maddenin uygulanmasına ilişkin usûl ve esaslar Kurulca belirlenir.” şeklindedir.

¹⁷³ Madde aynen “İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.” şeklindedir.

Bir başka örnek olarak 657 sayılı Devlet Memurları Kanunu'nun¹⁷⁴ 109. maddesi¹⁷⁵ ele alınabilir. Maddede açıkça memurun mesleki bilgilerinin, mevcut ise soruşturma/denetim raporu, başarı belgesi, ödül belgesi verilmesine ilişkin bilgilerin veri sorumlusu tarafından işlenmesi gerektiği belirtilmiştir. Netice itibarıyla belirtilen kişisel verilerin bu maddeye atıfla ve “kanunlarda açıkça öngörülme” şartına dayanarak işlenmesi mümkündür.

3-Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin Ya Da Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması

Bu veri işleme şartı, KVKK m. 5/ f. 2, b bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Veri işleme şartına ilişkin önem arz eden bazı hususlar bulunmaktadır.

Öncelikle ilgili kişi ya fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan bir kişi ya da rızasını açıklayabilecek durumda olsa bile rızasına hukuki geçerlilik tanınmayan bir kişi olmalıdır. Birinci duruma örnek olarak sel sebebiyle ağaca tırmanan ve mahsur kalan bir kişi örnek verilebilir. İkinci duruma ise yarı baygın vaziyette yerde yatan birisi örnek verilebilir.

İkinci aşamada ise bu kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olma unsuru ele alınmalıdır. Burada en önemli nokta zorunluluk unsurudur. Şayet veri işleme faaliyeti, kişinin hayat bütünlüğünü korumaya yönelik fakat zorunluluk arz etmiyor ise artık bu veri işleme şartına dayanılması mümkün değildir.

Bu veri işleme şartı çok spesifik durumları ele aldığından örnekler ile izah etmek daha faydalı olacaktır. Örneğin eşiyle birlikte تنها bir yolda yürüyen kişi, karşı kaldırımdaki yaşlı bir kişinin önce kalbini tuttuğunu sonrasında birden yere yığıldığını fark eder. Yardım etmek isteyen kişi, yolun karşısına koşar ve eşine hemen ambulans çağırmasını söyler. Kendisi de bayılan kişinin yakınlarına haber vermek amacıyla bayılan kişinin telefonunu ve cüzdanını alır, cüzdandan kimliği çıkartıp bayılan kişinin

¹⁷⁴ RG., 12056 S., 23.07.1965 T.

¹⁷⁵ Maddenin ilgili kısmı “Özlük dosyasına, memurun mesleki bilgileri, mal bildirimleri; varsa inceleme, soruşturma, denetim raporları, disiplin cezaları ile ödül ve başarı belgesi verilmesine ilişkin bilgi ve belgeler konulur.” şeklindedir.

adını öğrenir, cep telefonundan ise rehberine girer, rehberde kayıtlı “eşim” ve “oğlum” isimli kişileri arayarak durumu bilgi verir, ayrıca bu kişileri kendi telefon rehberine de ekler.

Bu örneğimizde bayılan kişi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan bir kişidir. Bu sebeple ilk kriter sağlanmıştır. İkinci etapta ise zorunluluk unsurunun kişinin hayatı veya beden bütünlüğü kapsamında ele alınması gerekir. Bayılan kişinin yakınlarına haber verilmesi, kişinin hayatı için son derece önemlidir. Zira kişi, özellik arz eden bir hastalık geçmişine sahip olabilir, çok özel bir durumu olabilir ve bu bilgi kişinin hayatı açısından önem arz edebilir. Örneğin kişinin ilaç alerjisi olabilir ve ilaç alerjisi bilgisi sağlık ekiplerine iletilmediği takdirde yapılacak müdahale bile alerjik reaksiyona sebebiyet vererek kişinin ölümüne sebebiyet verebilir. Bu nedenle örneğimizde zorunluluk seviyesinin de gerçekleştiği kabul edilebilir.

Netice itibariyle olayda baygın kişiye yardım eden bu kişinin gerçekleştirdiği veri işleme faaliyeti “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” veri işleme şartına dayanarak gerçekleştirilmiştir. Kişisel Verileri Koruma Kurumu’nun yayınlamış olduğu bir rehberde¹⁷⁶ de benzer nitelikte örnekler¹⁷⁷ mevcuttur.

4-Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

Bu veri işleme şartı KVKK m. 5/ f. 2, c bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması veri işleme şartına dayanılabilmesi için iki unsurun bir arada bulunması gerekmektedir. Bunlardan birincisi, kişisel veri, sözleşmenin taraflarına ait olmalıdır.

¹⁷⁶ Kişisel Verileri Koruma, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No: 29, Ankara, Haziran 2019, s. 12, (www.kvkk.gov.tr), (Erişim: 28.07.2023)

¹⁷⁷ Dağda mahsur kalan bir kişinin cep telefonu sinyalinin takip edilmesi, konum verisinin işlenmesi ve ilgili kişinin kurtarılması; kaçırılan bir kişiyi kurtarmak için yetkililer tarafından MOBESE görüntülerinin izlenmesi

İkincisi ise söz konusu kişisel veri, ya sözleşmenin kurulması için gerekli olmalıdır ya da sözleşmenin ifası için gerekli olmalıdır.

Bu veri işleme şartı açısından uygulamada yapılan en büyük hatalardan birisi, sözleşmenin taraflarına ait olmayan kişisel verilerin de bu kapsamdaymış gibi değerlendirilmesidir. Örneğin bir veri sorumlusu, ilgili kişiyle arasındaki satış sözleşmesi uyarınca bir ürün teslimatı yapacaktır. İlgili kişi ise teslimat gününde tatilde olacağı için teslimat yapılabilmesi amacıyla komşusunun adını, soyadını, telefon numarasını veri sorumlusu ile paylaşmıştır. Her ne kadar işlenen kişisel veri, sözleşmenin ifasıyla ilgili de olsa komşu, sözleşmenin tarafı olmadığı için komşunun kişisel verilerinin işlenmesi açısından bu veri işleme şartına dayanılması mümkün değildir. Ancak örneğimizde sözleşmenin tarafı olan kişi, veri sorumlusu ile ev adresi, telefon numarası gibi bilgilerini paylaşmış olsaydı artık veri sorumlusu bu maddeye dayanarak veri işleyebilecekti.

Bu maddeye dayanılarak gerçekleştirilen veri işleme faaliyetlerinde veri sorumlusu genellikle bir yükümlülüğünü yerine getirmektedir. Örneğin çalışanlarına maaş ödemesi yapmak isteyen bir işverenin, çalışanın banka hesap bilgilerini işlemesi veya kredi sözleşmesi için bir bankanın, ilgili kişiye ait tapu kayıtları, tapu takyidatları, maaş bilgisi gibi kişisel verileri işlemesi bu veri işleme şartına örnek olarak verilebilir.¹⁷⁸

Veri işleme şartıyla ele alınması gereken bir diğer konu ise maddede geçen “doğrudan doğruya ilgili olma” ibaresidir. Madde 29 Çalışma Grubu, burada dar yorum yapılması gerektiği kanaatinde olup söz konusu kişisel verilerin işlenmesine gerçekten ihtiyaç duyulması gerektiğini ifade etmektedir.¹⁷⁹ Örneğin ilgili kişinin bir e-ticaret sitesinde sürekli ayakkabı araştırdığını ve ilgili firmanın da potansiyel müşterilerinin hangi ürünü ne kadar görüntülediklerini ve profillemeye çalışması yaptıklarını varsayalım. Bu durumda veri sorumlusunun belirtilen veri işleme şartına dayanması mümkün değildir. Zira burada veri sorumlusunun veri işleme faaliyeti

¹⁷⁸ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 8, (www.kvkk.gov.tr), (Erişim: 28.07.2023)

¹⁷⁹ KVKK m.5/ f. 2, c bendi ile Direktif’in 7 (b) maddesi benzer şekilde kaleme alınmıştır. Bu nedenle Madde 29 Çalışma Grubu’nun görüşü kıyasen KVKK m. / f. 2, c bendi açısından kıyasen de olsa yol gösterici niteliktedir. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 844/14 EN, s. 16; Dar yorum yapılması gerektiğine ilişkin aynı doğrultuda: DÜLGER, a.g.e., s. 399

sözleşmenin kurulması için gerekli değildir. Konuyla ilgili Kişisel Verileri Koruma Kurulu'nun 27.01.2020 tarihli kararının da ele alınması faydalı olacaktır.¹⁸⁰

Karara konu olayda, ulaşım hizmeti sunan veri sorumlusu, mobil uygulama üzerinden bir puanlama sistemi oluşturmuştur. Uygulamada yer alan şoför müşteriye puanlamakta, müşteri de şoförü puanlamaktadır. Öte yandan, müşteri şoförü puanladığını bilmekle birlikte şoförün kendisini puanladığını bilmemektedir. Veri sorumlusu savunmasında buradaki veri işleme faaliyetinin KVKK m. 5/ f. 2, c bendi kapsamında olduğunu belirtmiştir. Kurul ise bu veri işleme faaliyetinin sözleşmenin ifasına yönelik ana kurucu öge olmadığını, aynı zamanda sözleşmenin ifasına yönelik de doğrudan doğruya bir ilişkisinin olmadığını tespit etmiş ve veri sorumlusu hakkında idari yaptırım uygulamıştır.¹⁸¹

Karardan anlaşılacağı üzere bu veri işleme şartının yorumlanmasında Kişisel Verileri Koruma Kurulu öncelikle işlenen kişisel verilerin sözleşmenin ana kurucu ögesi olup olmadığına bakmakta, akabinde doğrudan doğruya ilgisi olup olmadığını incelemektedir. Veri sorumluları da bu maddeye dayanmak istedikleri durumlarda önce sözleşmenin esas konusunun ne olduğunu belirlemeli, ardından sözleşme kapsamında ifa edeceği yükümlülüklerin ne olduğunu belirlemeli ve son olarak da söz konusu ifa yükümlülüğüne ilişkin ihtiyaç duyacağı minimum veri miktarını belirlemelidir.

5-Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Bu veri işleme şartı KVKK m. 5/ f. 2, ç bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Bu veri işleme şartı genellikle “kanunlarda açıkça öngörülme” veri

¹⁸⁰ “Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler hakkında” Kişisel Verileri Koruma Kurulu'nun 27/01/2020 tarih ve 2020/65 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 28.07.2023)

¹⁸¹ Kararın ilgili kısmı aynen “Müşterilerin/yolcuların yaptığı seyahatlerin şoförler tarafından puanlanmasına ve bu puanların ortalamasının alınmasına dayanan veri işleme faaliyetinin, Kanunun 5 inci maddesinin 2 inci fıkrasının (c) bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” şartı kapsamında sözleşmenin ifasına ilişkin ana kurucu öge olmadığı veya sözleşmenin ifasıyla doğrudan doğruya bir ilişkisinin var olmaması sebebiyle ve bu veri işleme faaliyetinin aynı maddede belirtilen diğer veri işleme şartlarından herhangi birine dayanmadığı dikkate alındığında veri sorumlusunun Kanunun 12 inci maddesinin 1 inci fıkrasının a bendinde yer alan “veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır” hükmüne aykırı hareket ettiği kanaatine varıldığından hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının b bendine istinaden 100.000 TL idari para cezası uygulanmasına” şeklindedir.

işleme şartının kapsamına girmeyen fakat veri sorumlusunun hukuki yükümlülüğünü yerine getirdiği durumlarda karşımıza çıkmaktadır.

Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması veri işleme şartı, içerisinde iki unsuru ihtiva etmektedir. Bunlardan birincisi, veri işleme faaliyeti, veri sorumlusunun bir hukuki yükümlülüğünü yerine getirmesi amacına dayanmalıdır. İkincisi ise bu hukuki yükümlülüğü yerine getirebilmek için veri sorumlusu, veri işlemek zorunda olmalıdır.

Örneğin bir işçinin, işçilik alacaklarına ilişkin dava açması durumunda mahkemeler tarafından işverene müzekkere yazılmak suretiyle işçinin bordrolarının, özlük dosyalarının, yıllık izin kullanım formlarının, yapılan ödemelere ilişkin dekontların dava dosyasına sunulması talep edilmektedir. Bu örneğimiz uyarınca veri sorumlusunun müzekkereye cevaben ilgili evrakları sunması ve haliyle kişisel verileri işlemesi, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması işleme şartına dayanmaktadır.

Kişisel Verileri Koruma Kurulu da bir kararında¹⁸² Enerji Piyasası Düzenleme Kurulu (EPDK) tarafından alınan bir karar uyarınca petrol piyasalarında faaliyet gösteren bir veri sorumlusunun, araç sahiplerinin kişisel verilerini işlemesinin veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması veri işleme şartına dayandırmaktadır.

Ayrıca Kişisel Verileri Koruma Kurulu’nun bir başka kararına¹⁸³ konu olayda veri sorumlusu sağlık sektöründe faaliyet gösteren bir şirkettir. Veri sorumlusu, ilgili kişiden e-posta adresini talep etmiş, bu bilgiyi hasta kayıt sürecinde kullanmış, hastane bilgi yönetim sistemine kaydetmiş, SGK’ya aktarmış ve ilgili kişiye ticari elektronik ileti göndermiştir. Kurul kararında, ticari elektronik ileti gönderilmesi dışındaki süreç açısından hem KVKK’nin 5’inci maddesinin (2) numaralı fıkrasının c bendinde yer alan “Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” veri işleme şartı ile (ç) bendinde yer alan “Veri sorumlusunun hukukî yükümlülüğünü

¹⁸² “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti

¹⁸³ “Sağlık sektöründe faaliyet gösteren veri sorumlusu tarafından ilgili kişinin kişisel verilerinin açık rızası alınmaksızın ticarî elektronik ileti gönderilmesi amacıyla işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 18/01/2022 tarihli ve 2022/31 sayılı Karar Özeti

yerine getirebilmesi için zorunlu olması” veri işleme şartına dayanıldığını tespit etmiştir.

6-İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Bu veri işleme şartı KVKK m. 5/ f. 2, d bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Bu veri işleme şartına dayanılabilmesi için işlenen kişisel verinin ilgili kişi tarafından aleni hale getirilmiş olması zorunludur. Başka bir anlatımla, şayet kişisel veri ilgili kişinin kendisi tarafından aleni hale getirilmemiş ise veya veri aleni nitelikte değilse bu veri işleme şartına dayanılması mümkün değildir.

Aleni nitelikte bir kişisel veriden bahsedebilmek için öncelikle kişisel verinin herhangi bir yöntemle herkesin erişimine açılmış olması¹⁸⁴ gerekmektedir. Örneğin bir avukatın kendi hukuk bürosunun web sitesinde telefon numarasını paylaşması; bir muhasebecinin işyeri tabelasında şahsi telefon numarası bilgisine yer verilmesi bu şekildedir. Her iki örnekte de ilgili kişi, kişisel verisini kendi arzusu ile aleni hale getirmektedir.

Ayrıca, aleni hale gelen kişisel verinin, ilgili kişinin iradesi doğrultusunda aleni hale gelmiş olması gerekmektedir. Başka bir anlatımla, ilgili kişinin rızası olmadığı halde kamuoyuna yansıyan ve aleni hale gelmiş veriler açısından bu veri işleme şartına dayanılması mümkün değildir. Önemli olan, ilgili kişinin veriyi alenileştirme iradesidir.¹⁸⁵ Örneğin bir kişinin gizlice alınan ses kaydında, ilgili kişinin veriyi aleni hale getirme rızası ve iradesi olmadığı için bu ses kaydı kamuoyuna yansısa bile bu veri işleme şartına dayanılması mümkün değildir. Yeri gelmişken belirtmekte fayda var ki gizli ses kaydına ilişkin Anayasa Mahkemesi’nin 29.09.2022 tarihli kararı son derece önemlidir.¹⁸⁶ Kararda, ilgili kişinin aleni olmayan bir ortamda gizliliğinin korunacağına dair makul bir beklentisi olduğu, ilgili kişinin rızası dışında ses kaydı

¹⁸⁴ DÜLGER, a.g.e., s. 405

¹⁸⁵ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 10, (www.kvkk.gov.tr), (Erişim: 30.07.2023)

¹⁸⁶ Anayasa Mahkemesi, Başvuru Numarası: 2018/16857, Karar Tarihi: 29.09.2022, kararın ilgili kısmı aynen “Başvurucunun gizliliğinin korunacağı konusundaki haklı beklentisine dayalı olarak aleni olmayan bir ortamda diğer kişilerle yaptığı konuşmalarının onun rızasına aykırı şekilde kayıt altına alınmasının ve söz konusu ses içeriğinin yine onun rızasına aykırı olarak kullanılmasının özel hayatı kapsamında olan kişisel verilerine saldırı teşkil ettiği ve saldırının anılan hukuki değerler üzerindeki etkilerinin ağır olduğu açıktır.” şeklindedir.

alınması ve bu ses kaydının kullanılmasının kişisel verilere saldırı teşkil ettiği tespit edilmiştir.

Uygulamada birçok idari yaptırıma konu olan ve dikkat edilmesi gereken en önemli noktalardan birisi, ilgili kişinin kişisel veriyi aleni hale getirmekteki esas amacıdır. Bu amaç, her veri sorumlusu açısından farklılık arz edebilir. Örneğin bu amaç, ilgili kişi ile işi kapsamında sınırlı olmak üzere iletişim kurulması olabilir. Veriyi işleyecek olan veri sorumlusunun da ilgili kişinin veriyi alenileştirmedeki esas amacına dikkat etmesi ve veri işleme faaliyetinin sınırlarını, ilgili kişinin esas amacına göre belirlemesi gerekmektedir.

Konuyla ilgili Kişisel Verileri Koruma Kurulu’nun çok güncel bir kararı bulunmaktadır.¹⁸⁷ Karara konu olayda, ilgili kişi bir avukat, veri sorumlusu ise hukuk büroları için yazılım üreten ve geliştiren bir şirkettir. Bu şirket, ilgili kişi olan avukatın e-posta adresini, online arama motorları üzerinden yaptığı bir arama neticesinde elde etmiş ve kendisine ürünleriyle ilgili reklam amaçlı bir e-posta göndermiştir. İlgili kişinin şikayeti üzerine olay Kurul önüne gelmiştir. Kurul, avukatın e-posta adresini kendisinin alenileştirdiğini, fakat her aleni verinin hiçbir sınır olmaksızın işlenebileceği anlamına gelmediğini, veri sorumlusunun alenileştirme amacıyla bağlantılı ve sınırlı olunması gerektiğini, avukatın e-posta adresini alenileştirmedeki maksadının reklam ve kampanyalardan haberdar olma iradesini içermediğini tespit etmiştir. Karardan açıkça anlaşılabileceği üzere Kişisel Verileri Koruma Kurulu, bu veri işleme şartı açısından öncelikle verinin ilgili kişi tarafından alenileştirilip alenileştirilmediğine bakmakta akabinde ilgili kişinin alenileştirme amacının sınırlarını belirlemekte ve gerçekleşen veri işleme faaliyetinin bu sınır içinde kalıp kalmadığını belirlemektedir.

¹⁸⁷ “İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının açık rızası alınmaksızın veri sorumlusu bir pazarlama şirketi tarafından ticarî elektronik ileti gönderilmesi suretiyle işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/861 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 30.07.2023); Kararın ilgili kısmı aynen “*Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (d) bendinde yer alan “ilgili kişinin kendisi tarafından alenileştirilmiş olması” şartı kapsamında kişisel verilerin açık rıza olmaksızın işlenmesinin mümkün olduğu, ancak ilgili verinin alenileştirilmiş olmasının diğer bir ifadeyle kamuya açık hale getirilmiş olmasının bu kişisel verilerin her türlü amaç için işlenebileceği anlamına gelmediği, ancak alenileştirme amacıyla bağlantılı ve amaçla sınırlı olarak işlenebileceği, şikayete konu somut olayda ise ilgili kişinin iş e-posta adresinin avukatlık mesleğine yönelik yapılacak iletişimler kapsamında aleni hale getirildiği, pazarlama/reklam amacıyla yapılacak işlemlere ilişkin bir alenileştirme iradesini içermediği*” şeklindedir.

Kişisel Verileri Koruma Kurulu'nun bir başka kararında¹⁸⁸ ise ilgili kişinin alenileştirme amacının kendi mesleki yeterliliğinden faydalanılmasını sağlamak olduğu, fakat karara konu olayda veri sorumlusu olan sigorta şirketinin kendi ticari faaliyetlerine yönelik ilgili kişi ile iletişime geçtiği, bu durumun KVKK m. 5/ f. 2, d bendi kapsamında değerlendirilemeyeceği hususları tespit edilmiş ve veri sorumlusu hakkında idari yaptırım uygulanmıştır.

Kişisel Verileri Koruma Kurulu tarafından verilen her iki kararın ortak noktalarından birisi de veri sorumlusunun reklam/pazarlama amaçlı hareket etmesidir. Hatalı bir değerlendirme yapmamak adına belirtmekte fayda var ki her aleni verinin reklam/pazarlama amaçlı kullanılması, belirtilen veri işleme şartı açısından sorun teşkil etmeyebilir. Örneğin kiralık ev arayan ilgili kişinin, kiralık ev arayışında olduğu bilgisini ve telefon numarasını içerecek şekilde bir facebook grubunda gönderi paylaşması halinde, bu kişinin telefon numarasının veri sorumlusu olan bir emlakçı tarafından ev kiralamaya yönelik işlenmesi durumunda belirtilen veri işleme şartına dayanılabilecektir.

Sonuç itibarıyla bu veri işleme şartına dayanılabilmesi için veri, ilgili kişinin alenileştirme iradesi doğrultusunda ilgili kişi tarafından aleni hale getirilmiş olmalı, veri sorumlusu da ilgili kişinin alenileştirme amacı doğrultusunda kişisel veriyi işlemelidir. Bu amaç her somut olayın özelliğine göre belirlenecektir.

7-Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması

Bu veri işleme şartı KVKK m. 5/ f. 2, e bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Bu veri işleme şartı iki unsuru içermektedir. Öncelikli veri işleme

¹⁸⁸ “İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/331 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 30.07.2023); Kararın ilgili kısmı aynen “Şikâyetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Şirket tarafından Şikâyetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı, diğer bir deyişle Şikâyetçinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine Şirket faaliyetlerine ilişkin randevu talebi ile Şikâyetçinin arandığı anlaşıldığından, Şirket tarafından gerçekleştirilen veri işleme faaliyetinin 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci maddesinin (2) numaralı fıkrasının (d) bendi çerçevesinde değerlendirilemeyeceği kanaatine varılmış olup, bu kapsamda Şirketin kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almayarak Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı davranmış olması nedeniyle Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına karar verilmiştir.” şeklindedir.

faaliyeti bir hakkın tesisi, kullanılması ya da korunmasına yönelik olmalıdır. İkinci aşamada ise anılan veri işleme faaliyeti zorunlu olmalıdır. Bir başka ifadeyle, ilgili kişisel veri işlenmeden hakkın tesisi, kullanılması veya korunması neredeyse imkânsız olmalıdır.

Maddede belirtilen “hak” kavramı kanaatimizce geniş yorumlanmalıdır. Hak ekonomik olabileceği gibi manevi de olabilir. Önemli olan hukuk sisteminin koruyacağı bir hakkın bulunmasıdır.¹⁸⁹ Ayrıca veri işleme şartında yer alan “zorunluluk” unsurunun, veri sorumlusu açısından bir zorunluluk mu olduğu yoksa ilgili kişiye yönelik bir zorunluluk mu olduğu konusunun ele alınması gerekmektedir.

Kanunda açık bir düzenleme yer almamakla birlikte Kişisel Verileri Koruma Kurumu yayınladığı bir rehberde hem veri sorumlusu açısından hem de ilgili kişi açısından zorunluluk teşkil edebilecek örneklerle yer vermiştir.¹⁹⁰ Bir hakkın kullanılması, korunması veya tesisi açısından hakkına ulaşmak isteyen tarafın ilgili kişi veya veri sorumlusu olması arasında bir fark olmadığı, kanun koyucunun esas iradesinin hakka yönelik bir koruma sağlamak olduğu, bu nedenle de Kişisel Verileri Koruma Kurumu’nun yaklaşımı ile aynı doğrultuda olacak şekilde, zorunluluk unsurunun her iki taraf için de mümkün olabileceği kanaatindeyiz.

Bu veri işleme şartına örnek olarak işten ayrılan bir çalışanın ileride açabileceği davalarda hak kaybına uğramamak amacıyla işverenin dava zamanaşımı süresince çalışanın bordrolarını, performans verilerini, hakkındaki tutanakları saklaması ele alınabilir. Bir başka örnek olarak, bir belediye otobüsünün ayda bir kamera kayıtlarını silerek üzerine yeni görüntüleri kaydettiğini varsayalım. Belediye otobüsünün bir kazaya sebebiyet vermesi halinde, ilgili belediyenin görüntüleri aylık periyodun sonunda silmek yerine dava zamanaşımı boyunca saklaması bu kapsamda değerlendirilebilir.

¹⁸⁹ DÜLGER, a.g.e., s. 411

¹⁹⁰ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 11, (www.kvkk.gov.tr), (Erişim: 30.07.2023); İlgili kısım aynen “Örneğin, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması ya da kısıtlı bir kişinin haklarının korunması amacıyla vasisinin veya kayyumun, kısıtlının mali bilgilerini tutması gibi. Ayrıca, sözleşme sona erdikten sonra, olası yasal takiplere karşı zamanaşımı süresinin sonuna kadar fatura, sözleşme, kefaletname gibi belgelerin bu amaçlar için saklanması bu kapsamda değerlendirilecektir.” şeklindedir.

8-İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması

Bu veri işleme şartı KVKK m. 5/ f. 2, f bendinde düzenlenmiş olup ilgili madde uyarınca veri sorumlusu, ilgili kişinin açık rızasına ihtiyaç duymadan kişisel verilerini işleyebilecektir. Veri işleme şartının ismi çok uzun olduğundan çalışmanın bu bölümünde meşru menfaat kısaltmasını kullanacağız.

Meşru menfaat uygulamada en çok tercih edilen veri işleme şartlarından birisi olup tespiti konusunda son derece tereddütlere yol açan ve hakkında ciltlerce kitap yazılabilecek kadar detayları olan bir veri işleme şartıdır. Meşru menfaatin şartlarına değinmeden önce neden uygulamada çok tercih edildiğini izah etmenin faydalı olacağı kanaatindeyim. KVKK sistematığında bir veri sorumlusu, genellikle açık rıza veri işleme şartına dayanmak istemez.

Bunun temelinde, ilgili kişinin her zaman açık rızasını geri çekebilme imkanına sahip olması yatar. Veri sorumlusu genellikle, sürekli güncellemeyi gerektirecek bir opsiyondan ziyade hiç değiştirmeyeceği ve güncelleme ihtiyacı da hissetmeyeceği bir yöntemi tercih etme eğilimindedir. Hal böyle olunca veri sorumlusu mümkün mertebe her veri işleme faaliyetini KVKK m. 5/ f. 2’de yer alan şartlardan birisine dayandırmaya çalışır. Meşru menfaat de açık rızadan kaçınmak isteyen veri sorumlusunun adeta son çaresi olarak görülmektedir. Zira diğer veri işleme şartları meşru menfaate oranla daha açıktır. Şartları daha keskindir. Veri sorumlusunun tereddüt yaşadığı süreçlere ilişkin veri işleme faaliyetleri genellikle bu şartlara uymamaktadır.

Öte yandan veri sorumluları, zorlama da olsa meşru menfaatin uygulama imkânı olabileceğini düşünür. Bu nedenle de Türkiye özelinde hemen hemen KVKK uyum süreci geçiren her şirket “açık rıza almak yerine meşru menfaate dayanabilir miyiz?” sorusunu kendisine sormaktadır. Bu bakış açısının bir sonucu olarak da kanaatimce meşru menfaat uygulamada bir veri işleme şartı olarak görülmekten ziyade açık rızadan kaçınmak için alternatif bir yol olarak görülmektedir. Nitekim Kişisel Verileri Koruma Kurumu da bu eğilimin farkında olarak ilgili veri işleme şartının sınırsız bir veri işleme yetkisi tanımadığını ifade etmektedir.¹⁹¹

¹⁹¹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 16, (www.kvkk.gov.tr), (Erişim: 30.07.2023), İlgili kısım aynen: “Ayrıca belirtmek gerekir ki; meşru menfaat şartı, maddede yer alan diğer haller uygulanmadığı takdirde veri işlenmesi bakımından başvurulacak son çare

KVKK m. 5/ f. 2, f bendine dayanabilmek için üç şartın bir arada bulunması gerekir. Öncelikle veri sorumlusunun veri işlemeye yönelik meşru menfaati olmalıdır. İkinci aşamada, veri işleme faaliyeti ilgili kişinin temel hak ve özgürlüklerine zarar vermemelidir. Son olarak, bu veri işleme faaliyeti zorunlu olmalıdır. Bu üç şartın bir arada bulunması halinde bir veri işleme faaliyeti için KVKK m. 5/ f. 2, f bendine dayanılabilir.

İlk ele alacağımız unsur, veri sorumlusunun meşru menfaatinin olması unsurudur. Bu veri işleme şartına dayanmak isteyen veri sorumlusu öncelikle kendi meşru menfaatini tespit etmelidir. Veri sorumlusunun meşru menfaati ile kastedilen, veri işleme faaliyeti ile veri sorumlusunun elde edeceği faydadır.¹⁹² Bu fayda önemli, etkin, belirli ve mevcut¹⁹³ bir menfaatle ilgili olmalıdır.¹⁹⁴

Kişisel Verileri Koruma Kurulu, meşru menfaatin taşınması gereken özellikleri ele aldığı bir kararında meşru menfaatin çok sayıda kişiyi etkilemesi gerektiğini, sadece ekonomik menfaat edilmesine yönelik olmaması gerektiğini, bir işleyişi kolaylaştırması gerektiğini, şeffaf ve hesap verilebilir olması gerektiğini belirtmiştir.¹⁹⁵ Buradan hareketle veri sorumlusunun, veri işleme anında mevcut olmayan fakat ileride olması muhtemel olan bir sonuca yönelik veri işleme faaliyetini bu veri işleme şartına dayandıramayacağı söylenebilir.¹⁹⁶

Meşru menfaat, somut olayın özelliklerine göre tespit edilmesi gereken bir unsurdur. Meşru menfaat, niteliksel olarak hukuksal, ekonomik ya da sosyal nitelikte olabilir.¹⁹⁷ Hukuka aykırı olmadığı sürece her türlü menfaatin bu kapsamda ele alınmasının önünde bir engel bulunmamaktadır.¹⁹⁸ Öte yandan, yukarıda değindiğimiz

olmadığı gibi her şeyi kapsamına dâhil edebilecek ve tüm kişisel verilerin işlenmesine ilişkin faaliyetleri kanuna uygun hale getirecek bir düzenleme de değildir” şeklindedir.

¹⁹² Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları No: 01, Aralık 2019, Ankara, s. 78

¹⁹³ Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları No: 03, Aralık 2019, Ankara, s. 43, (www.kvkk.gov.tr), (Erişim: 01.08.2023)

¹⁹⁴ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 13, (www.kvkk.gov.tr), (Erişim: 01.08.2023)

¹⁹⁵ “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 01.08.2023)

¹⁹⁶ GÜNAL/ ÜSTÜN, s. 11.

¹⁹⁷ Murat ALTINDERE, **Kişisel Verilerin Korunması Hukuku ve Uygulaması**. 1.Basım. Ankara, Adalet Yayınevi, s. 47-51

¹⁹⁸ Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 Nisan 2014, s. 24-29

karar uyarınca Kişisel Verileri Koruma Kurulu, yalnızca ekonomik menfaatin meşru menfaat kapsamında ele alınamayacağını ifade etmiştir.

İkinci ele alacağımız şart, ilgili kişinin temel hak ve özgürlüklerine zarar vermeme şartıdır. Bu şarta uygunluğun kontrolü açısından veri sorumlusunun öncelikle ilgili kişinin sürece ilişkin temel hak ve özgürlüklerinin kapsamını belirlemesi gerekir.¹⁹⁹ Zira veri sorumlusu, buna göre zarar verip vermeyeceğini tartabilecektir. Sonrasında, daha önce tespit etmiş olduğu, veriyi işlemekteki meşru menfaatini terazinin diğer ucuna yerleştirecektir. En son aşamada da ilgili kişiye dair tespit ettiği temel hak ve özgürlükler ile kendi menfaatini yarıştırmalı, bir denge testi yapmalıdır. Bu testte veri sorumlusunun aradığı, orantılı bir dengedir. Somut olayın özelliğine göre bu denge değişiklik gösterebilecektir.

Kişisel Verileri Koruma Kurulu’nun 30.09.2021 tarihli kararı, denge testinin nasıl yapılması gerektiği noktasında önemli tespitleri içermektedir.²⁰⁰ Kararda kişilik hakkı ve ifade özgürlüğü hakkı, “kamu ilgi ve yararı taşıması”, “gerçek ve güncel olma” ve “öz ve biçim arasındaki denge” kriterleri bağlamında kıyaslanmış ve karara konu olay açısından kişilik hakkının daha üstün tutulması gerektiğine kanaat getirilmiştir.

İlgili kişinin temel hak ve özgürlükleri ile veri sorumlusunun meşru menfaati yarışabilir düzeyde olmalıdır. Uygulamada genellikle yarıştırılan iki unsur, ilgili kişinin özel hayatına ve kişisel verilerinin korunmasına saygı hakkı ile veri sorumlusunun ekonomik menfaatidir. Burada yapılması gereken bir denge testidir.

¹⁹⁹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 14, (www.kvkk.gov.tr), (Erişim: 01.08.2023)

²⁰⁰ “İlgili kişiye ait görselin, açık rızası alınmaksızın bir internet sitesinde yer alan haber içeriğinde kullanılması” hakkında Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli 2021/989 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 01.08.2023), kararın ilgili kısmı aynen “*Kamu yararının tespitinde, haberin kişilerin merak duygularına mı yoksa yüksek ahlaki ve hukuki değerlerin korunmasına mı hizmet ettiğinin değerlendirilmesi gerektiği, örneğin; yasa dışı uygulamaların, rüşvet ve yolsuzlukların kamuoyuna iletilmesinde, eleştirilmesinde kamu yararı bulunduğu, öte yandan, kamu ilgi ve yararı kriteri kapsamında siyasetçiler ve kamu görevlilerine dair yapılan haberler bakımından basın özgürlüğüne yapılan sınırlamaların daha dar yorumlanması uygun olacağı, öte yandan, haberin gerçek ve güncel olmasının ikinci kriter olduğu, gerçeklik unsurunun, somut gerçeğe değil, olayın, haberin verildiği andaki belirli biçimine uygunluk olarak anlaşılması gerektiği, Haberin güncel olmasının ise somut olayın açıklandığı tarihlerde kamu yararının bulunması esasına dayandığı, üzerinden süre geçmiş ve açıklanmasında artık kamu yararı bulunmayan bir olayın yayımlanmasında haber verme hakkından söz edilemeyeceğinden hareketle kişilik hakkına üstünlük tanınması gerekeceği*” şeklindedir.

Denge testi ile kastedilen, ilgili kişinin menfaatinin veri sorumlusunun menfaatinden daha üstün olup olmadığının tartılmasıdır. Şayet bu teste göre, terazi ilgili kişinin menfaatinden yana ağır basıyor ise artık bu veri işleme şartına dayanılması mümkün değildir. Menfaatlerin yarışır düzeyde olması, yani neredeyse eşdeğer olması ya da veri sorumlusunun menfaatinin ilgili kişinin menfaatinden daha ağır basması gerekmektedir.²⁰¹ Örneğin bir şirketin, çalışanlarının terfilerini belirlemek üzere performans değerlendirme raporlarını arşivlemesi ve yıl sonunda analiz etmesi bu kapsamda değerlendirilebilir.²⁰²

Ele alacağımız son unsur ise zorunluluk unsurudur. Uygulamada bu ilkeye dayanmak isteyen veri sorumlularını en çok zorlayan nokta zorunluluk kriteridir. Buna göre bir veri işleme faaliyeti, ilgili kişinin temel hak ve özgürlüklerine zarar vermiyor olabilir; veri sorumlusunun meşru bir menfaatine de yönelik olabilir ancak o menfaatin gerçekleşmesi için ilgili kişisel verinin işlenmesi zorunlu değilse artık bu veri işleme şartına dayanılması mümkün değildir. Daha farklı bir anlatımla, veri sorumlusu menfaatine ulaşmak için ilgili kişisel veriye o kadar ihtiyaç duymalıdır ki, o kişisel veriyi işlemezse menfaatine ulaşamamalıdır. Örneğin veri sorumlusunun meşru menfaatini karşılamak için ilgili kişinin adı soyadı ve telefon numarası yeterliyken bir de ilgili kişinin evinin adresi talep ediliyor ise adres verisi açısından bu şarta dayanılması mümkün değildir. Zira ilk iki veri zorunlu iken üçüncü veri zorunlu değildir.

Veri işleme şartını daha iyi kavrayabilmek adına Kişisel Verileri Koruma Kurumu'nun konuya yaklaşımını da ele almak gerekmektedir. Meşru menfaat veri işleme şartına ilişkin Kurum tarafından verilen bazı örnekler, bir işletmenin devri halinde devralacak kişinin mevcut şirket personellerinin kişisel verilerini incelemesi,²⁰³ çalışan bağlılığını arttıran ödül ve prim uygulaması amacıyla işçinin kişisel verilerinin işlenmesi²⁰⁴ şeklindedir.

²⁰¹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 14, (www.kvkk.gov.tr), (Erişim: 03.08.2023)

²⁰² Kişisel Verileri Koruma Kurumu, **Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, KVKK Yayınları, Mart 2019, Ankara, s. 20, (www.kvkk.gov.tr), (Erişim: 03.08.2023)

²⁰³ Kişisel Verileri Koruma, **Örneklerle Kişisel Verilerin Korunması**, KVKK Yayınları No: 29, Ankara, Haziran 2019, s. 17, (www.kvkk.gov.tr), (Erişim: 03.08.2023)

²⁰⁴ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin İşlenme Şartları**, s. 4, (www.kvkk.gov.tr), (Erişim: 03.08.2023)

Son olarak Kişisel Verileri Koruma Kurulu'nun vermiş olduğu meşru menfaat veri işleme şartının konu edildiği bazı kararları ele alacağız. Kişisel Verileri Koruma Kurulu'nun 11.02.2020 tarihli kararına²⁰⁵ konu olayda ilgili kişi, yeni çalışmaya başladığı şirkete, gerçeğe aykırı bir şekilde son çalıştığı pozisyonu “Etik Direktör” olarak beyan etmiştir. İlgili kişi, yeni şirkette çalışmaya başlamış ve şirket tarafından ilgili kişinin bünyelerinde çalışmaya başladığına ilişkin bir duyuru yayınlanmıştır. Duyuruda ilgili kişinin eskiden “Etik Direktör” olarak çalıştığı bilgisine yer verilmiştir. Bu duyuruyu gören eski şirket ise ilgili kişinin çalışmaya başladığı şirkete e-posta göndererek ilgili kişinin şirketlerinde hangi tarihler arasında hangi pozisyonda çalıştığına ilişkin bilgileri iletmiştir. E-postayı alan son şirket, ilgili kişinin işten ayrılış nedenini eski şirkete sormuş ve cevaben ilgili kişinin ailevi nedenlerden dolayı yurtdışına taşınacağı bilgisini edinmiştir. İlgili kişi de bu veri akış sürecinin, kendisinin açık rızası olmadan gerçekleştirilmesinin KVKK'ye aykırı olduğu düşüncesi ile konuyu Kurul'un önüne taşımıştır. Kurul yaptığı değerlendirmede veri akışının veri sorumlusunun insan kaynakları departmanı ile yeni şirketin insan kaynakları departmanları arasında olduğu, ilgili kişinin hem eski işvereni hem de yeni işvereni verdiği yanlış bilgiler yanılmış olduğu, veri sorumlusunun bu bilgilerde düzeltme yapılması talebinin makul olduğu, bu talebinin ilgili kişinin temel hak ve özgürlüklerine zarar verecek düzeyde olmadığı, şirket itibarının korunması gerektiği hususlarını gözeterek ilgili veri akış sürecinin meşru menfaat veri işleme şartına dayandığını tespit etmiştir.

Kurul'un bir başka kararına konu olayda ise²⁰⁶ veri sorumlusu bir araç kiralama şirketi, ilgili kişi ise bu şirketin müşterisidir. Taraflar arasındaki sözleşme uyarınca

²⁰⁵ “Veri sorumlusu sağlık firması tarafından eski çalışanı olan ilgili kişinin kişisel verilerinin rızası alınmaksızın aktarımı” hakkında Kişisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 03.08.2023); Kararın ilgili kısmı aynen “*Şikâyeteye konu kişisel veri işleme faaliyetinin hem kişisel verilerin korunması hem de iş mevzuatının ilgili maddelerine aykırılık teşkil etmediği, veri sorumlusu tarafından gerçeği yansıtmayan bilginin düzeltilmesi, şirket itibarının korunması, şirket adı kullanılarak yanlış bilgi üzerinden menfaat temin edilmesinin önlenmesi, ilerde oluşabilecek hukuki etkilerinin ortadan kaldırılması, iş yaşamında dürüstlük ve etik ilkelerin teşvik edilmesi amacıyla gerçekleştirildiği belirtilen söz konusu veri aktarımının Kanunun “Kişisel verilerin işleme şartları” başlıklı 5 inci maddesinin (2) numaralı fıkrasının (f) bendi uyarınca “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işleminin zorunlu olması” kişisel veri işleme şartına dayandığı, bu kapsamda Kanunun “Kişisel verilerin aktarılması” başlıklı 8 inci maddesi kapsamında söz konusu veri aktarımının hukuka aykırı bir veri işleme olmadığı sonucuna varıldığından veri sorumlusu hakkında herhangi bir müeyyide uygulanmasına yer olmadığına*” şeklindedir.

²⁰⁶ “İlgili kişinin kullanımına izin vermediği kredi kartı bilgilerinin veri sorumlusu araç kiralama şirketi tarafından kullanılması hakkında” Kişisel Verileri Koruma Kurulunun 27/02/2020 tarihli ve 2020/166 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 03.08.2023); Kararın ilgili kısmı aynen “*Aynı şekilde somut olayda, veri sorumlusunun mevcut durumda ön provizyon işlemi ile geçerliliğini ve limitini*

ilgili kiři tahsilat yapılması için sonu 22 ile biten bir kredi kartı bilgisini, veri sorumlusuna iletmiştir. Veri sorumlusu ise taraflar arasındaki sözleşme uyarınca HGS ücretinin tahsilatında yine ilgili kiřiye ait olan fakat sonu 67 ile biten başka bir kredi kartını kullanmıştır. Bu durumun kendi rızasına dayalı olmadan gerçekleştirilmesinden rahatsız olan ilgili kiři konuyu Kiřisel Verileri Koruma Kurulu'na taşımıştır. Veri sorumlusu, savunmasında özetle sonu 67 ile biten kredi kart numarasının, ilgili kiřinin veri sorumlusundan daha önce kiralamış olduđu bir araca ilişkin ücret tahsilat sürecinde kullanıldığını, bu nedenle daha önceden bu bilgiyi edinmiş olduklarını, řikayete konu veri işleme sürecinin meşru menfaat veri işleme şartına dayandığını ifade etmiştir.

Kurul kararında ilgili kiřinin tüketici konumunda olması sebebiyle hukuki ilişkinin zayıf tarafı olduğunu gözetmiş, belirtilen veri işleme faaliyetinin ilgili kiřinin makul beklentisi kapsamında olmadığını değerlendirmiş, durumun dürüstlük kuralına da uygun olmadığını tespit etmiş, veri sorumlusunun menfaati ile ilgili kiřinin temel hak ve özgürlüklerinin yarışabilir düzeyde olmadığını belirlemiş, ilgili kiřinin haberi olmadan başka bir kredi kartından çekim işlemi yapılmasının ve ileride doğabilecek ihtimallere istinaden ilgili kiřisel verilerin saklanması temel hak ve özgürlüklerine zarar verebileceđi kanaatine ulaşmıştır. Netice itibariye veri sorumlusuna idari yaptırım uygulanmıştır.

Kurul'un 22.07.2020 tarihli kararına²⁰⁷ konu olayda ise veri sorumlusu, müşterilerine toplu SMS gönderilebilmesi için bir řirket ile anlaşmış (veri işleyen) olup veri işleyen sunucuları Avrupa Birliđi üyesi bir ülkede bulunan ve bulut veri tabanı kullanan bir řirkettir. Veri sorumlusu, ilgili kiřinin kiřisel verilerini anlaştıđı firmaya aktarmakta ve bunun hukuki dayanađı olarak meşru menfaat veri işleme

onayladığı ilgili kiřinin sözleşme kapsamında kullanımına izin verdiđi kredi kartı bilgisine sahip olduđu ve ödemeyi bu kredi kartından tahsil edebileceđi halde daha önce elde ettiđi başka bir kredi kartı bilgisini kullanmaya çalışması ve ilgili kiřiye ait toplam üç kredi kartına ilişkin bilgilerin daha sonra kullanılabileceđi düşüncesiyle sisteminde saklaması faaliyetine ilişkin olarak; menfaatlerin yarışabilir olmadığı, kiřinin hem ilgili kiři hem de tüketici olarak zayıf konumda olan taraf olduđu, dolayısıyla temel hak ve hürriyetlerinin ihlale açık olduđu ve ileride söz konusu veri işleme faaliyetinden (haber verilmeksizin kredi kartından tahsilat/ çekim vb. yapılabilmesi suretiyle) zarar görebileceđi hususları dikkate alınarak yapılan değerlendirme ile, söz konusu veri işleme faaliyetinin "ilgili kiřinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" kiřisel veri işleme şartına dayandırılmasının da uygun olmadığı, söz konusu veri işlemenin açık rızaya veya diđer kiřisel veri işleme şartlarından herhangi birine dayandırılmayacađı ve hukuka aykırı bir veri işleme olduđu kanaatine varıldıđı" şeklindedir.

²⁰⁷ "Kiřisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında" Kiřisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/559 sayılı Karar Özeti, (www.kvkk.gov.tr), (Eriřim: 03.08.2023)

şartını öne sürmektedir. Kurul kararında veri sorumlusunun denge testi yapmadığından bahisle bu veri işleme şartına dayanamayacağı kanaatini belirtmiştir.

Kurul, 09.06.2021 tarihli kararında²⁰⁸ ise veri sorumlusunun reklam/pazarlama süreçlerine yönelik kişisel veri işleminin meşru menfaat veri işleme şartına dayandırılması halinde artık kişilerin, kişisel verileri üzerindeki denetim ve kontrol yetkisini kaybedebileceği riskinden bahsetmiş ve veri sorumlusunun hedeflediği meşru menfaati başka yollar ile de elde edebileceğinden bahisle veri işleme faaliyetinin zorunlu olmadığını, bu nedenle meşru menfaat veri işleme faaliyetine dayanılamayacağını belirtmiştir.

Kurul, 06.07.2021 tarihli kararında²⁰⁹ ise veri sorumlusunun, ilgili kişinin kişisel verilerinin silinmesi yönündeki talebini kabul etmesi halinde artık zorunluluk unsurunun gerçekleştiğinden bahsedilemeyeceğini ifade etmiştir. Ayrıca veri sorumlusunun meşru menfaatinin açık ve belirli olmadığı, veri sorumlusunun

²⁰⁸ “Sigortacılık ve bireysel emeklilik alanında faaliyet gösteren bir şirket tarafından ilgili kişiye ait kişisel verilerin hukuka aykırı olarak işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 09/06/2021 tarihli ve 2021/584 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 03.08.2023); Kararın ilgili kısmı aynen “*Veri sorumlusunun, faaliyetleri sonucunda ticari kazanç elde etmeyi amaçlayan ve sektördeki diğer tüm şirketler gibi faaliyet alanında meşru çalışmalar yürüten bir tüzel kişilik olduğu, söz konusu faaliyetlerin yürütülmesi sırasında şirketin var olma amaçlarından olan poliçe satış işleminin gerçekleştirilmesinin de şirketleri için meşru bir menfaat olması sebebiyle bu kapsamda gerçekleştirilen kişisel veri işleme faaliyetlerinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan “İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şartı kapsamında ilgili kişinin kişisel verilerinin işlendiğine ilişkin açıklamaları ile ilgili olarak ise, veri sorumlusu tarafından reklam ve pazarlama amacıyla kişisel verilerin meşru menfaat kapsamında işlenmesinin kişilerin kişisel verileri üzerindeki denetiminin sağlanmasını engelleyeceği, öte yandan poliçe satışının gerçekleştirilmesi için kişisel veri işlenmesinin bir zorunluluk olmadığı ve başka yollarla da ticari anlamda kazanç sağlanmasının mümkün olduğu, ilgili kişilerin bu şekilde ilgilendikleri veya ilgilenmedikleri alanlarda reklam ve pazarlama amacıyla aranma ve kısa mesaj almaya maruz bırakılmasının temel hak ve hürriyetlerinin zarar görmesine yol açacağı, sonuç olarak salt ekonomik fayda elde etmek amacıyla kişisel verilerin reklam, pazarlama ve bilgilendirme amacıyla işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendinde yer alan “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hükmü çerçevesinde değerlendirilemeyeceği” şeklindedir.*

²⁰⁹ “İlgili kişinin veri sorumlusu bankaya yaptığı iş başvurusunun olumsuz sonuçlanması sonrası kişisel verilerinin işlenmeye devam etmesi” hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarih ve 2021/670 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 05.08.2023); Kararın ilgili kısmı aynen “*Bu kapsamda, ilgili kişinin verilerinin tamamının silinmesi talebine karşın veri sorumlusunun bahse konu verileri ilk periyodik imhada dikkate alacağına yönelik açıklamasının veri sorumlusunun söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmediğinin bir göstergesi olduğu, kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olmadığı, ilgili kişinin verilerinin saklanması hususunda veri sorumlusunun meşru menfaatinin açık ve belirli olmadığı, veri sorumlusunun işleme faaliyetinden sağlaması beklenen yararın kişisel veri işlenmeksizin başkaca bir yol ve yöntemle elde edilebileceği ve söz konusu veri işleme faaliyetinin çok sayıda kişiyi etkileyecek şekilde kurumsal bir fayda sağlamadığı değerlendirildiğinden söz konusu kişisel verilerin işlenmesinde veri sorumlusunun meşru menfaatinin ilgili kişinin temel hak ve özgürlüklerine baskın gelmediği,*” şeklindedir.

hedeflediği meşru menfaate farklı yollar ile de ulaşabileceği, ilgili veri işleme faaliyetinin çok sayıda kişiyi etkileyecek düzeyde kurumsal bir menfaat sağlamadığı, bu nedenle de veri sorumlusunun meşru menfaatinin ilgili kişinin temel hak ve özgürlüklerine baskın gelmediği değerlendirilmelerine yer verilmiştir.

Son ele alacağımız karar ise Kurul'un 24.11.2022 tarihli kararıdır.²¹⁰ Karara konu olayda ilgili kişi, veri sorumlusu olan bir döviz bürosundan döviz alırken ilgili personelin hatası sebebiyle fazla miktarda döviz almıştır. Veri sorumlusu, ilgili kişinin aldığı fazla dövizini kendilerine iade etmesi için uzun bir süre beklediğini, ilgili kişinin döviz bürosuna geri gelmemesi üzerine veri sorumlusunun ilgili kişiye ulaşabileceği herhangi bir kişisel veriye sahip olmaması nedeniyle şikayete konu olaya ilişkin görüntüleri bir haber ajansı ile paylaştığını, bunun gerekçesinin ise şayet ilgili kişi iyi niyetli ise ilgili kişi hakkında bir suç duyurusunda bulunmadan sorunun sulh ile çözümlenmesini sağlamak olduğunu, temel maksadın ilgili kişiye ulaşmak olduğunu, paylaşılan videoda ilgili kişinin maske takması sebebiyle sadece gözleri ve çevresinin görüldüğünü ifade ederek savunmasını yapmıştır.

Uyuşmazlığa ilişkin Kişisel Verileri Koruma Kurulu tarafından yapılan inceleme uyarınca döviz bürosunun, ilgili kamera kayıtlarını haber ajansı ile paylaşmasında meşru menfaatinin bulunduğu, amacın fazla ödemenin iadesinin sağlanması olduğu, aksi durumda hatalı işlemi yapan veznedarın ekonomik anlamda mahvolacağı ve ilgili durumun veznedarın siciline işleneceği, ayrıca ilgili kişinin fiili kasten yapmış olma ihtimalinin bulunduğu, döviz bürosunun adli makamlara başvurmadan önce ilgili kişiye ulaşmak için tek yolunun bu olduğu zira elinde hiçbir kişisel veri bulunmadığı ve bu nedenle meşru menfaatinde bahsedilebileceği değerlendirilmiştir. İkinci aşamada ise ilgili kişinin görüntülerde yalnızca ve gözü ve göz çevresinin görüldüğü, bu görüntülerin tek başına ilgili kişiyi tanımlamaya yeterli olmayacağı ve bu sebeple de veri sorumlusunun meşru menfaati ile ilgili kişinin temel hak ve özgürlüklerinin yarışabilir nitelikte olduğu değerlendirilmiştir. Ayrıca döviz bürosunun elinde başkaca bir kişisel veri de bulunmadığından ilgili veri işleme

²¹⁰ “İlgili kişinin döviz bürosundaki güvenlik kamerası ile kayıt altına alınmış görüntülerinin haber ajansları ile paylaşılması” hakkında Kişisel Verileri Koruma Kurulunun 24/11/2022 tarihli ve 2022/1249 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 05.08.2023);

faaliyetinde zorunluluk unsurunun da gerçekleştiği belirtilmiştir. Netice itibariyle veri sorumlusu hakkında herhangi bir yaptırım uygulanmamıştır.²¹¹

Sonuç itibariyle Kişisel Verileri Koruma Kurulu önüne gelen uyuşmazlıklarda öncelikle veri sorumlusunun meşru menfaatinin tespit etmekte, ardından ilgili kişinin temel hak ve özgürlükleri ile meşru menfaatin yarışabilir düzeyde olup olmadığını ele almakta, son aşamada ise ilgili veri işleme faaliyetinin zorunlu olup olmadığını incelemektedir.

²¹¹ Kararın ilgili kısmı aynen “Hükümün uygulanabilmesinin iki aşamalı bir değerlendirme gerektirdiği, ilk değerlendirmede veri sorumlusunun meşru menfaatinin varlığının tespit edilmesinin gerektiği, somut olayda veri sorumlusunun, fazla ödeme yapılan ilgili kişinin tespit edilmesi amacıyla ilgili kişiye ait görüntü kayıtlarını üçüncü kişi/kurumlara aktarması suretiyle gerçekleşen eylemde menfaatinin bulunduğunu “1- İlgili kişiye yapılan fazla-haksız ödemenin iadesinin sağlanması 2- İlgili kişiye ulaşılamaması durumunda eksik kalan para bedelinin veznedardan tahsil edilmesi ve siciline işlemesi sebebiyle veznedarın ekonomik anlamda mahvına sebep olması” şeklinde izah ettiği, Söz konusu menfaatler açısından bir değerlendirme yapıldığında; fiilin kasten yapılmış olabileceği şüphesinin mevcut olduğu da göz önünde bulundurulduğunda suç soruşturmasına neden olabileceği için veri sorumlusunca makul ve normal şartlarda beklenen hareket tarzının adli mercilere başvuruda bulunmak şeklinde olduğunun düşünüldüğü, bununla birlikte döviz bozdurma işlemi sırasında müşterilerin adları ve soyadlarıyla işlem yapılmadığından ad-soyad-iletişim bilgisi gibi ilgili kişiye ait herhangi bir kişisel veriye sahip olmadığı ve yapılan fazla/haksız ödemenin iadesinin sağlanmasında tek yol olarak görüldüğü dikkate alındığında söz konusu aktarımın kişinin kendisinin geri dönüşünün sağlanabilmesi adına yararlı olacağı düşüncesiyle ilgili kişiye ait göz çevresinin ve silüetinin görüldüğü görüntülerin, kendinin tanyabileceği şekilde TV kanalına verilmesinde meşru olarak değerlendirilebilecek bir menfaatin varlığından söz edilebileceği, Bununla birlikte veri sorumlusunun elde edeceği faydanın; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek düzeyde etkin, belirli ve halihazırda mevcut olan bir menfaatinin ilişkin olması gerektiği, bu kapsamda menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar verip vermeyeceği yönünde yapılan ikinci değerlendirmede temel hak ve özgürlüklere konu olan kişisel verilerin korunması hakkına, ilgili kişinin şikâyetine ve aktarıma konu olan kamera kaydı görüntüleri incelendiğinde, ilgili kişinin maske takmasından dolayı gözünün, göz çevresinin ve silüetinin görünür olduğu görüntülerin, bir gerçek kişiyle ilişkilendirildiği ve ilgili kişiyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli olduğu için kuşkusuz kişisel veri niteliğini haiz olduğu, buna karşın ilgili kişinin yalnızca göz, göz çevresinin ve silüetinin görünür olduğu görüntülerle ilgili kişiyi tanımlamanın mümkün olmadığı, bu verilerin tek başına ilgili kişiyi belirlemeye imkân sağlayacak nitelikte de olmadığı, kişileri doğrudan değil ama dolaylı yoldan belirlenebilir kılan veriler açısından da kişisel veriden bahsedilmekle birlikte bunların ilgili kişilerin temel hak ve hürriyetleri açısından yaratacağı risklerin daha az olduğundan söz edilebileceği, somut görüntülerin değerlendirilmesinden de ilgili kişinin yalnızca göz, göz çevresi ve silüetinin yer aldığı görüntülerin tek başına ilgili kişiyi belirlemeye imkân sağlayacak nitelikte olmadığından hareketle yukarıda belirtilen menfaatin gerçekleştirilmesinin bahsi geçen görüntülerin aktarılması karşısında yarışabilir nitelikte olduğu, Bu itibarla veri sorumlusu tarafından ilgili kişiye yapılan fazla-haksız ödemenin iadesinin sağlanabilmesini ve kaybın önlenmesini teminen ilgili kişinin göz çevresinin ve silüetinin görüntülediği kamera kaydı görüntülerinin ilan amacıyla yerel haber kanalına aktarılmasının, ilgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte bir yarar sağladığı ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın elde edilmesinin mümkün olmayacağı, Bu çerçevede, meşru menfaatin ortaya koyulmasına ilişkin olarak yukarıda yer verilen kriterler esas alınarak yapılan değerlendirme sonucu; veri sorumlusu tarafından ilgili kişiye yapılan fazla-haksız ödemenin iadesini sağlamak ve ekonomik kaybın önlenmesini teminen ilgili kişinin göz çevresinin ve silüetinin görüntülediği kamera kaydı görüntülerini ilan amacıyla yerel haber kanalına aktarılmasının Kanun’un 5’inci maddesinin (2) numaralı fıkrasının (f) bendine göre, “İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” kapsamında olduğu” şeklindedir.

B-ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Özel nitelikli kişisel veriler, KVKK m. 6/ f. 1’de sınırlayıcı olarak sayılmıştır.²¹² KVKK m. 6/ f. 1 aynen “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.*” şeklindedir.

Özel nitelikli kişisel verilerin işlenme şartları açısından KVKK ikili bir ayrıma gitmiştir. KVKK m. 6/ f. 3 hükmü aynen “*Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*” şeklindedir. Açık hüküm uyarınca çalışmanın bu bölümünde özel nitelikli kişisel veriler, sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ile sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler olarak iki ayrı başlıkta ele alınacaktır.

1-Sağlık ve Cinsel Hayata İlişkin Özel Nitelikli Kişisel Veriler Bakımından

Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi için KVKK’de iki veri işleme şartı bulunmaktadır. Bunlardan birincisi KVKK m. 6/ f. 2 uyarınca ilgili kişinin açık rızasıdır. Açık rızaya ilişkin yaptığımız açıklamalar²¹³ özel nitelikli kişisel veriler açısından da aynen geçerli olduğundan bu başlık altında tekrara düşmemek için ayrıca incelenmeyecektir. İkinci veri işleme şartı “*Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.*” şeklindeki KVKK m. 6/ f. 3 hükmüdür.

KVKK m. 6/ f. 3’te yer alan veri işleme şartı temelinde iki unsur barındırmaktadır. Bunlardan birincisi amaç unsuru, ikincisi ise kişi unsurudur. Amaç

²¹² Kişisel Verileri Koruma Kurumu, **Özel Nitelikli Kişisel Verilerin İşlenme Şartları**, s. 1, (www.kvkk.gov.tr), (Erişim: 05.08.2023)

²¹³ Bkz: s. 58 vd.

unsuru uyarınca sağlık veya cinsel hayat verisinin açık rıza alınmaksızın işlenebilmesi için amaçların kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi olması gerekmektedir. Kişi unsuru uyarınca veriyi işleyecek kişi ya sır saklama yükümlülüğü altında bulunan kişi olmalı ya da yetkili kurum/kuruluş olmalıdır.

Sağlık ve cinsel hayat verisinin KVKK m. 6/ f. 3 uyarınca işlenmesine yönelik verilen en yaygın örnek, bir hekimin hastasının sağlık verilerini işlemesidir. Gerçekten de hem veriyi işleyen kişi bir doktor olduğundan sır saklama yükümlülüğü altında bulunan kişi olma unsuru sağlanmaktadır hem de doktorun sağlık verisi işlemekteki amacı tıbbî teşhis yapabilmek ve tedaviyi planlayabilmek olduğundan amaç unsuru sağlanmaktadır.

Kişisel Verileri Koruma Kurulu'nun bir kararına²¹⁴ konu olayda, doktor kontrolünde ilaç kullanan ilgili kişinin kişisel verilerinin izah olunan şartlar sağlanmadan işlenmesi hali için veri sorumlusu hakkında idari yaptırım uygulamıştır. Bu karara konu olay genellikle eczaneler nezdinde meydana gelmektedir. Özellikle MEDULA çıktılarının hukuki altyapı sağlanmadan paylaşılması, eczanelerin KVKK kapsamında en riskli olduğu alanlardır.

Kişisel Verileri Koruma Kurulu'nun bir başka kararında²¹⁵ ise veri sorumlusu bir spor salonu, ilgili kişi ise salonun müşterisidir. Kararda Kurul tarafından ilgili kişinin kan grubu bilgisinin sağlık verisi olduğu ve bu verinin spor salonu tarafından ancak açık rıza alınmak suretiyle işlenebileceği belirtilmiştir.

²¹⁴ “Sağlık verilerini Kanunun 6 ncı maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü bir kişiye aktaran veri sorumlusu hakkında” Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 05.08.2023)

²¹⁵ “Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu verisini ilgili kişinin açık rızasını almaksızın işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1357 sayılı Karar Özeti (www.kvkk.gov.tr), (Erişim: 05.08.2023), Kararın ilgili kısmı aynen “*Spor salonu üyeliği için özel nitelikli kişisel veri niteliğindeki kan grubu verisinin işlendiği ve bu işleme için açık rıza alınmadığı dikkate alındığında Kanun’un 12’nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, veri sorumlusunca işletilen spor salonunun üyelik sözleşmesi kapsamında çok sayıda üyenin kişisel verilerinin işlendiği, bunlar arasında özel nitelikli kişisel verilerin de bulunmasının kullanıcıların mahremiyeti açısından önemli bir risk arz ettiği, veri sorumlusunca ilgili kişi başvurusunun cevapsız bırakıldığı, ve spor salonu işletmeciliğinin yanı sıra turizm ve otel işletmeciliği ile inşaat taahhüt gibi birçok sektörde faaliyet gösteren veri sorumlusunun ekonomik durumu da dikkate alınarak Kanun’un 18’inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına*” şeklindedir.

Kişisel Verileri Koruma Kurulu’nun bir başka kararına²¹⁶ konu olayda, veri sorumlusu tarafından ilgili kişi olan işçiye yönelik uyuşturucu madde bağımlılığı testi yaptırılmış ve test sonuçları ilgili çalışanlar yerine şirketteki başka bir personele gönderilmiştir. Bu uygulama tek bir personel için değil bütün personelin test sonuçlarını kapsayacak şekilde gerçekleştirmiştir. Kurul kararında ilgili personelin sır saklama yükümlülüğü altında bulunan bir kişi olmadığı, bu nedenle de KVKK m. 6/ f. 3 hükmüne dayanılamayacağını belirtmiştir.²¹⁷ Bu karar son derece önemlidir. Zira anılan kararda olduğu kadar büyük bir hata yapılmasa da genellikle şirketlerde çalışanların sağlık süreci, insan kaynakları birimi tarafından yönetilmektedir. Öte yandan insan kaynakları personeli, sır saklama yükümlülüğü altında bulunan kişilerden oluşmamaktadır. Bu nedenle, bir şirketin insan kaynakları departman çalışanları, işçilerin sağlık verilerine yönelik veri işleme faaliyetinde bulunurken KVKK m. 6/ f. 3 veri işleme şartına dayanamaz.

Kişisel Verileri Koruma Kurulu’nun 04.08.2022 tarihli kararına²¹⁸ konu olayda ise bir kamu kurumu ile ilgili kişi arasında derdest bir idari dava bulunmaktadır. Davalı konumunda olan kamu kurumu, bir üniversite hastanesinden ilgili kişinin sağlık verilerini temin etmiş ve dava dosyasına sunmuştur. Olayda, üniversite hastanesi tarafından kamu kurumuna gönderilen bilgi ve belgeler arasında istirahat raporu, anamnez formları, epikriz raporları, konsültasyon formları, hasta medikal klinik seyir bilgileri, patoloji raporu, radyoloji raporları yer almaktadır. Kurul kararında, veri sorumlusu olan üniversite hastanesinde ilgili sağlık verilerinin talep edilmesi aşamasında “yürütülmekte olan bir İdari Davaya esas teşkil etmek üzere” ibaresine yer verildiği, oysa KVKK m. 6/ f. 3’te belirtilen veri işleme amaçları içerisinde bu

²¹⁶ “Özel nitelikli kişisel sağlık verisi niteliğindeki bağımlılık yapıcı madde testinin sonuçlarının ilgili kişilerin açık rızası alınmaksızın veri sorumlusu özel bir sağlık kuruluşu tarafından ilgili kişilerin işyerinde görevli üçüncü bir kişiye ait e-posta adresine gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 22/06/2022 tarihli ve 2022/594 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.08.2023)

²¹⁷ Kararın ilgili kısmı aynen “Şikâyeteye konu iddialara ilişkin olarak, veri sorumlusundan ve işverenden alınan cevap yazılarının incelenmesi neticesinde, “ilgili tarihte anılan üçüncü kişinin herhangi bir yetkisinin bulunmadığı, mağaza çalışanı olarak görev yaptığı” şeklindeki açıklamadan anlaşıldığı üzere veri sorumlusu tarafından ilgili kişiye ait özel nitelikli kişisel veri niteliğindeki test sonuçlarının gönderildiği üçüncü kişinin, Kanun’un 6’ncı maddesi kapsamında işveren bünyesinde çalışanların kişisel sağlık verilerini ilgili kişilerin açık rızası olmaksızın işleyebilecek sır saklama yükümlülüğü altında bulunan iş yeri hekimi olmadığı,” şeklindedir.

²¹⁸ “Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir davaya esas teşkil etmek üzere talebine binaen davalı kamu kurumuna aktarılması” hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/790 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 05.08.2023)

doğrultuda bir amaç bulunmadığından bahisle veri sorumlusu olan üniversite hastanesi hakkında idari yaptırım uygulamıştır.

Kişisel Verileri Koruma Kurulu’nun 02.04.2020 tarihli kararına konu olayda ise veri sorumlusu olan eğitim kurumu, öğrenciler üzerinde, zeka ve bilişsel yetkinlik, psikolojik sorunların olup olmadığı gibi sonuçların alınmasını yarayan CAS (Cognitive Assessment System) testini yapmıştır. Kurul kararında, veri sorumlusunun amacının KVKK m. 6/ f. 3’te belirtilen amaç ile örtüşmediğini ve bu nedenle açık rıza alınması gerektiğini tespit etmiştir.²¹⁹

Netice itibarıyla KVKK m. 6/ f. 3 veri işleme şartının sağlık ve cinsel hayata yönelik kişisel veriler açısından uygulama alanı bulabilmesi için öncelikle amacın maddede sayılan amaçlardan olması ve ilgili veriyi işleyen de sır saklama yükümlülüğü altında bulunan kişi veya yetkili kurum/kuruluş olması gerekmektedir.

2-Sağlık ve Cinsel Hayat Dışındaki Özel Nitelikli Kişisel Veriler Bakımından

Sağlık ve cinsel hayat dışındaki kişisel veriler, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir. Bu verilerin işlenebilmesi için KVKK’de iki veri işleme şartı bulunmaktadır. Bunlardan birincisi KVKK m. 6/ f. 2 uyarınca ilgili kişinin açık rızasıdır. Açık rızaya ilişkin yaptığımız açıklamalar²²⁰ özel nitelikli kişisel veriler açısından da aynen geçerli olduğundan bu başlık altında tekrara düşmemek için ayrıca incelenmeyecektir. İkinci veri işleme şartı ise “kanunlarda öngörülen hallerde” ilgili verilerin işlenmesidir.

Örneğin özel güvenlik görevlisi olabilmenin şartları Özel Güvenlik Hizmetlerine Dair Kanun’da düzenlenmiştir.²²¹ Kanunun 10. maddesine göre özel

²¹⁹ “Veri sorumlusu eğitim kurumu tarafından şikayetçinin çocuklarının özel nitelikli kişisel verilerinin hukuka aykırı olarak işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 02/04/2020 tarihli ve 2020/255 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 05.08.2023), Kararın ilgili kısmı aynen “*Bununla birlikte somut vakada, ilgili kişi öğrenciye CAS testinin uygulanması sonucunda, zekâ ve bilişsel becerilerin yanı sıra dikkat eksikliği ve hiperaktivite bozukluğu gibi öğrencinin ruh sağlığına ilişkin özel nitelikli kişisel verilerin de işlenmiş olduğu dikkate alındığında; Kanunun 6 ncı maddesinin (3) numaralı fıkrasında yer verilen “kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi” amaçları da bulunmadığından, veri sorumlusu tarafından söz konusu veri işleme faaliyetinin “açık rıza” şartına dayandırılması gerektiği sonucuna varılacağı*” şeklindedir.

²²⁰ Bkz: s. 58 vd.

²²¹ RG., 25504 S., 10.06.2004 T.

güvenlik olmak isteyen bir kişinin kasten işlenen bir suçtan dolayı bir yıl veya daha fazla süreyle hapis cezası almamış olması gerekir. Kanun açıkça bu şartı öngördüğünden, özel güvenlik görevlisi olarak çalışmak isteyen bir kişinin adli sicil kaydının özel güvenlik hizmetleri sunan bir veri sorumlusu tarafından işlenmesi bu kapsamda ele alınabilir.

Anayasa Mahkemesi'nin 10.03.2022 tarihli kararı²²², sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin işlenmesi açısından önemlidir. Mesai takibi amacıyla parmak izi uygulamasının uyumsuzluk konusu olduğu kararda Anayasa Mahkemesi, ilgili kişinin açık rızası olup olmadığını ve konuyla ilgili yasal bir düzenleme olup olmadığını değerlendirmiştir. Anayasa Mahkemesi, ilgili kişinin açık rıza göstermemiş olduğunu, konuyla ilgili de bir yasal düzenleme olmaması sebebiyle ilgili veri işleme faaliyetinin hukuka aykırı olduğunu tespit etmiş ve özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir.

Kanun koyucu, ilgili kişisel veri işleme şartını, KVKK m. 5/ f. 2, a bendinde düzenlenen “*Kanunlarda açıkça öngörülmesi*” veri işleme şartından farklı olarak KVKK m. 6/ f. 3'te “*Kanunlarda öngörülen haller*” şeklinde düzenlemiştir. Bu nedenle, belirtilen veri işleme şartının kanunlarda açıkça öngörülmeye nispeten daha geniş bir kapsamı ifade ettiği kanaatindeyiz.²²³ Yukarıdaki örneğimizde de Özel Güvenlik Hizmetlerine Dair Kanun açıkça ceza mahkumiyeti verisi işlenmesini düzenlememektedir. Öte yandan, bir özel güvenliğin belirtilen şekilde ceza mahkumiyeti almaması gerektiği düzenlemektedir. Hal böyle olunca, ilgili kanun aslında veri sorumlusuna güvenlik görevlisi olmak isteyen ilgili kişinin ceza mahkûmiyet bilgisini kontrol etme, adli sicil kaydını isteme hakkını dolaylı olarak tanımaktadır. Bu açıkça yazmamakla birlikte kanunda dolaylı olarak ifade edildiği için ve ilgili şart da “kanunlarda öngörülen haller” olduğu için KVKK m. 6/ f. 3'e dayanılması mümkündür.

²²² Anayasa Mahkemesi, Başvuru Numarası: 2018/11988, Karar Tarihi: 10.03.2022

²²³ Belirtmek gerekir ki Anayasa Mahkemesi, yukarıda bilgileri verilen kararında, kanunlar ile ayrıca ve açıkça bir düzenleme olup olmadığını değerlendirmiş, genel nitelikteki düzenlemelere itibar etmemiştir. Bu nedenle Anayasa Mahkemesi'nin yaklaşımı özel bir düzenleme olması gerektiği yönündedir. Kararın ilgili kısmı aynen “*Açıklamalar çerçevesinde, başvurucunun özel nitelikli kişisel verilerinin işlenmesine dair rızasının olmadığı, çalışanın mesaiye uyumunun kontrolünde biyometrik verilerin işlenmesinin ve kullanılmasının anılan kanunlar ile ayrıca ve açıkça öngörülmediği hususları dikkate alındığında başvuruya konu müdahalenin kanunilik şartını sağlamadığı sonucuna varılmıştır.*” şeklindedir.

İKİNCİ BÖLÜM

TÜRK TİCARET ŞİRKETLERİNİN 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ YÜKÜMLÜLÜKLERİ

Çalışmamızın bu bölümüne kadar genel olarak veri sorumlusu kavramını kullanmaya özen gösterdik. Veri sorumlusu, genellikle tüzel kişi olarak karşımıza çıkmaktadır. Tüzel kişi kapsamında ise en sık karşılaşılan veri sorumlusu, özel hukuk tüzel kişileridir.

Türkiye’de genellikle veri sorumlusu bir tüzel kişidir. KVKK’nin uygulama alanı bakımından bir kamu kurumu ile bir anonim şirket arasında hiçbir fark bulunmamaktadır. Öte yandan, ülkemizde kamu ile özel sektörün ihtiyaçları ve hareket mekanizması çok farklıdır. Bu nedenle çalışmanın bundan sonraki bölümünde veri sorumlusunun kapsamı Türk ticaret şirketleri²²⁴ ile sınırlandırılacak ve ülkemizdeki yaygın uygulamalar da bu bölümde ele alınacaktır.

I-AYDINLATMA YÜKÜMLÜLÜĞÜ

Veri sorumlusunun aydınlatma yükümlülüğü, “*Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.*” şeklindeki KVKK m. 10 hükmünden doğmaktadır. Aydınlatma, veri sorumlusu için bir yükümlülükken ilgili kişi açısından bir hak teşkil etmektedir.²²⁵ Aydınlatma yükümlülüğünü yerine getirmeyen veri

²²⁴ Ticaret şirketleri Türk Ticaret Kanunu’nun (TTK) 124. maddesinin birinci fıkrasında düzenlenmiştir. Maddeye göre kollektif, komandit, anonim, limited ve kooperatif şirketler, ticaret şirketleridir.

²²⁵ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Nisan 2019, Ankara, s. 3 (www.kvkk.gov.tr), (Erişim: 08.08.2023)

sorumluları hakkında KVKK m. 18/ f. 1, a bendi uyarınca idari para cezası yaptırımını uygulanabilmektedir.

En basit anlatımla aydınlatma yükümlülüğü, ilgili kişinin kişisel verilerinin işlenmesi sürecine ilişkin bilgilendirilmesini ifade etmektedir. Bu yükümlülüğün yerine getirilebilmesinde uyulacak usul ve esaslar son derece önemlidir. Aydınlatma yükümlülüğünün yerine getirilmesinde uyulacak usul ve esaslara ilişkin en önemli iki kaynak Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ²²⁶ ve Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi'dir. Bu bölümde Türk ticaret şirketlerinin aydınlatma yükümlülüğü, KVKK m. 10, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi ve Kurul kararları ışığında detaylıca ele alınacaktır.

A-Aydınlatma Yükümlülüğünü Yerine Getirecek Kişi

KVKK m. 10/ f. 1 hükmü öncelikle kişi unsurunu düzenlemektedir. Maddeye göre aydınlatma yükümlülüğünü yerine getirecek olan ya veri sorumlusu olmalıdır ya da veri sorumlusunun yetkilendirdiği bir kişi olmalıdır. Kişisel Verileri Koruma Kurulu bir kararında, burada veri sorumlusuna bir seçimlik hak tanındığını, aydınlatmayı ya veri sorumlusunun kendisinin yapabileceğini veya yetki verdiği bir kişinin yapabileceğini, hatta yetki verdiği kişinin veri işleyen dahi olabileceğini belirtmiştir.²²⁷

B-Aydınlatma Yükümlülüğünün Kapsamı

KVKK m. 10/ f. 1'de yer alan ikinci unsur, aydınlatma yükümlülüğünün kapsamıdır. Bu kapsam, KVKK m. 10 uyarınca veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki

²²⁶ RG., 30356 S., 10.03.2018 T.

²²⁷ “Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği”ne ilişkin Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 08.08.2023), Kararın ilgili kısmı aynen “Her ne kadar aydınlatma yükümlülüğü veri sorumlusuna ait olsa da veri işleyene verdiği talimatlar doğrultusunda veri işleyen tarafından da aydınlatma yükümlülüğünün yerine getirilebileceği değerlendirilmektedir. Nitekim, Kanunun 10 uncu maddesinde “kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi aracılığıyla” denilmek suretiyle veri sorumlusuna aydınlatma yükümlülüğü konusunda iki seçenek tanınmıştır. Diğer bir deyişle, aydınlatma yükümlülüğünün bizzat veri sorumlusu tarafından mı yoksa yetkilendireceği kişi tarafından mı yerine getirileceği konusunda Kanun, veri sorumlusuna seçim hakkı tanımıştır. Sonuç olarak; Kanunun 10 uncu maddesinde düzenlenen “aydınlatma yükümlülüğü” bizzat veri sorumlusu tarafından veya veri sorumlusunun yetkilendirdiği bir kişi tarafından yerine getirilebilir. Veri sorumlusu tarafından yetkilendirilen kişi de veri işleyen olabilir.” şeklindedir.

sebebi, ilgili kişinin 11 inci maddede sayılan diğer hakları aydınlatma şeklinde düzenlenmiştir. Ayrıca Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 4. maddesi de aydınlatma yükümlülüğünün kapsamını düzenlemektedir. Bu maddede belirtilen kapsam ile KVKK m. 10'da belirtilen kapsam birebir aynıdır. Burada dikkat edilmesi gereken önemli nokta, sayılan unsurların asgari unsurlar olmasıdır. Yani kanun koyucu diğer şartları sağlaması kaydıyla bu kapsamdaki bir aydınlatma faaliyetini yeterli kabul etmektedir. Maddede belirtilen unsurlar asgari unsurlar olduğundan veri sorumlusunun daha fazla bilgi vermesinin önünde de hiçbir engel yoktur. Örneğin bir anonim şirket, çalışan adayına yapacağı aydınlatmada adayın başvurusunun olumsuz değerlendirilmesi halinde süreç içerisinde elde ettiği kişisel verileri ne kadar süre sonra imha edeceğini belirtebilir. Görüleceği üzere, imhanın ne zaman yapılacağı hususu aydınlatma metinlerinde yer alması gereken bir zorunlu bir unsur değildir. Bununla birlikte, bu bilgiye aydınlatma metinlerinde yer verilmesinin önünde hiçbir engel bulunmamaktadır.

Aydınlatma yükümlülüğünü yerine getirmek isteyen veri sorumluları uygulamada "aydınlatma metni" isimli yazılı dokümanları tercih etmektedir. Bunun sebebi, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/ f. 1, e bendinde yer alan "*Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.*" düzenlemesidir.²²⁸ Veri sorumlusu hem aydınlatmayı yapmalı hem de bunu ispat edebilir pozisyonda olmalıdır. Bunun en güvenilir yolu da ilgili kişiden aydınlatıldığına dair bir imza almaktır. Ayrıca çağrı merkezi kayıtları, dijital kayıtlar da önemli ispat vasıtalarıdır.

Aydınlatma yükümlülüğünün ispatında kullanılacak ispat vasıtaları açısından bir sınırlama söz konusu değildir. Nitekim Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5 / f. 1 hükmünün ilgili kısmı aynen "*Veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi esnasında aşağıda sayılan usul ve esaslara uyulması gerekmektedir*" şeklindedir. Maddede "gibi" ibaresine yer verildiğinden bu ispat vasıtalarının çoğaltılabileceği anlaşılmaktadır. Önemli olan veri

²²⁸ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 7 (www.kvkk.gov.tr), (Erişim: 08.08.2023)

sorumlusunun bir vesileyle aydınlatma yükümlülüğünü yerine getirdiğini ispat edebilmesidir.

Aydınlatma yükümlülüğü yerine getirilirken ilk dikkat edilmesi gereken husus ilgili kişiye, veri sorumlusunun ve varsa temsilcisinin kimliğinin bildirilmesidir. Örneğin Türkiye’de kurulmuş bir limited şirketin aydınlatma metninde ticari unvanını belirtmesi gerekmektedir. Bu bilgilendirme, birazdan anlatılacak olan²²⁹ ilgili kişinin haklarının kullanabilmesi açısından da önemlidir. Ayrıca, telefon numarası, e-posta adresi, adres bilgisi şeklindeki bilgiler de açıklanmalıdır.²³⁰

Kapsamda yer alan ikinci önemli nokta, kişisel verilerin hangi amaçla işlenebileceğidir. Amaç ile kastedilen, veri sorumlusunun kişisel veriye neden ihtiyaç duyduğudur. Örneğin gıda sektöründe yer alan bir şirketin, müşterilerinin şikayetlerini ad, soyad, telefon numarası ve şikayet konusu başlıkları altında kategorize ederek kayıt altına aldığını varsayalım. Burada şirketin ilgili kişiye belirtmesi gereken amaçlardan birisi “talep ve şikayetlerin takibi ve neticelendirilmesi” olabilir.

Kişisel verilerin hangi amaçla işlenebileceği açıklanırken ileride doğması muhtemel amaçlara yer verilmemeli, muğlak ifadeler kullanılmamalıdır. Nitekim Kişisel Verileri Koruma Kurulu, Türkiye Cumhuriyeti Ziraat Bankası Anonim Şirketi hakkında verdiği bir kararında, ileride gerçekleşmesi muhtemel durumlar için kişisel verilerin işlenemeyeceği ve aydınlatmanın da bu şekilde yapılamayacağı hususunun altını çizmiştir.²³¹ Uygulamada, aydınlatma metinlerinde karşılaşılan en büyük hata “gibi amaçlar”, “sair amaçlar” şeklindeki kapsamı geniş tutabilecek yuvarlak ifadelerin tercih edilmesidir. Kişisel Verileri Koruma Kurulu’nun bu konuya yaklaşımı

²²⁹ Bkz: s. 132 vd.

²³⁰ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 9 (www.kvkk.gov.tr), (Erişim: 08.08.2023)

²³¹ “İlgili kişinin yaptığı başvuruyu cevaplandırmayan ve internet sitesi üzerinden yayımladığı aydınlatma metni mevzuatta düzenlenen şartları taşımayan T.C. Ziraat Bankası A.Ş. hakkında” Kişisel Verileri Koruma Kurulunun 02/05/2019 tarihli ve 2019/122 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 08.08.2023), kararın ilgili kısmı aynen “*Bankanın internet sitesinde yer alan aydınlatma metninde, Bankanın kişisel veri işleme amaçlarının, ilgili kişilerin kişisel verilerinin Kanunun 5 inci ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğine yönelik hukuki sebep açıkça belirtilmeksizin sıralandığı; kişisel veri işleme amaçları sıralandıktan sonra metin içerisinde yer verilen “gibi amaçlar kapsamında işlenmektedir” ifadesinin ise, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandırır nitelikte olduğu; bu çerçevede söz konusu aydınlatma metninin “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”in (Tebliğ) 5 inci maddesinin birinci fıkrasının (g) ve (h) bentlerinde yer verilen hükümlere uygun hazırlanmaması nedeniyle, Bankanın internet sitesinde yer alan aydınlatma metninin yeniden gözden geçirilerek Tebliğ hükümlerine uygun hale getirilmesi yönünde talimatlandırılmasına karar verilmiştir.*” şeklindedir.

çok net olup aydınlatma metinlerinde muhakkak sade, açık ve net bir dil kullanılması gerekmektedir.

Ele alacağımız üçüncü unsur, kişisel verilerin kimlere ve hangi amaçla aktarılabileceğidir. Kişisel verilerin yurtiçinde aktarılması KVKK m. 8’de, kişisel verilerin yurt dışına aktarılması ise KVKK m. 9’da düzenlenmiştir. Bu nedenle, veri sorumluları aydınlatma yaparken bu maddelere uygun olarak hareket etmek zorundadır.²³² Ayrıca, kişisel verilerin kimlere aktarılacağına da belirtilmesi gerekmektedir.

Uygulamada karşılaşılan tereddütlerden birisi, alıcının açık kimliğinin belirtilmesinin gerekip gerekmediğidir. Hemen belirtmek gerekir ki önemli olan kategorik olacak şekilde alıcı grubunun belirtilmesidir. Yani çalışanlarının maaş ödemesini yapmak isteyen bir tekstil şirketi, X bankası ile çalışıyorsa ve bu bağlamda işçilerinin kişisel verilerini aktarıyor ise X bankasının ticari unvanını belirtmesine gerek yoktur. Önemli olan ilgili kişinin, bilgilerinin bir banka ile paylaşıldığını bilmesidir. Hatta VERBİS’te yer alan alıcı grupları incelendiğinde, yetkili kamu kurum ve kuruluşları, tedarikçiler gibi çok kapsayıcı isimler kullanıldığı görülmektedir. Netice itibarıyla veri sorumlusu, kişisel veriyi aktaracağı alıcının ticari unvanını ilgili kişiyle paylaşabilir. Bu noktada bir engel bulunmamaktadır ancak bahsedilen yaklaşım, veri sorumlusunun tercihinin dayalı olup veri sorumlusu aydınlatma metninde alıcının ticari unvanını yazmak zorunda değildir.

Kapsamda yer alan dördüncü unsur ise kişisel veri toplamanın yöntemi ve hukuki sebebidir. Maddede yer alan “hukuki sebep” ifadesinden ne anlaşılması gerektiği Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/ f. 1, h bendinde düzenlenmiş olup aynen “*Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep” ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir.*” şeklindedir.

²³² Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 10, (www.kvkk.gov.tr), (Erişim: 08.08.2023)

Burada dikkat edilmesi gereken iki önemli nokta vardır. Birincisi, veri sorumlusu veriyi tamamen/kısmen otomatik yollar mı topladığını ya da otomatik olmayan yöntemler ile mi topladığını belirtmelidir. Verinin toplandığı araç bir form, telefon görüşmesi ya da kamera kaydı olabilir.²³³ Aracın tercihi, veri sorumlusuna ait olup önemli olan veri toplama yönteminin ilgili kişiye izah edilmesidir.

İkinci önemli nokta ise işlenecek olan kişisel veri için KVKK m. 5 veya KVKK m. 6'da düzenlenen veri işleme şartlarından hangisine dayanıldığının açık bir şekilde belirtilmesi gerektiğidir. Kişisel Verileri Koruma Kurulu konuyla ilgili bir kararında, veri sorumlusunun aydınlatma metninden KVKK m. 5'te düzenlenen açık rıza şartına mı dayanıldığı yoksa yasal yükümlülüklerin yerine getirilmesi şartına mı dayanıldığının tam olarak anlaşılamadığından ve ayrıca hangi verilerin açık rıza hangi verilerin ise yasal yükümlülüklerin yerine getirilmesi kapsamında olduğunun anlaşılamadığından bahisle veri sorumlusu olan şirketin talimatlandırılmasına karar vermiştir.²³⁴ Dolayısıyla aydınlatma yapılırken hangi kişisel verinin hangi maddeye dayanarak işlendiğinin rahatlıkla anlaşılabilir bir şekilde belirtilmesi gerekmektedir. Kafa karıştırıcı, muğlak ifadelerle yer verilmemelidir. Nitekim Kişisel Verileri Koruma

²³³ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 11, (www.kvkk.gov.tr), (Erişim: 08.08.2023)

²³⁴ “Veri sorumlusunun, web sitesinde kişisel verilerin işlenmesini hizmet şartı olarak talep ettiği ve aydınlatma yükümlülüğünü usulüne uygun yerine getirmediği iddiaları hakkında” Kişisel Verileri Koruma Kurulunun 08/07/2019 tarih ve 2019/206 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 08.08.2023), Kararın ilgili kısmı aynen “İhbara konu web adresi üzerinden erişim sağlanan ‘GİZLİLİK ve KVK Politikamız’ başlıklı metin, söz konusu mevzuat düzenlemeleri çerçevesinde incelendiğinde; Web sitesinin ilgili kişiler hakkında işlediği ad, soyadı, doğum tarihi, cep telefonu numarası, e-posta, cinsiyet, adres, sosyal medya hesaplarıyla bağlanması durumunda üyenin o kanallar aracılığıyla paylaşılmasına onay verdiği bilgilerin, üyenin tüm alışveriş bilgilerinin, yani hangi üye işyeri, alışveriş noktası ve zamanı, ne kadar ödeme yaptığı, hangi kampanyadan faydalandığı, aldığı indirim tutarı, alışverişindeki ürün bilgileri, uygulama üzerindeki gezinme ve tıklama bilgilerinin, uygulamayı açtığı lokasyon bilgilerinin, ‘ilgili mevzuat’tan kaynaklanan yasal yükümlülük çerçevesinde mi yoksa ilgili kişilerin açık rızalarına istinaden mi işlendiğinin ya da söz konusu kişisel verilerin hangilerinin ‘ilgili mevzuat’tan kaynaklanan yasal yükümlülük çerçevesinde hangilerinin ise ilgili kişilerin açık rızalarına istinaden işlendiğinin açıkça belirtilmemiş olduğu” şeklindedir.

Kurulu'nun 05.04.2021 tarihli kararı²³⁵ ve 20.04.2021 tarihli kararı²³⁶ da aynı doğrultudadır. Netice itibariyle, veri sorumlusu hangi kişisel veriyi hangi veri işleme şartına dayandırarak işleyeceğini açık ve sade bir şekilde izah etmelidir. Aydınlatma metninden, KVKK m. 5'te veya KVKK m. 6'da belirtilen veri işleme şartlarından hangisine dayanıldığı rahat bir şekilde anlaşılmalıdır.

Kapsamda ele alacağımız son unsur ise ilgili kişinin Kanunun 11'inci maddesinde sayılan diğer haklarıdır. Uygulamada genellikle veri sorumluları tarafından KVKK m. 11 hükmünün tamamına aydınlatma metninde yer verilmektedir. Bununla birlikte maddeye atıf yapmak suretiyle de bu şartın yerine getirilmesi mümkündür. Nitekim Kişisel Verileri Koruma Kurumu da bir rehberinde, KVKK'ye uygun bir aydınlatma metni olarak örneğini verdiği metinde “*Kanunun ilgili kişinin haklarını düzenleyen 11. maddesi kapsamındaki taleplerinizi*” şeklinde bir ifadeye vermiştir.²³⁷ Dolayısıyla maddeye atıf yapılması da yeterli kabul edilmektedir.

²³⁵ “Bir sigorta şirketi tarafından işlenen kişisel verilerin üçüncü kişiye aktarılması ve ilgili kişiye veri aktarımına ilişkin aydınlatma yapılmaması” hakkında Kişisel Verileri Koruma Kurulunun 05/04/2021 tarih ve 2021/333 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 08.08.2023), Kararın ilgili kısmı aynen “İlgili kişiye kişisel verisinin aktarımına ilişkin aydınlatma yapılmadığı iddiasına ilişkin olarak aydınlatma metni incelendiğinde; “Kişisel Verilerinizin Kimlere ve Hangi Amaçla Aktarılabileceği” bölümünde yer alan “*Kişisel Verilerin İşlenme Amaçları*” başlığı altında “sayılan amaçlarla ve bunlarla sınırlı olmamak üzere kişisel verilerin aktarılabileceğinin” belirtildiği tespit edilmiş olup söz konusu ibarenin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin (Tebliğ) 5 inci maddesinin (1) numaralı fıkrasının (g) bendinde yer alan; “Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmemelidir.” hükmüne aykırı olduğu; ayrıca “*Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi*” başlığı altında hangi kişisel verinin hangi veri işleme şartına dayanılarak işlendiğinin açıkça ortaya konulmadığı, bununla birlikte veri sorumlusunca daha sonra internet sitelerinde yayımlanan aydınlatma metninin güncellendiği ancak hangi kişisel verinin hangi veri işleme şartına dayanılarak işlendiğinin hala net olarak ortaya konulmadığı,” şeklindedir.

²³⁶ “Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbar” ile ilgili olarak Kişisel Verileri Koruma Kurulunun 20/04/2021 tarihli ve 2021/389 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 08.08.2023), Kararın bir bölümünde “Bununla birlikte, mezkûr metnin “*C-Kişisel Verilerinizi Kimlere ve Hangi Amaçla Aktarıyoruz?*” başlığı altında geçen “sigortacılık ve sair mevzuat” ibaresinin muğlak olduğu, zira kişisel verilerin aktarımı hangi mevzuat kapsamında gerçekleştiriliyor ise ayrı ayrı açıkça belirtilmesi gerektiği, ayrıca metinde yer alan kurum ve kuruluşların isimlerinin de güncellenmediğinin anlaşıldığı,” şeklinde değerlendirmede bulunulmuş, “sigortacılık ve sair mevzuat” şeklindeki kapsamın muğlak olduğu ifade edilmiş ve ayrıca başka bir bölümde “Metnin devamında kişisel verileriniz, “6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde sadece sigortacılık faaliyetlerinin yürütülmesi amacı ile ve bu amacın gerektirdiği yasal sürelerle sınırlı olarak işlenmektedir.” şeklinde açıklama yapıldığı, ancak Tebliğin 5 inci maddesinin birinci fıkrasının (h) bendinde de düzenlendiği üzere, Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan “hukuki sebep”ten kastın, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiği olduğu, bu anlamda hukuki sebep olarak Kanunda düzenlenen 5 inci veya 6 ncı maddelerden hangisine veya hangilerine dayanıldığına ilişkin bir bilgilendirmede bulunulmadığının anlaşıldığı,” şeklinde değerlendirmelerde bulunulmuştur.

²³⁷ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, Nisan 2019, s. 18, (www.kvkk.gov.tr), (Erişim: 08.08.2023)

C-Aydınlatma Yükümlülüğünün Yerine Getirileceği Zaman

Veri sorumlularının aydınlatma yükümlülüğüyle ilgili dikkat etmesi gereken bir diğer nokta ise bunu ne zaman yapması gerektiğidir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 4/ f. 1 düzenlemesinin ilgili kısmı “*Kanunun 10 uncu maddesine göre; kişisel verilerin elde edilmesi sırasında*” şeklindedir. Öte yandan, 6. maddede ise kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğünün usul ve esasları düzenlenmektedir. Buradan hareketle, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmesi gereken zamanın belirlenmesinde veriyi ilgili kişiden mi aldığı yoksa başka bir kişiden mi aldığı hususunun önem arz ettiği söylenebilir.

Şayet kişisel veri ilgili kişiden elde ediniyor ise Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 4/ f. 1 hükmü uyarınca aydınlatmanın yapılacağı zaman, kişisel verilerin elde edilmesi anıdır. Kanaatimizce burada önem arz eden, veri sorumlusunun kişisel veriyi işlemeye başlamadan önce herhangi bir zaman diliminde aydınlatmayı yapması ve ilgili kişinin de bu aydınlatma durumundan haberdar olmasıdır. Örneğin özel güvenlik hizmeti sunan bir şirketin çalışan adaylarına yönelik talep ettiği kişisel veriler her çalışan adayı açısından aynı olduğundan ilgili şirketin web sitesinde herkesin erişimine açık bir şekilde çalışan adayı aydınlatma metnini yayınlaması ve bunun da adayların bilgisine sunulması halinde, diğer koşulları sağlaması şartıyla ilgili kişinin aydınlatıldığından bahsedilmesi mümkündür. Bu durum veri sorumlusunun aydınlatma yükümlülüğünü yerine getirdiğinin ispatında zorluk teşkil etse de bu yöntemin tercihinin önünde bir engel bulunmamaktadır.

Kişisel verilerin ilgili kişiden elde edilmemesi halinde ise aydınlatmanın yapılacağı zaman farklılık arz etmektedir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 6, bu durumu düzenlemektedir. Maddeye göre aydınlatma yükümlülüğü, kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde ya da kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında veya kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada yerine getirilmelidir. Burada üç farklı zaman dilimi belirtilmektedir. Maddenin a bendi genel, b ve c bentleri ise özel iki durumu düzenlemektedir. Maddenin a bendi uyarınca aydınlatmanın yapılacağı zaman, kişisel

verilerin elde edilmesinden itibaren makul bir süredir. Örneğin, ürünleri yüksek oranda hediye amaçlı sipariş edilen bir şirket, çoğu durumda işleyeceği kişisel verileri üçüncü bir kişiden almaktadır. Bu pozisyonadaki bir şirketin aydınlatma yükümlülüğünü yerine getireceği an kanaatimizce ürünün teslim edildiği andır. Zira daha öncesinde ilgili kişi aydınlatılır ise hediye siparişinde ilgili şirket bir daha tercih edilemeyecektir çünkü sürpriz yapma imkânı ortadan kalkmaktadır. Kanaatimizce burada makul süre, ürünün teslim edildiği andır.

Maddenin b bendi ilgili kişiyle iletişim kurulması amacını düzenlemektedir. Bu durumda aydınlatma yükümlülüğü ilk iletişim kurulması esnasında yerine getirilecektir. Örneğin bir varlık yönetim şirketi tarafından mevcut bir borç için aranan kişi, konu hukuki bilgi gerektirdiğinden kendisi yerine süreçle ilgili olarak avukatının bilgilendirilmesini isteyebilir ve bu kapsamda telefonda görüştüğü kişiye avukatının telefon numarasını iletebilir. Şayet şirket yetkilisi, avukat ile görüşmek isterse telefon açıldıktan sonra, konuşma içeriğine girmeden aydınlatma yükümlülüğünü yerine getirmelidir. Maddenin c bendinde ise kişisel verilerin aktarılması durumu düzenlenmektedir. Buna göre, eğer bir kişisel veri ilgili kişi dışında üçüncü bir kişiden elde ediliyorsa ve bu veri, veri sorumlusu tarafından aktarılmak isteniyor ise en geç ilk aktarımın yapılacağı esnada aydınlatma yapılması gerekmektedir.

D-Aydınlatma Yükümlülüğüne İlişkin Diğer Usul ve Esaslar

Aydınlatma yükümlülüğü yerine getirilirken uyulması gereken usul ve esaslar Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5'te düzenlenmiştir. Bu başlık altında, özellik arz eden bazı durumlara ilişkin usul ve esasları ele alacağız.

İlk önem arz eden husus, aydınlatmanın her halde yapılması gerektiğidir. Bir başka ifade ile, aydınlatma ilgili kişinin talebine bağlı değildir.²³⁸ Veri sorumlusu, ister açık rızaya dayanarak isterse başka bir sebeple kişisel veri işlemek isterse muhakkak ilgili kişiyi aydınlatmak zorundadır.

İkinci önemli nokta, kişisel veri işleme amacı değiştiğinde yeniden aydınlatma yapılması gerektiğidir. Veri sorumluları, ilgili kişiden kişisel veri temin ederken bunu neden temin ettiğini, amacının ne olduğunu ilgi kişiye bildirmektedir. İlgili kişi de bu

²³⁸ Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Nisan 2019, Ankara, s. 6, (www.kvkk.gov.tr), (Erişim: 08.08.2023)

bilgi doğrultusunda kişisel verisini paylaşmaktadır. Aradan belirli bir zaman geçtikten sonra veri sorumlusu, ilgili kişinin verisini farklı amaçlar için de kullanmak isteyebilir. İşte bu gibi durumlarda artık ilgili kişinin yeniden aydınlatılması gerekmektedir. Zira ortada veri sorumlusunun veriyi aldığı dönemden farklı olarak yeni bir amacı vardır ve bu amacın ilgili kişinin bilgisine sunulması gerekmektedir.

Kişisel Verileri Koruma Kurulu’nun bir kararına²³⁹ konu olayda veri sorumlusu, petrol piyasasında dağıtıcı lisansı kapsamında faaliyet gösteren bir şirkettir. Veri sorumlusu, Enerji Piyasası Düzenleme Kurulu (EPDK) tarafından alınan bir karar ile kendilerine pompa satış hareketlerini plaka, akaryakıt türü, miktar, fiyat, zaman (saat, dakika ve saniye) bilgilerini almaları gerektiği yönünde bir yükümlülük yüklendiğini ve kendilerinin de bir otomasyon sistemi kurduklarını ve bu sistemi de EPDK’nın erişimine açtıklarını belirtmiştir. Veri sorumlusu, bu verileri yasal yükümlülüğünü yerine getirmek için aldığını ancak bu verileri daha farklı bir süreçte de kullanmak istediğini, hatalı akaryakıt dolumlarının önüne geçebilmek için araç tanıma projesi geliştirdiğini ve ellerindeki mevcut veriyi bu projede kullanmak istediklerini ve bu kullanımın KVKK’de yer alan meşru menfaat veri işleme şartına dayandırılıp dayandırılmayacağını Kişisel Verileri Koruma Kurumu’na sormuştur. Kişisel Verileri Koruma Kurulu kararında, veri sorumlusunun veriyi ilk aldığı anda KVKK m. 5’te sayılan hallerden veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması unsurunun gündeme geldiğini, bununla birlikte veriyi ilk elde etme anındaki amaç ile projede güdülen amacın farklılık arz ettiğini, bu nedenle ikincil amacın genel ilkelere ve KVKK’de yer alan işleme şartlarına uygun olması gerektiğini, mevcut verilerin belirtilen projede kullanılmasının yeni bir veri işleme faaliyeti olduğunu, bu faaliyetin meşru menfaat veri işleme şartı kapsamında değerlendirilebileceğini, ancak veri sorumlusunun bu konuda erişilebilir ve görülebilir bir aydınlatma yapması gerektiğini ifade etmiştir. Dolayısıyla kişisel verilerin işleme amacının değiştiği durumlarda muhakkak ilgili kişinin aydınlatılması gerekmektedir.

Bir başka önemli nokta, aydınlatma yükümlüsü olan veri sorumlusunun VERBİS kayıt yükümlülüğünün de bulunup bulunmadığıdır. Şayet bir şirket, VERBİS kayıt yükümlüsü ise aydınlatma metni ve VERBİS kaydı örtüşmek zorundadır. Örneğin bir şirket, aydınlatma metninde alıcı grubu olarak “tedarikçiler” grubunu

²³⁹ “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 10.08.2023)

belirtmiş fakat VERBİS kaydında alıcı grupları içerisinde “tedarikçiler” grubunu seçmemiş ise aydınlatma metni ile VERBİS kaydı arasında bir uyumsuzluk olacaktır. Kanaatimizce böyle bir durum Kişisel Verileri Koruma Kurulu’nun önüne geldiğinde, ihtilaf konusu olay sadece bu durumla sınırlı ise veri sorumlusu hakkında idari para cezası uygulanması yerine talimat verilmesi gerekmektedir. Zira aydınlatma metinleri çok detaylı metinler olduğundan metnin hazırlanması ve kontrol edilmesi anında böyle bir detayın gözden kaçırılabilmesi mümkündür. Uyumluluğun sağlanması için veri sorumlusunun talimatlandırılması yeterli olacaktır.

Aydınlatma yükümlülüğüne ilişkin en önemli noktalardan birisi ispat yükümlülüğüdür. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/ f. 1, e bendi uyarınca aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir. Aydınlatma sürecinde kullanılan aracın hiçbir önemi yoktur. Örneğin aydınlatma sözlü yapılabilir. Veri sorumlusu web sitesinde bir aydınlatma metni yayınlamış olabilir. İlgili kişiden imza alınmak suretiyle aydınlatma metni imzalatılabilir. Önemli olan veri sorumlusunun ilgili kişiyi aydınlattığını ispat edebilmesidir.

Aydınlatmanın ispatı açısından sıklıkla tercih edilen bir yöntem veri sorumlusunun web sitesinde aydınlatma metni yayınlamasıdır. Burada özellik arz eden bazı durumlar söz konusudur. Örneğin suni çim üretimi alanında faaliyet gösteren bir şirket, web sitesinde müşterilerine yönelik bir aydınlatma metni hazırlamış olabilir. Acaba şirketin aydınlatma metnini web sitesine yüklemesi tek başına aydınlatma yapıldığını ispata yeterli olacak mıdır? Kanaatimizce aydınlatma yükümlülüğünün yerine getirilmesi için ya aydınlatma metninin tamamı bir şekilde ilgili kişinin bilgisine sunulmalı veya bu yapılamıyor ise ilgili kişinin erişebileceği bir noktada aydınlatma metninin bulunduğu bilgisi ilgili kişiye verilmelidir.²⁴⁰ Örneğin çağrı merkezi bulunan çoğu veri sorumlusu ya web sitelerinde aydınlatma metni

²⁴⁰ Kişisel Verileri Koruma Kurumu 26.06.2020 tarihinde yayınladığı “Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu” isimli duyuruda bir eksiklik olarak aynen “*Katmanlı aydınlatma yöntemi tercih edildiğinde, ilgili kişilerin ayrıntılı bilgi için başka bir mecraaya yönlendirilmesinden önce, ilk aşamada temel bilgilerin sunulmadığı, detaylı aydınlatmaya erişim için uygun yol ve yöntemlerin izlenmediği, genellikle gizlilik politikaları veya veri işleme politikalarına yönlendirildiği*” ifadesine yer vermiştir. Kişisel Verileri Koruma Kurumu’na göre katmanlı aydınlatma durumunda dahi ön bilgiden sonra asıl metne erişim için uygun bir yol gösterilmemesi eksiklik ve mevzuata aykırılık olarak değerlendirilmiştir. Öyleyse ilk bilgilendirmenin dahi bulunmadığı durumlarda evleviyetle KVKK’ye aykırılık söz konusu olacaktır. (İlgili duyuru için: <https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU>), (Erişim: 17.08.2023)

bulunduğunu ifade ederek web sitesine yönlendirme yapmakta veya bir tuşa basmak suretiyle aydınlatma metninin dinlenilmesine imkan tanımaktadır. Diğer koşulların sağlanması kaydıyla yöntem olarak bu doğru bir uygulamalıdır. Kanaatimizce ilgili kişinin, en azından aydınlatma metnine nereden erişebileceği konusunda bilgi sahibi olması gerekmektedir.

Kişisel Verileri Koruma Kurulu da bir kararında aydınlatma metninin erişilebilir ve görülebilir nitelikte olması gerektiğini belirtmiştir.²⁴¹ Yeri gelmişken belirtmekte fayda var ki yazılı yapılan aydınlatmalarda veri sorumlusu, ilgili kişiye aydınlatma metnini okutmak zorunda değildir. Önemli olan doğru ve usulüne uygun bir aydınlatma metninin bulunması ve bu metni ilgili kişinin erişimine, bilgisine sunmasıdır.

Konuyla ilgili bir diğer önem arz eden husus, kişisel veri işleme şartının açık rıza olması halinde aydınlatmanın nasıl yapılacağıdır. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/ f. 1, f bendi uyarınca açık rızanın alınması ile aydınlatma işleminin ayrı ayrı yapılması gerekmektedir. Uygulamada, bazı veri sorumlularının web sitelerinde “Aydınlatma metnini okudum, açık rıza veriyorum.” şeklinde işaretlenmesi zorunlu kutucuk oluşturduğu görülmektedir. Bu uygulama belirtilen madde uyarınca hatalı bir uygulamalıdır. Zira bir veri sorumlusu, ilgili kişinin aydınlatma metnini okuduğunun teyidini isteyebilir. Bu bir zorunluluk olmasa bile aydınlatma metninin okunduğuna dair zorunlu bir kutucuk oluşturabilir.²⁴² Öte yandan açık rıza verilmesi konusunda bir

²⁴¹ “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 10.08.2023)

²⁴² Kişisel Verileri Koruma Kurumu bu konu hakkında görüş değişikliğine gitmiştir. İlk etapta, Kişisel Verileri Koruma Kurumu bu uygulamanın hatalı olduğu, mevzuata aykırılık teşkil ettiği beyan etmiştir Kurum görüşünü “Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu” isimli duyuruda açıklamıştır. (https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU), (Erişim: 17.08.2023) Ancak veri sorumlusu, aydınlatma metnini ilgili kişinin bilgisine sunduğunu ispat etmek için ilgili kişiden teyit amaçlı bir kutucuk işaretlemesini isteyebilir. Bu, ilgili kişinin menfaatinde. Hatta çoğu web sitesinde, ilgili kişi bu kutucukları işaretlemeyip üye olmaktan veya işlemi devam ettirmekten vazgeçmektedir. Bu da veri sorumlusunun müşteri kaybı anlamına gelmektedir. Buna rağmen veri sorumlusunun ilgili kişiyi aydınlatma metnini okumaya teşvik etmesi olumlu karşılanması gerekirken Kurum tarafından eksiklik ve mevzuata aykırılık olarak değerlendirilmiştir. Belirtilen gerekçe ile Kişisel Verileri Koruma Kurumu’nun bu yaklaşımına katılmıyoruz. Nitekim Kişisel Verileri Koruma Kurumu çok yakın bir tarihte vermiş olduğu bir kararda (Bir özel sağlık kuruluşu tarafından sunulan sağlık hizmetinin açık rıza şartına bağlanması hakkında Kişisel Verileri Koruma Kurulunun 02/05/2023 tarihli ve 2023/692 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), görüş değişikliğine gitmek suretiyle aydınlatma metninin okunduğuna dair bir kutucuk işaretlemesi düzenlemesinin olabileceği hususunda veri sorumlusunu talimatlandırmıştır. Kararın ilgili kısmı aynen “Randevu başvuru formunun altında yer alan “Kişisel

zorunluluk olamaz. Haliyle burada zorunlu olabilmesi makul karşılanan ve zorunlu olmaması gereken iki unsurun tek çatıda toplanması söz konusudur.

Bu uygulamalar gerek belirtilen maddeye gerekse KVKK'nin ruhuna aykırı uygulamalardır. Nitekim Kişisel Verileri Koruma Kurulu bir kararında²⁴³ açık rıza alınmasına ilişkin metin ile aydınlatma metninin ayrılması konusunda veri sorumlusunu talimatlandırmıştır. Ayrıca, Kişisel Verileri Koruma Kurulu, TikTok hakkında verdiği bir kararda da²⁴⁴ aynı hususu vurgulamıştır. Hemen belirtmek gerekir ki Kurulun kararlarına konu olaylarda açık rıza alınması, aydınlatma metninin içerisine dahil edilmekte, adeta bir paket haline getirilip ilgili kişinin önüne sunulmaktadır.

Öte yandan, ilgili kişiden açık rıza alınabilmesi için zaten ilgili kişinin neye rıza göstereceğine dair aydınlatılması gerekmektedir. Dolayısıyla burada açık rıza alabilmek için gerekli olan aydınlatma ile genel manada yapılan aydınlatma işlemini karıştırmamak gerekir. Kurulun işaret etmek istediği nokta, aydınlatma işleminin bir süreç, açık rıza alınmasının ayrı bir süreç olduğu ve bu süreçlerin birbirine karışmaması gerektiği yönündedir.

verilerimin işlenmesine ilişkin aydınlatma metnini okudum. Kişisel Verilerin Korunması Kanunu'na uygun şekilde verilerimin işlenmesine onay veriyorum.” ifadesinin ilgili kişiler tarafından aydınlatma metnine onay veriliyormuş izlenimi yarattığı dikkate alındığında söz konusu metinden “onay veriyorum” ifadesinin çıkarılarak aydınlatma yükümlülüğünün yerine getirildiğinin veri sorumlusu tarafından ispat edilmesini teminen yalnızca aydınlatma metninin okunduğuna dair bir kutucuğun işaretlenmesi şeklinde bir düzenlemenin yapılması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına” şeklindedir.

²⁴³ “Veri sorumlusu tarafından aydınlatma yükümlülüğü ve açık rıza onayı alınması süreçlerinin ayrı ayrı yerine getirilmesi gerektiği ile ilgili” Kişisel Verileri Koruma Kurulunun 26/07/2018 tarihli ve 2018/90 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 10.08.2023), kararın ilgili kısmı aynen “Ayrıca, veri sorumlusu tarafından aydınlatma yükümlülüğünün yerine getirilmesi herhangi bir onaya bağlı değildir. Aydınlatma yükümlülüğünün yerine getirilmesindeki amaç kişisel verilerin işlenmesi noktasında ilgili kişinin bilgi sahibi olmasının temin edilmesidir. Açık rıza alınmasında amaç ise, veri sorumlusu tarafından kişisel verilerinin işlenmesinin hukuki bir gerekçeye dayandırılmasıdır. Bu sebeple, ilgili kişi aydınlatma metni sayesinde kişisel veri işleme faaliyeti ile ilgili olarak bilgi edinmiş olmakla birlikte, söz konusu metinde yazılanlara açık rıza vermek zorunda değildir. Tüm bu hususlar bir arada değerlendirildiğinde; söz konusu uygulamanın 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) amacına ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinin (1) numaralı fıkrasının (f) bendinde yer alan hükme uygun olmadığı, bu itibarla aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların ayrıştırılması hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir.” şeklindedir.

²⁴⁴ TikTok Pte. Ltd. hakkında Kişisel Verileri Koruma Kurulunun 2023/134 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 16.08.2023), kararın ilgili kısmı aynen “TikTok’un Gizlilik Politikasının, esasen aydınlatma yükümlülüğünü yerine getirmek için hazırlanmış bir metin olduğu, ancak açık rıza metni yerine de kullanıldığı, dolayısıyla, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ’in 5’inci maddesinin (f) bendine göre açık rıza şartına dayalı olarak gerçekleştirilen kişisel veri işleme faaliyetleri bakımından açık rızanın aydınlatma yükümlülüğünden ayrı olarak yerine getirilmesi şartının sağlanmadığı” şeklindedir.

Ayrıca Kişisel Verileri Koruma Kurulu açık rıza ile aydınlatmanın aynı metinde yapılmasını eksiklik ve mevzuata aykırılık olarak nitelendirmektedir fakat biz bu değerlendirmeye katılmamaktayız.²⁴⁵ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ m. 5/ f. 1, f bendi aynen “*Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir.*” şeklindedir. Maddeye göre ayrı ayrı yapılması gereken, işlemlerdir. Bu nedenle işlemler ayrıldığı sürece, aynı metnin kullanılmasının bir eksiklik olmadığı ve mevzuata aykırılık teşkil etmediği kanaatindeyiz. Örneğin bir veri sorumlusunun işçilerine imzalatmak üzere üç sayfalık bir evrak hazırladığını varsayalım. Evrakın ilk 2 sayfası ve son sayfasının yarısı işçilere yönelik aydınlatma metnidir. Bu bölümün altında “işçi aydınlatma metnini okudum, anladım.” şeklinde bir bölüm bulunmaktadır. Ardından yeni bir başlık atılmak suretiyle sayfanın kalan yarısında ise açık rıza alınmasına yönelik bir aydınlatma ve açık rızanın kabul ve reddine ilişkin birer kutucuk bulunmakta ve işçi hangisine kanaat getirirse karşısında bulunan kutucuğa imza atması istenmektedir. Kanaatimizce burada aydınlatma ile açık rıza alınması süreçleri ayrılmıştır. Her iki metnin aynı dokümanda yer alması süreçlerin birleştirildiği anlamına gelmez. Zira ilk bölümde işçinin sadece aydınlatma metnini okuması beklenmektedir. İkinci bölümde ise açık rızaya ilişkin kararı istenmektedir. Dolayısıyla burada aydınlatma ile açık rıza alma süreçlerinin ayrıldığı söylenebilir. İşlemler ayrıldığı için de ilgili maddede öngörülen usule uyulduğu kanaatindeyiz. Fakat aynı veri sorumlusu bu metinlerin sonunda “aydınlatma metnini okudum, açık rıza veriyorum” şeklinde bir ibare ile imza atılmasını isteseydi, bu durumda Kurulun kararlarına konu olayların bir benzeri gerçekleşmiş olacak ve uygulama KVKK’ye aykırı olacaktı.

Aydınlatmaya ilişkin bir diğer önemli husus katmanlı aydınlatma kavramıdır.²⁴⁶ Katmanlı aydınlatma uyarınca veri sorumlusu, ilgili kişiyi kısaca kişisel

²⁴⁵ Kişisel Verileri Koruma Kurumu bu görüşünü “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Kamuoyu Duyurusu” isimli duyuruda açıklamıştır. (<https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU>), (Erişim: 10.08.2023)

²⁴⁶ Katmanlı aydınlatma kavramı Kişisel Verileri Koruma Kurulu’nun Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Rehberi’nde tanımlanmış bir kavram olup ilgili tanım aynen “*Kişisel verilerin elde edilmesi sırasında ilgili kişiye, kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin Kanunun 10. maddesine uygun aydınlatmaya yönlendirilmesini ifade eder*” şeklindedir.

verisini işlediği hususunda bilgilendirmekte ve ilgili kişiyi aydınlatma metnine yönlendirmektedir.

Kişisel Verileri Koruma Kurumu tarafından verilen katmanlı aydınlatma örneğinde kamera kaydı alan veri sorumlusu, tek bir cümle ile kameranın kayıt aldığını bildirmekte, detaylı aydınlatma metni için web sitesinin linkine ve bir qr koda yönlendirmektedir.²⁴⁷

Veri sorumlusu, katmanlı aydınlatma metni yöntemini tercih ettiğinde ilk aşamada ilgili kişiyi genel hatlarıyla da olsa bilgilendirmeli, detaylı aydınlatma için bir erişim yolu sunmalı, genel nitelikteki “gizlilik politikası” veya “veri işleme politikası” formatındaki evraklara yönlendirme yapmamalıdır.²⁴⁸

Yeri gelmişken belirtmekte fayda var ki aydınlatma metni olarak birçok veri sorumlusu ilgili kişileri aydınlatmak yerine çok genel nitelikte herkesi kapsayacak ve fakat ihtiyacı karşılamayan tek bir metin hazırlama ve yayınlama eğilimindedir. Ancak bu metinlerin çoğu aydınlatma yükümlülüğünün yerine getirilmesi için yeterli değildir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında²⁴⁹ bu formattaki metinlerin çok genel nitelikte olduğunu, karışık yapıya sahip olduğunu ve ilgili kişilerin ihtiyacı olan belirliliği sağlayamadığını ifade etmiştir.

Konuya ilişkin ele alacağımız son husus çocukların ve görme engellilerin nasıl aydınlatılacağıdır. Çocukların aydınlatma metinleri çocuklara özel olarak hazırlanmalı, hitap edilen yaş kesimine uygun olmalı, mümkünse resimler ile desteklenmeli, basit bir anlatım tercih edilmeli, çocukların yaşının doğrulanabileceği sistemler kullanılmalıdır.²⁵⁰ Görme engelliler açısından da görme engelli bir bireyin anlayabileceği usul ve yöntemler tercih edilmelidir. Örneğin perakende satış yapan bir

²⁴⁷ Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Nisan 2019, Ankara, s. 19, (www.kvkk.gov.tr), (Erişim: 10.08.2023)

²⁴⁸ (İlgili duyuru için: <https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU>), (Erişim: 10.08.2023)

²⁴⁹ “İlgili kişinin Kanunun 11 nci maddesi kapsamındaki başvurusuna veri sorumlusu tarafından verilen cevabın yeterli bulunmaması” hakkında Kişisel Verileri Koruma Kurulunun 03/02/2021 tarihli ve 2021/85 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 10.08.2023), Kararın ilgili kısmı aynen “*Bu doğrultuda hazırlanan bir Aydınlatma Metninin, ilgili kişilere, yaptıkları işlem bazında, söz konusu işlem dahilinde kullanılan kişisel verilerine ilişkin bilgilendirme sağlamanın beklendiği, veri sorumluları için genel hukukî metinler niteliğinde olan “Gizlilik Politikası”, “Veri İşleme Politikası” gibi metinlerin, karışık yapıları ve ilgili kişilerin ihtiyacı olan belirlilikteki bilgilendirmeleri sağlayamamaları nedenleriyle Aydınlatma Metni olarak kullanılmamaları gerektiği*” şeklindedir.

²⁵⁰ Kişisel Verileri Koruma Kurumu, Çocukların Kişisel Verilerinin Korunması “Ürün ve Hizmet Geliştirilenler Tarafından Dikkat Edilmesi Gerekenler”, (www.kvkk.gov.tr), (Erişim: 12.08.2023)

tekstil firmasının müşteri aydınlatma metnini kasa arkasına asması, görme engelli bireyler içinse aynı aydınlatma metninin Braille alfabesi²⁵¹ ile hazırlanmış bir versiyonunun ayaklı panoda bulundurulması bu kapsamda doğru bir uygulama olacaktır.

II-VERBİS KAYIT YÜKÜMLÜLÜĞÜ

Veri Sorumluları Sicili (VERBİS) KVKK m. 16'da düzenlenmiş olup maddenin ikinci fıkrası aynen “*Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.*” şeklindedir. VERBİS kayıt yükümlülüğünün detayları ise Veri Sorumluları Sicili Hakkında Yönetmelik'te düzenlenmiştir.²⁵²

Öncelikle belirtmek gerekir ki VERBİS kayıt yükümlülüğü KVKK kapsamındaki yükümlülüklerden sadece bir tanesidir. Uygulamada ne yazık ki çoğu veri sorumlusunda VERBİS kayıt yükümlülüğü, diğer bütün yükümlülüklerden daha önemliymiş izlenimi mevcuttur. Zira genellikle veri sorumluları VERBİS'e kayıt olduğunda KVKK'ye uyumlu olduğunu, artık yapacak başkaca bir şeyi olmadığını düşünmektedir. Hatta VERBİS kayıt yükümlülüğünün yerine getirilip getirilmediğinin kontrolü çok kolayken diğer yükümlülüklerin yerine getirilip getirilmediğinin kontrolünün bir şikayete bağlı olduğu anlayışı ve kolay kolay da şikayet olmayacağı düşüncesiyle sadece VERBİS kaydının yapılmasının yeterli olduğu izlenimi mevcuttur. Oysa Veri Sorumluları Sicili Hakkında Yönetmelik m. 5/ f. 1, f bendi bu durumu “*Kanunun 28 inci maddesinde belirtilen durumlar saklı kalmak kaydıyla Yönetmeliğin 16 ncı maddesinde belirtilen objektif kriterlere dayalı olarak belirli şartları taşıyan veri sorumlularının Kurul tarafından Sicile kayıtlı yükümlü tutulmaması; bu veri sorumlularının Kanun kapsamındaki yükümlülüklerini ortadan kaldırmaz.*” demek suretiyle düzenlemiştir. Dolayısıyla, ister VERBİS kayıt yükümlüsü olsun ister olmasın her veri sorumlusunun KVKK kapsamında belirli yükümlülükleri vardır ve bu yükümlülüklerle uygun hareket etmek zorundadır.

²⁵¹ Braille alfabesi, Louis Braille tarafından geliştirilmiş altı kabartılmış noktalar ile görme engellilerin okuma ve yazmasını sağlayan bir alfabetir. (https://orgm.meb.gov.tr/alt_sayfalar/yayimlar/ozelegitim/braille/braille.pdf), (Erişim: 12.08.2023)

²⁵² RG., 30286 S., 30.12.2017 T.

A-VERBİS'E KAYDOLMASI GEREKEN VERİ SORUMLULARI

VERBİS kayıt yükümlülüğü bulunan dört grup mevcuttur. Bu gruplar için Kişisel Verileri Koruma Kurulu bazı kriterleri göz önünde bulundurarak kayıt yükümlülüğü başlangıç tarihleri belirlemiştir.²⁵³

VERBİS kayıt yükümlülüğü bulunan birinci grup “Yıllık çalışan sayısı 50’den çok veya yıllık mali bilanço toplamı 100 milyon TL’den çok olan gerçek ve tüzel kişi veri sorumluları”dır.²⁵⁴ Yıllık mali bilanço toplamının tespitinde gelir veya kurumlar vergisi beyanname ekindeki mali tablolarda yer alan mali bilanço bilgisi dikkate alınmaktadır.²⁵⁵ Yıllık çalışan sayısının tespitinde ise Muhtasar ve Prim Hizmet Beyannamesinde bildirilen çalışan sayısı dikkate alınmakta olup beyanname verilen 12 ayın en az 7’sinde 50’den çok çalışan bulunması gerekmektedir.²⁵⁶

VERBİS kayıt yükümlülüğü bulunan ikinci grup, yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularıdır. Üçüncü grup “Yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 100 milyon TL’den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumluları”dır. Dördüncü ve son grup ise kamu kurum ve kuruluşlarıdır.

Çalışmamızın öznesini teşkil eden Türk ticaret şirketleri açısından iki grup büyük önem arz etmektedir. Buna göre Türkiye’de mukim bir ticaret şirketi, ilk olarak çalışan sayısının 50’den çok olup olmadığını ve yıllık mali bilanço toplamının 100 milyon TL’nin üzerinde olup olmadığını kontrol edecektir. Eğer bu iki kriterden herhangi birisini sağlıyor ise VERBİS kayıt yükümlülüğünü yerine getirecektir. Şayet bu iki kriter de mevcut değilse ikinci aşamaya geçilecek ve veri sorumlusu, ana faaliyet konusunun özel nitelikli kişisel veri işleme olup olmadığını kontrol edecektir. Eğer ana faaliyet konusu özel nitelikli kişisel veri işlemek ise VERBİS kayıt yükümlülüğünü yerine getirecektir. Aksi durumda ise kayıt yükümlülüğü bulunmayacaktır.

Anılan kriterlerden çalışan sayısı ve yıllık mali bilanço toplamı kriterinin sağlanıp sağlanmadığının tespiti kolaydır. Asıl sorunlu kısım “ana faaliyet konusu özel

²⁵³ Kişisel Verileri Koruma Kurumu, “Veri Sorumluları İçin VERBİS 'e Kayıtlar Başladı” Duyurusu, (www.kvkk.gov.tr), (Erişim: 12.08.2023)

²⁵⁴ 100 milyon TL kriteri çok uzun bir süre 25 milyon TL şeklinde uygulanmış olup Kişisel Verileri Koruma Kurulu’nun 06.07.2023 tarihli ve 2023/1154 sayılı kararı ile 100 milyon TL’ye çıkartılmıştır.

²⁵⁵ Kişisel Verileri Koruma Kurumu, **Sorularla VERBİS**, s. 13, (www.kvkk.gov.tr), (Erişim: 12.08.2023)

²⁵⁶ Kişisel Verileri Koruma Kurumu, **Sorularla VERBİS**, s. 13, (www.kvkk.gov.tr), (Erişim: 12.08.2023)

nitelikli kişisel veri işleme olma” kriterinin neye göre belirleneceğidir? Soruya cevap verebilmek için özel nitelikli kişisel verileri hatırlamakta fayda vardır. KVKK m. 6/ f. 1 uyarınca özel nitelikli kişisel veriler “*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.*” demek suretiyle sınırlı olarak sayılmıştır.

Öyleyse bu grubun tespitinde veri sorumlusunun ana faaliyetinin, sayılan verilerden biri veya birkaçını işlemek olması gerekmektedir. Burada akla ana faaliyet konusunun ne anlama geldiği sorusu gelebilir. Kişisel Verileri Koruma Kurumu bu kavram için “en çok katma değer üretilen faaliyet” ya da “yürütülen temel işin görevi gereği” tanımlamasını yapmakta ve “temel olarak yürütülen faaliyetlerin özel nitelikli kişisel veri işlenmesini gerektirme” unsurlarını göz önünde bulundurmaktadır.²⁵⁷ Örneğin estetik merkezleri, saç ekim merkezleri, diyetisyenler, diş hekimleri, psikologlar bu kapsamdadır. Bazı meslek gruplarının ise kapsamını tespit etmek bu kadar kolay değildir. Örneğin müşterilerinin iris fotoğrafını çeken ve büyük tablolar halinde satışını gerçekleştiren bir fotoğrafçı acaba bu kapsama girecek midir? Burada çok farklı ihtimaller bulunabilir. Örnekteki fotoğrafçının sunduğu hizmet sadece bununla sınırlı olabilir. Öyleyse ana faaliyet konusu özel nitelikli kişisel veri işlemek olduğundan VERBİS kayıt yükümlülüğünün tespiti gerekir.

Öte yandan örnekteki fotoğrafçı, düğün fotoğrafı çekimi, vesikalık çekimi, işyerlerinde fotoğraf çekim hizmeti gibi birçok hizmetinin yanında iris fotoğrafçılığı da yapabilecektir. Acaba bu durumda da VERBİS kayıt yükümlülüğü bulunmakta mıdır? Kanaatimizce bu durumda iris fotoğrafçılığı ana faaliyetten ziyade sunulan bütün hizmetlerden sadece bir tanesidir. Ana faaliyet kapsamında işlenen kişisel veri, ilgili kişinin fotoğrafı olduğundan burada VERBİS kayıt yükümlüsü bulunmadığı kanaatindeyiz.

²⁵⁷ Kişisel Verileri Koruma Kurumu, **Sorularla VERBİS**, s. 28, (www.kvkk.gov.tr), (Erişim: 12.08.2023), Açıklamanın ilgili kısmı aynen “*Ana faaliyetin özel nitelikli kişisel veri işleme olup olmadığının tespitinde, veri sorumlularının en çok katma değer ürettiği faaliyetleri veya yürüttükleri temel iş ve görevleri gereği özel nitelikli kişisel veri işlenmesi durumu olup olmadığı dikkate alınmalıdır. Diğer bir deyişle burada değerlendirilmesi gereken; veri sorumlularının herhangi bir faaliyeti içerisinde özel nitelikli kişisel veri işlenmesi değil, temel olarak yürütmekte oldukları işlerinin kapsamının özel nitelikli kişisel veri işlenmesi durumudur*” şeklindedir.

Kişisel Verileri Koruma Kurumu, bu grubun tespitinde NACE faaliyet kodlarından yararlanıldığını ifade etmektedir.²⁵⁸ Kanaatimizce bu yaklaşım doğru değildir. Örneğin ilk bakışta bir gözlükçünün VERBİS kayıt yükümlüsü olduğu çok rahat bir şekilde söylenebilir. Zira gözlükçüler müşterilerinin reçeteleri uyarınca ürün temin etmekte ve satış yapmaktadır. Dolayısıyla da sağlık verisi işlemektedir. Pek karşılaşılmasa bile acaba bir gözlükçünün satışlarının %80'i reçetesiz ürünlerden ve yan ürünlerden oluşsa ve sadece %20'si reçeteli ürünlerden oluşsa acaba yine de VERBİS kayıt yükümlülüğünden bahsetmek mümkün olacak mıdır? Kanaatimizce bu örnekte de VERBİS kayıt yükümlülüğü bulunmaktadır. Örneğimizde her ne kadar satışlarının küçük bir kısmı reçeteli ürünlerden gerçekleşse de bir gözlükçünün asıl faaliyeti ve görevinin gereği sağlık verisi işlemeyi gerektirdiğinden yine kayıt yükümlülüğü söz konusudur.

Belirtmek isteriz ki VERBİS kayıt yükümlülüğünde belirlenen kriterler kişisel verilerin korunması hukukunun ruhuyla hiçbir şekilde örtüşmemektedir. Bu kriterlere göre 60 çalışanı bulunan bir tekstil şirketinin VERBİS kayıt yükümlülüğü bulunurken 4 çalışanı olan ve işlerinin %40'ı iris fotoğrafçılığı olan bir fotoğrafçının VERBİS kayıt yükümlülüğü bulunmamaktadır. Bu kriterlere göre kişisel veriye çok teması olan hatta tek işi kişisel veri işleme olan şirketler kapsam dışında kalabilmekteyken tabiri caizse kişisel veriyle hiçbir işi olmayan şirketler kapsam içinde kalabilmektedir. Bu da uygulamada düzensizliği getirmektedir.

Kanaatimizce VERBİS kayıt yükümlülüğü istisna olmaksızın ya tüm şirketler için getirilmeli ya da tamamen kaldırılmalıdır. Kayıt yükümlülüğü veriden ziyade çalışan sayısı, mali bilanço, ana faaliyet konusu gibi kriterlere bağlandığından uygulamada da bir belirsizlik söz konusudur.

Ayrıca, Kişisel Verileri Koruma Kurumu'nun bu veri sorumlularını nasıl tespit edeceği de bir muammadır. İlk bakışta, mesleği kapsamında ana faaliyet konusu itibarıyla özel nitelikli kişisel veri işlemiyor gibi duran ancak ana faaliyeti itibarıyla özel nitelikli kişisel veri işleyen bir veri sorumlusunu Kurum nasıl tespit edecektir? Bunun tespiti için Türkiye'de VERBİS kaydı bulunmayan bütün şirketlerin kontrol edilmesi gerekir ki bu imkansızdır. Ya da bir kişinin bu şirketleri VERBİS kayıt

²⁵⁸ Kişisel Verileri Koruma Kurumu, **Sorularla VERBİS**, s. 28, (www.kvkk.gov.tr), (Erişim: 12.08.2023),

yükümlülüğünü yerine getirmediği gerekçesiyle şikayet etmesi gerekir ki bu da çok sık karşılaşılan bir durum değildir. Öyleyse bu grup açısından getirilen kriterler tamamen anlamsız kalmaktadır.

Her ne kadar kanaatimiz VERBİS kayıt yükümlülüğünün tüm şirketlere getirilmesinden yana olsa da mevcut uygulamada Kişisel Verileri Koruma Kurumu tarafından belirttiğimiz grup açısından en azından kayıt yükümlülüğü bulunan meslek gruplarının yayımlanmasının farkındalık açısından faydalı olacağı kanaatindeyiz.

B-VERBİS KAYIT YÜKÜMLÜLÜĞÜNÜN DOĞDUĞU VE YÜKÜMLÜLÜĞÜN YERİNE GETİRİLDİĞİ AN

VERBİS kayıt yükümlülüğünün zamansal olarak tespitinde ikili bir ayırım ile konuyu ele almak gerekmektedir. Veri sorumlusunun halihazırda kayıt yükümlüsü olması ile sonradan kayıt yükümlüsü olması halinde süreler farklılık arz edecektir.

Kural olarak veri sorumlularının kişisel veri işlemeye başlamadan önce VERBİS'e kayıt yükümlülüğünü yerine getirmesi gerekmektedir.²⁵⁹ Buna göre Kişisel Verileri Koruma Kurumu tarafından ilan edilen sürelerle riayet edilmesi gerekmektedir. Kişisel Verileri Koruma Kurulu almış olduğu bir karar ile yukarıda izah olunan gruplara ilişkin VERBİS kayıt yükümlülüğünün başladığı tarihleri web sitesinde duyurmuştur.²⁶⁰ Dolayısıyla KVKK yürürlüğe girdiğinde eğer bir veri sorumlusu yukarıda belirtilen gruplardan birisi kapsamında ise Kişisel Verileri Koruma Kurumu'nun yaptığı duyuruda belirtilen tarihler uyarınca VERBİS kayıt yükümlülüğü başlamış olacaktır.²⁶¹

²⁵⁹ Veri Sorumluları Sicili Hakkında Yönetmelik, m. 8/ f. 1

²⁶⁰ Kişisel Verileri Koruma Kurumu web sitesinde yer alan “Veri Sorumluları İçin VERBİS 'e Kayıtlar Başladı” isimli duyuruda Yıllık çalışan sayısı 50’den çok veya yıllık mali bilanço toplamı 25 milyon TL’den (duyuru tarihi itibarıyla kriter 25 milyon TL idi) çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumluları için VERBİS kayıt yükümlülüğünün başlangıç tarihinin 01.10.2018 olarak belirlendiği, yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olmakla birlikte ana faaliyet konusu özel nitelikli kişisel veri işleme olan veri sorumluları için 01.01.2019 tarihinde, kamu kurum ve kuruluşu veri sorumluları için ise 01.04.2019 tarihinde başlayacağı belirtilmiştir.(<https://www.kvkk.gov.tr/Icerik/5290/Veri-Sorumlulari-Icin-VERBIS-e-Kayitlar-Basladi>), (Erişim: 12.08.2023)

²⁶¹ Belirtmekte fayda var ki Kişisel Verileri Koruma Kurumu tarafından bu yükümlülüğün yerine getirilmesi için son tarihler belirlenmiş ve bu tarihler sürekli ertelenmiştir. Son kayıt tarihlerinin ertelenmesi, piyasada bu yükümlülüğün sürekli olarak erteleneceği izlenimini uyandırmış ve kanaatimizce yükümlülüğün ciddiyetini kaybetmesine sebebiyet vermiştir. Nitekim Kişisel Verileri Koruma Kurumu tarafından VERBİS kayıt yükümlülüğünü yerine getirmeyenler hakkında idari para cezası uygulaması yapılması gerektiği halde hakkında henüz hiçbir işlem yapılmayan çok sayıda veri sorumlusu olduğu gözetildiğinde son kayıt tarihinin birçok kez ertelenmesi ve yükümlülüğü yerine getirmeyen veri sorumlularının çoğunu kapsayacak bir yaptırım uygulanmaması sonuç itibarıyla bu yükümlülüğün çok da önemli olmadığı izlenimini veri sorumlusu nezdinde uyandırmaktadır.

Öte yandan, bazı veri sorumlularının sonraki bir tarihte de VERBİS kayıt yükümlüsü olması mümkündür. Örneğin 2019 yılında faaliyete başlayan bir veri sorumlusu, 2022 yılında yukarıda belirtilen kriterleri sağlayan gruplardan birisine girmiş olabilir. Bu durumlardaki veri sorumlularının, kayıt yükümlülüğü doğduğu andan itibaren 30 gün içerisinde VERBİS'e kaydolması gerekmektedir.²⁶² Özellikle yıllık mali bilanço toplamı veya çalışan sayısı kriterinin esas alındığı veri sorumluları açısından bu zaman diliminin doğru tespiti son derece önemlidir.

Kişisel Verileri Koruma Kurumu, yıllık mali bilanço toplamının tespiti noktasında Gelir Vergisi Beyannamesi veya Kurumlar Vergisi Beyannamesini esas almaktadır.²⁶³ Buna göre, daha önce VERBİS kayıt yükümlüsü olmayan bir limited şirketin, 1 Mayıs 2023 tarihinde verdiği kurumlar vergisi beyannamesinde beyan ettiği yıllık mali bilanço toplamının 120 milyon TL'ye ulaştığını varsayalım. Öyleyse bu limited şirket, belirttiği miktara ilk defa beyannameyi verdiği tarih itibarıyla ulaşmış olacaktır. Bu durumda örnekteki limited şirketin 1 Haziran 2023 tarihine kadar VERBİS kaydını tamamlamış olması gerekecektir.

VERBİS kayıt yükümlülüğünün yerine getirildiği anı tespit edebilmek için VERBİS kaydının nasıl yapıldığının bilinmesi gerekmektedir. VERBİS kayıt süreci, veri sorumlusunun Kişisel Verileri Koruma Kurumu'na yapacağı bir başvuru ile kullanıcı adı ve şifre temin talebiyle başlamaktadır. Başvuruyu alan Kişisel Verileri Koruma Kurumu, veri sorumlusu adına bir kullanıcı adı ve şifre tanımlamakta ve bu bilgiyi veri sorumlusuna iletmektedir. Veri sorumlusu, VERBİS paneli üzerinden bilgilerini güncelledikten sonra bir irtibat kişisi²⁶⁴ atamaktadır. Akabinde irtibat kişisi de e-devlet üzerinden giriş yapmak suretiyle veri sorumlusunun kendisine tanıdığı bu yetkiyi kabul etmektedir. Akabinde usulünce kayıt işlemini tamamlamaktadır.²⁶⁵ En son aşamada da “Bildirim KVKK'ya gönderilecektir, emin misiniz?” şeklinde bir

²⁶² Veri Sorumluları Sicili Hakkında Yönetmelik, m. 8/ f. 2 aynen “Kayıt yükümlülüğü altında bulunmayan, sonradan kayıt yükümlüsü haline gelen veri sorumluları, yükümlülük altına girmelerini müteakip otuz gün içerisinde Sicile kaydolurlar.” şeklindedir.

²⁶³ Kişisel Verileri Koruma Kurumu, **Sorularla VERBİS**, s. 13, (www.kvkk.gov.tr), (Erişim: 12.08.2023)

²⁶⁴ İrtibat Kişisi, Veri Sorumluları Sicili Hakkında Yönetmelik, m. 4/ f. 1, ç bendinde tanımlanmış olup ilgili tanım aynen “Türkiye’de yerleşik olan tüzel kişiler ile Türkiye’de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişi” şeklindedir.

²⁶⁵ VERBİS kayıt sürecinin tamamına yönelik detayları içeren Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Kılavuzu isimli kılavuz, Kişisel Verileri Koruma Kurumu tarafından web sitesinde yayımlanmış olup kayıt süreci açısından yol gösterici niteliktedir.

pencere açılmakta ve “evet” kutucuğuna tıklandığı anda bildirim Kişisel Verileri Koruma Kurumu’na ulaşmaktadır. İşte veri sorumlusunun VERBİS kayıt yükümlülüğünü tamamladığı an bu kutucuğu işaretleyip bildirimini gönderdiği andır.

Uygulamada birçok veri sorumlusu ne yazık ki ilk etapta aldığı kullanıcı adı ve şifre ile bilgi güncellemesini yaptıktan sonra VERBİS kayıt yükümlülüğünü yerine getirdiğini zannetmektedir. İşlemleri bu aşamada bırakan bir veri sorumlusu sadece kullanıcı adı ve şifre temin etmiş olacak ancak kayıt yükümlülüğünü yerine getirmiş olmayacaktır. Nitekim Veri Sorumluları Sicili Hakkında Yönetmelik m. 10 / f. 1 hükmü aynen “*Veri sorumluları, 9 uncu maddede belirtilen bilgileri VERBİS’e yüklemek suretiyle kayıt yükümlülüğünü yerine getirmiş sayılır.*” şeklindedir.

Son olarak değinmek istediğimiz husus ise VERBİS kaydının güncel tutulması gerektiğidir. Veri Sorumluları Sicili Hakkında Yönetmelik m. 13 hükmü aynen “*Veri sorumluları, sicilde kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, VERBİS üzerinden yedi gün içerisinde Kuruma bildirir.*” şeklindedir. Buna göre bir veri sorumlusunun VERBİS kaydında güncelleme yapması gerekiyor ise bu ihtiyacın doğduğu andan itibaren yedi gün içerisinde güncellemeyi yapması gerekmektedir. Örneğin, bir veri sorumlusunun VERBİS’te belirttiği adres değişmiş olabilir. Bu durumda ilgili güncellemenin yedi gün içerisinde yapılması gerekmektedir.

III-VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

A-GENEL OLARAK

Veri güvenliğine ilişkin yükümlülükler KVKK m. 12’de düzenlenmiştir. Madde kapsamında kanun koyucunun veri güvenliğine yönelik üç temel noktayı işaret ettiği görülmektedir. Bunlar, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamaktır. Bu yükümlülükler aşağıda detaylıca anlatılacaktır.

Kişisel verilerin korunması hukukunun temelinde ilgili verilerin KVKK’ye uygun olarak işlenmesi ve bu verilerin güvenli bir şekilde tutulması yer almaktadır. Bunun sağlanabilmesi için bir veri sorumlusunun yapması gereken ilk şey, işleyeceği tüm kişisel verileri tespit etmektir.²⁶⁶ Zira bir veri sorumlusu ancak işleyeceği bütün

²⁶⁶ Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi** (Teknik ve İdari Tedbirler), s. 8 (www.kvkk.gov.tr), (Erişim: 14.08.2023)

kişisel verileri tespit edebilirse hukuka uygunluğunu sağlayabilir ve güvenliğini temin edebilir.

Veri sorumlusunun bir sonraki aşamada yapması gereken, işleyeceği kişisel verileri, KVKK m. 5'te veya KVKK m. 6'da belirtilen hangi veri işleme şartına dayandıracağını tespit etmektir. Bunu takiben, kişisel verinin niteliğini, gizlilik arz eden bir verinin olup olmadığını, kişisel veriyi nasıl muhafaza edeceğini, kimlerin erişim yetkisi olacağını belirlemeli ve bu doğrultuda gerekli idari ve teknik tedbirleri almalıdır.

Belirtmekte fayda var ki Kişisel Verileri Koruma Kurulu'nun kararlarına konu olaylar incelendiğinde, ihlale sebebiyet veren eylemlerin temelinde genellikle insan faktörü yer almaktadır. Bu nedenle veri sorumlularının KVKK kapsamında eğitim almaları gerektiği, kişisel veriye teması olan çalışanlarının da aynı eğitimden istifade etmesinin veri güvenliğine ilişkin yükümlülükler bakımından faydalı olacağı ve riski azaltacağı kanaatindeyim.

B-KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK İŞLENMESİNİ ÖNLEME YÜKÜMLÜLÜĞÜ

Veri sorumlusunun veri güvenliği kapsamında ilk yükümlülüğü, kişisel verilerin hukuka aykırı olarak işlenmesini önlemektir. Bu yükümlülük KVKK m. 12/ f. 1, a bendinde düzenlenmiştir. Ayrıca, kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünü yerine getirmeyen veri sorumluları hakkında KVKK m. 18/ f. 1, b bendi uyarınca Kişisel Verileri Koruma Kurulu'nun idari para cezası yaptırımını uygulayabilme yetkisi bulunmaktadır. Belirtmek gerekir ki Kurul tarafından idari para cezası yaptırımını uygulanan kararların çok büyük bir bölümünde bu maddenin ihlal edildiği görülmektedir.

Kişisel verilerin hukuka aykırı olarak işlendiği durumlar farklı şekillerde karşımıza çıkabilir. Örneğin veri sorumlusu, açık rıza alması gerektiği halde açık rıza almadan kişisel veri işlemiş olabilir. Kişisel Verileri Koruma Kurulu'nun birçok kararı bu doğrultudadır.²⁶⁷ Veri sorumlusu, açık rızayı hizmet şartına bağlamış olabilir.

²⁶⁷ Bir anonim şirketin (veri sorumlusu) ilgili kişinin açık rızası dışı elektronik ticari ileti göndermesine ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 Tarihli ve 2019/162 Sayılı Karar Özeti; "Bir doktor tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi" hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/332 Sayılı Karar Özeti; "Bir Eğitim Kurumu tarafından ilgili kişinin cep telefonu numarasının herhangi bir veri işleme şartına dayanmaksızın işlenmesi ve ilgili numaraya reklam/bilgilendirme içerikli mesaj gönderilmesi" hakkında Kişisel

Örneğin Kişisel Verileri Koruma Kurulu'nun 25.03.2019 tarihli²⁶⁸ kararı bu doğrultudadır. Herhangi bir kişisel veri işleme şartına dayanmaksızın kişisel veri işlemiş olabilir. Genellikle Kurul kararlarının çoğunda bu durum söz konusudur.²⁶⁹ Ya da veri sorumlusu KVKK m. 4'te belirtilen genel ilkelere riayet etmemiş olabilir. Örneğin Kişisel Verileri Koruma Kurulu'nun 31.05.2019 tarihli kararı bu doğrultudadır.²⁷⁰ Dolayısıyla KVKK m. 4, m. 5, m. 6 ve m. 8 ve m. 9 hükümlerine aykırılıklarının hepsinin bu yükümlülük kapsamında ele alınabilmesi mümkündür.

Veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğü kapsamında ilk yapması gereken KVKK m. 4'te belirtilen genel ilkelere uygunluğun sağlanmasıdır. Zira işlenecek olan kişisel verinin türü ne olursa olsun bu ilkelere uyulması zorunludur. Özellikle belirtmek gerekir ki bir kişisel veri işleme faaliyetinin KVKK m. 5'te veya KVKK m. 6'da bir dayanağı olabilir ancak yine de o veri işleme faaliyeti KVKK m. 4'te belirtilen ilkelere aykırılık teşkil edebilir.

Ölçüsüz bir şekilde açık rıza alınması bunun en somut örneğidir. Açık rıza alındığı halde bile kişisel verilerin işlenmesinin KVKK m. 4'te belirtilen “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine aykırı olabilme ihtimali söz konusu olabilmektedir. Örneğin Kişisel Verileri Koruma Kurulu'nun 31.05.2019 tarihli kararı bu konuya ilişkindir.²⁷¹

Verileri Koruma Kurulunun 14/01/2020 Tarihli ve 2020/20 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.08.2023)

²⁶⁸ Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.08.2023)

²⁶⁹ “İlgili kişinin irtibat numarasının bir elektrik dağıtım şirketi tarafından herhangi bir işleme şartına dayanmaksızın işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 27/01/2020 tarihli ve 2020/66 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.08.2023)

²⁷⁰ Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/159 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 14.08.2023)

²⁷¹ Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 20.08.2023), Kararın ilgili kısmı aynen “Ölçülülük ilkesinin ise, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması anlamına geldiği, bu kapsamda, kişisel veri işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verilerin toplanmaması ve/veya işlenmemesi gerektiği, veri sorumlusunun amacı çerçevesinde ölçülülük ilkesine uygun olarak ilgili kişiden minimum düzeyde bilgi talep etmesi, bunun dışındaki amaç için gerekli olmayan veri işlemeden kaçınması gerektiği, kişisel verilerin işlenmesinin ilgili kişinin iznine bağlı olarak gerçekleştirilse ve belirli bir amaca bağlı olsa bile açık rızanın, aşırı miktarda veri toplanmasını meşrulaştırmayacağı, buna göre kişisel verilerin yalnızca belirli amaçlar için ve gerektiği kadar toplanması, amacın gerektirdiği yerlerde kullanılması ve amaç için gerekli olandan uzun süre tutulmaması gerektiği” şeklindedir.

Bir başka aykırılık durumu ise muhafaza süresine ilişkin KVKK m. 4/ f. 2, d bendi kapsamında gündeme gelebilir. Örneğin çalışan adayı seçme ve yerleştirme sürecinde bir veri sorumlusunun çalışan adayının açık rızasına istinaden fotoğraf verisini işlediğini ve adayın işe seçilmediğini, açık rızasını da hiçbir zaman geri almadığını varsayalım. Bu örneğimizde eğer veri sorumlusu, seçme ve yerleştirme sürecinin tamamlanmasının ardından 6 yıl geçtiği halde ilgili adayın fotoğrafı şeklindeki kişisel verisini hala işliyorsa, açık rıza geri alınmamış olsa dahi “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkesine aykırı hareket etmiş olacaktır.

Netice itibarıyla KVKK’de öngörülen kişisel veri işleme şartlarından birisine dayanıyor olmak genel ilkelere de uygun davranıldığına karine teşkil etmez. Aksine, veri işleme faaliyeti genel ilkelere aykırı olabilir. Bu durumda veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünü yerine getirmemiş olur.

İkinci dikkat edilmesi gereken husus, her işlenecek kişisel verinin KVKK m. 5’te ve KVKK m. 6’da düzenlenen bir veri işleme şartına dayanması gerektiği ve veri işleme şartının doğru tespit edilmesi gerektiğidir. Bu nedenle, eğer bir kişisel verinin işlenebilmesi için hiçbir veri işleme şartına dayanılamıyorsa ilgili kişisel verinin işlenmemesi gerekmektedir. Uygulamada en çok karşılaşılan durum, açık rıza almak istemeyen veri sorumlusunun meşru menfaat veri işleme şartına dayanmasıdır. Bu durumun son derece sakıncalı olduğunu veri işleme şartları bölümünde²⁷² anlattığımız için tekrara düşmemek adına hatırlatmakla yetineceğiz.

Üçüncü dikkat edilmesi gereken nokta kişisel verilerin aktarılması sürecidir. Bir veri sorumlusu kendi bünyesinde işlediği kişisel veriler açısından genel ilkelere uygun hareket ediyor olabilir ve işlediği tüm kişisel veriler açısından KVKK’de öngörülen bir veri işleme şartına da dayanabilir. Ancak kişisel verilerin aktarılması sürecinde de KVKK m. 8 ve KVKK m. 9 hükümlerine uygun hareket etmesi gerekmektedir. Aksi takdirde kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünü yerine getirememiş olacaktır.

²⁷² Bkz: s. 76 vd.

Kişisel verilerin aktarılması KVKK’de iki ayrı maddede ele alınmıştır. Kişisel verilerin yurt içinde aktarılması KVKK m. 8’de, kişisel verilerin yurtdışına aktarılması ise KVKK m. 9’da düzenlenmiştir. İlk ele alacağımız konu, KVKK m. 8’de düzenlenen kişisel verilerin yurt içinde aktarılmasıdır. Hemen belirtmek gerekir ki kişisel verilerin aktarılması bir kişisel veri işleme faaliyetidir.²⁷³ Bu nedenle aktarımın da KVKK’de belirtilen veri işleme şartlarından birisine dayanması gerekmektedir.

Kanun koyucu kişisel verileri kategorize ederken yaptığı ayrımı burada da sürdürmüştür. Buna göre genel nitelikte olan kişisel verilerin aktarılmasında KVKK m. 8/ f. 1 hükmü uyarınca açık rızaya veya KVKK m. 8/ f. 2 atfıyla KVKK m. 5/ f. 2’de belirtilen veri işleme şartlarından birisine dayanılabilir. Öyleyse bir veri sorumlusu, genel nitelikte bir kişisel veriyi yurt içinde aktarmak istediği takdirde ya ilgili kişiden açık rıza almalı ya da KVKK m. 5/ f. 2’de belirtilen bir veri işleme şartına dayanmalıdır. Ayrıca aktarım sürecinde de KVKK m. 4’te belirtilen genel ilkelere uygun hareket etmelidir.

Kişisel verilerin aktarılması farklı yöntemler ile gerçekleşebilir. Örneğin bir şirket yetkilisi tarafından başka bir şirket yetkilisine aylık raporlama şeklinde bir veri akışı gerçekleşebilir. Sözlü olarak paylaşım yapılmış olabilir. Fiziken bir evrakı elden teslim etmek suretiyle aktarım yapılabilir ya da bu süreç alıcının hazırladığı bir sisteme kişisel verilerin yüklenmesi suretiyle de gerçekleşebilir. Hemen belirtmek gerekir ki bir şirketin insan kaynakları departmanının muhasebe departmanına kişisel veri aktarması gibi departmanlar arası kişisel veri paylaşılması, kişisel verilerin aktarılması olarak nitelendirilmemektedir. Zira burada üçüncü bir alıcı yoktur.

Kişisel verilerin aktarılması durumunda meydana gelebilecek veri ihlalleri açısından farklı senaryolar söz konusu olabilir. Bu nedenle ilgili durumu Kurul kararları ışığında ele almanın faydalı olacağı kanaatindeyiz. Kişisel Verileri Koruma Kurulu bir kararında mahkeme tarafından talep olunan kişisel veriden daha fazla kişisel verinin mahkemeye aktarılmasında, veri sorumlusunun hukuki yükümlülüğünü

²⁷³ KVKK m. 3/ f. 1, e bendi aynen “*Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*” şeklindedir.

yerine getirebilmesi için veri işlemenin zorunlu olması veri işleme şartına dayanılamayacağını belirtmiştir.²⁷⁴

Türk ticaret şirketleri özeline konuyu indirgeyecek olursak mahkemeler tarafından müzekkere yazılmak suretiyle ya da savcılık tarafından talep olunmak suretiyle birtakım kişisel verilerin aktarılması talep olunabilmektedir. Bu gibi durumlarda yalnızca talep olunan kişisel veri aktarımı yapılmalı, daha fazlası yapılmamalıdır. Kişisel Verileri Koruma Kurulu'nun 03.03.2020 tarihli kararı da açıklamalarımız ile aynı doğrultudadır.²⁷⁵ Bu nedenle kamu kurumları ile yalnızca talep olunan kişisel veriler ve yalnızca ilgili kişinin kişisel verileri paylaşılmalı, konuyla alakası olmayan üçüncü kişilerin kişisel verileri paylaşılmamalıdır.

Kişisel Verileri Koruma Kurulu'nun 20.05.2020 tarihli kararına²⁷⁶ konu olayda ise ilgili kişi, veri sorumlusu olan hastanenin tüp bebek bölümünde tahlil yaptırmış ve tahlil sonucu kendisine ve tanımadığı başka birisine e-posta olarak gönderilmiştir. Kişisel Verileri Koruma Kurulu önüne gelen bu uyuşmazlıkta konu dışı üçüncü kişiye yapılan aktarım açısından KVKK m. 6/ f. 3 uyarınca bir veri işleme şartına dayanılmadığı ve açık rıza da olmadığından bahisle veri sorumlusu hakkında idari para

²⁷⁴ İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık), (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁷⁵ “İlgili kişiye ait kişisel verinin denetim faaliyeti kapsamında bir kamu kurumuna aktarılmasına ilişkin şikayet hakkında” Kişisel Verileri Koruma Kurulunun 03/03/2020 Tarihli ve 2020/196 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “Denetim için gerekli olan tüm bilgi ve belgelerin talep edilmesi şeklinde gerçekleşen kişisel veri işleme faaliyetinin, Kanunun 5 inci maddesinin 2 numaralı fıkrasının (a) bendinde yer alan “kanunlarda açıkça öngörülme” hükmü kapsamında olduğu, şirketin söz konusu verileri aktarmasının ise Kanunun 5 inci maddesinin 2 nci fıkrasının (ç) bendi hükmüne göre “veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması ” hükmü kapsamında olduğu, bu çerçevede söz konusu verilerin bahse konu şirket tarafından, kamu kurumuna Kanunun 8 inci maddesinin 2 nci fıkrasının (a) bendi uyarınca aktarıldığı, ancak söz konusu aktarım ile idari soruşturmanın konusu olmayan üçüncü kişilerin kişisel verilerinin de veri sorumlusu şirket tarafından ilgili veri sorumlusuna aktarıldığı dikkate alındığında, idari soruşturma konusu olmayan kişisel verilerin aktarılmasının Kanunun 4 üncü maddesinin 2 numaralı fıkrasının (ç) bendinde yer alan “amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine aykırı olduğu, bu hususun ise hukuka aykırı bir veri işleme faaliyeti olduğu bu itibarla Kanunun 12 nci maddesinin 1 numaralı fıkrasında yer alan veri güvenliğine ilişkin yükümlülükleri yerine getirmediği değerlendirilen veri sorumlusu hakkında Kanunun 18 inci maddesinin 1 numaralı fıkrasının (b) bendi kapsamında 50.000 TL idari para cezası uygulanmasına” şeklindedir.

²⁷⁶ “İlgili kişinin tahlil sonuçlarının veri sorumlusu hastane tarafından hukuka aykırı şekilde üçüncü kişilere aktarılması” hakkında Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/407 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “Bu çerçevede başvuruya konu olayda, ilgili kişinin veri sorumlusu Hastanede bulunan tahlil sonuçlarının sağlığa ilişkin özel nitelikli kişisel veri olduğu dikkate alındığında, bahse konu tahlil sonuçlarının üçüncü bir taraf olarak, hastaneden bağımsız şekilde çalışan ve ayrı bir gerçek kişi veri sorumlusu olarak değerlendirilen doktorun asistanına mail atılmak suretiyle aktarılmasında Kanunun 8 inci maddesi kapsamında herhangi bir hukuki dayanak söz konusu olmadığından ve veri sorumlusu Hastane tarafından da söz konusu aktarımın sehven yapıldığının beyan edilmiş olmasından hareketle ilgili kişinin kişisel verilerinin hukuka aykırı olarak aktarıldığı kanaatine varıldığı” şeklindedir.

cezası yaptırımını uygulamıştır. Buradan hareketle özellikle müşterilerine e-mail ile bildirimde bulunan veri sorumluları açısından yalnızca ilgili kişiye e-mail gönderilmesi gerektiği, başka kişilere e-mail gönderilmemesi gerektiği, konuyla ilgisi bulunmayan kişilerin e-maillerin “cc” kısmında bulundurulmaması gerektiği söylenebilir. Bu konuda veri sorumlularının her türlü idari ve teknik tedbiri alması gerekmektedir.

Kişisel Verileri Koruma Kurulu’nun 05.04.2021 tarihli kararına²⁷⁷ konu olayda ise aracı ağır hasarlı hale gelen ilgili kişi, veri sorumlusu olan sigorta şirketine hasar bildiriminde bulunmuş, sigorta şirketi de araç pert işlemlerinin tamamlanabilmesi için bu sektörde faaliyet gösteren üçüncü bir şirkete ilgili kişinin kişisel verilerini aktarmıştır. Kurul kararında, sigorta şirketinin veri sorumlusu olduğunu, araç pert işlemlerini tamamlamak için bilgi paylaşımı yapılan şirketin ise veri işleyen olduğunu, üçüncü şirketin sigorta şirketi adına kişisel verileri işlediğini, bu nedenle de aradaki akışın KVKK m. 8 kapsamında ele alınamayacağını belirtmiştir. Kişisel Verileri Koruma Kurulu’nun bu tespitine katılmamaktayız. Kişisel verilerin aktarılması ile kastedilen kişisel verinin, veri sorumlusu ve departmanları haricinde üçüncü bir gerçek veya tüzel kişiye aktarılmasıdır. Öyleyse dışarıdan hizmet alınan bir şirkete kişisel verilerin gönderilmesi işlemi kişisel verilerin aktarılması anlamına gelmektedir. Aksi halde, birtakım hizmetlerin dışarıdan temin edilmesi halinde kişisel veri aktarımı yapılan durumların hiçbirinde kişisel veri aktarımından bahsedilemeyecektir ki Türkiye’de muhasebe hizmetleri, avukatlık hizmetleri, bilişim hizmetleri gibi hizmetlerin büyük çoğunluğu dış kaynaktan temin edilen hizmetlerdir. Kanaatimizce örneği verilen durumların hepsinde bir kişisel veri aktarımı vardır. Bu nedenle Kişisel Verileri Koruma Kurulu’nun veri sorumlusu-veri işleyen arasındaki bilgi akışının KVKK m. 8 kapsamında değerlendirilemeyeceği yönündeki tespitine iştirak etmemekteyiz.

Netice itibarıyla kişisel verilerin yurt içinde aktarılması durumu söz konusu olduğunda veri sorumluları tarafından KVKK m. 4’te belirtilen genel ilkelere riayet

²⁷⁷ “Bir sigorta şirketi tarafından işlenen kişisel verilerin üçüncü kişiye aktarılması ve ilgili kişiye veri aktarımına ilişkin aydınlatma yapılmaması” hakkında Kişisel Verileri Koruma Kurulunun 05/04/2021 tarih ve 2021/333 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “*Veri sorumlusu ile veri işleyen üçüncü kişi Şirket arasında imzalanan Ağır Hasarlı Araç Satış Sözleşmesi incelendiğinde ise, üçüncü kişi şirketin veri sorumlusunun verdiği talimatlar doğrultusunda ve veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işlemesi sebebiyle veri işleyen olarak hareket ettiği anlaşıldığından, veri sorumlusu ile onun adına kişisel verileri işleyen arasında yapılan paylaşımların Kanunun 8 inci maddesi kapsamında ele alınamayacağı*” şeklindedir.

edilmeli, KVKK m. 8 atfıyla KVKK m. 5’te veya KVKK m. 6’da belirtilen veri işleme şartlarından birisine dayanılmalıdır. Aksi halde veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünü yerine getirememiş olacaktır.

Kişisel verilerin aktarılması konusunda değinilmesi gereken önemli noktalardan birisi de kişisel veri işleme sözleşmesidir. Kişisel veri işleme sözleşmesi, veri sorumlusu ile veri işleyen arasında tanzim olunan, veri işleyenin veri sorumlusundan alacağı emir ve talimatlar uyarınca kişisel veri işlemeyi üstlendiği, veri sorumlusunun da ücret ödeme yükümlülüğü altına girdiği bir sözleşmedir. Bu sözleşme ile veri işleyen, veri sorumlusunun iradesine uyacak şekilde veri işleme faaliyetini yerine getireceğinin taahhüdünü vermektedir.²⁷⁸ Veri sorumlusu açısından esaslı unsur ise ücret unsurudur.²⁷⁹

Kişisel veri işleme sözleşmesi, kanunlarda adı geçmeyen, hüküm ve sonuçları da düzenlenmemiş olan bir sözleşme olduğundan isimsiz sözleşmeler²⁸⁰ kategorisinde yer almaktadır. Kanaatimizce kişisel veri işleme sözleşmesi içeriği itibariyle vekalet sözleşmesi ile eser sözleşmesinin esaslı unsurlarını içermektedir. Zira veri işleyen, veri sorumlusunun kendisine çizdiği çerçevede veri işleme işlemini yerine getirmeyi üstlenmektedir. Ayrıca veri işleyen, sadece veri işleme faaliyetini yerine getirmeyi üstlenmemekte aynı zamanda veri işleme faaliyeti ile veri sorumlusunun ulaşmayı hedeflediği sonucun da meydana geleceğini taahhüt etmektedir. Dolayısıyla bir sonuç taahhüdü de söz konusudur. Bu kanaatlerimiz uyarınca kişisel veri işleme sözleşmesi hem vekalet sözleşmesinin hem de eser sözleşmesinin unsurlarını barındırmaktadır.

Kişisel veri işleme sözleşmesi kapsamında, vekalet sözleşmesi ve eser sözleşmesi bir bütün olarak varlığını korumamakta, sadece esaslı unsurları yönüyle yer almakta ve kanunlarda düzenlenmemiş yeni bir sözleşme ortaya çıkmaktadır. Bu nedenle kişisel veri işleme sözleşmesi, karma nitelikte bir sözleşmedir.²⁸¹

Sözleşme, iki tarafa borç yükleyen bir sözleşmedir. Yapısı itibariyle tam iki tarafa borç yükleyen bir sözleşme olabileceği gibi eksik iki tarafa borç yükleyen bir

²⁷⁸ TAŞTAN, a.g.e., s. 119

²⁷⁹ Gamze TURAN BAŞARA, *Uyuşmazlık Mahkemesi Dergisi*, “Kişisel Veri İşleme Sözleşmesi”, Yıl: 8, Sayı: 16, Aralık 2020, s. 70

²⁸⁰ Fahrettin ARAL/ Hasan AYRANCI, *Borçlar Hukuku Özel Borç İlişkileri*, 9. Baskı, Ankara, 2012, s.50; Fikret EREN, *Borçlar Hukuku Özel Hükümler*, 3. Baskı, Ankara, 2016, s. 865; Aydın ZEVKLİLER/ Emre GÖKYAYLA, *Borçlar Hukuku Özel Borç İlişkileri*, 15. Baskı, Ankara, 2015, s. 12

²⁸¹ Aynı görüşte TAŞTAN, a.g.e., s. 121; TURAN BAŞARA, a.g.e., s. 68

sözleşme de olabilir. Örneğin veri sorumlusu ücret ödemeyi taahhüt etmişse sözleşme tam iki tarafa borç yükleyen bir sözleşme olarak nitelendirilebilir.

Öte yandan bazı durumlarda farklı tüzel kişiliklere sahip fakat aynı yönetim tarafından yönetilen şirketler arasında aktarım söz konusu olabilir ve bu tür şirketler veri aktarımında birbirine herhangi bir ücret ödememektedir. Bu gibi durumlarda ücret unsuru olmayacağı için eksik iki tarafa borç yükleyen bir sözleşmeden bahsedilebilecektir. Kişisel verilerin aktarılması, genellikle bir hizmetin ifası kapsamında taraflar arasında bulunan başkaca bir sözleşmenin ifası amacıyla gündeme gelmekte ve veri sorumlusu da bu hizmet için bir ücret ödemektedir. Bu nedenle kural olarak kişisel veri işleme sözleşmesi tam iki tarafa borç yükleyen bir sözleşmedir.²⁸²

Kişisel veri işleme sözleşmesi herhangi bir şekle tabi değildir. Öte yandan birazdan inceleyeceğimiz²⁸³ KVKK m. 9/ f. 2, b bendi kapsamında tanzim olunacak sözleşmelerin yazılı olarak yapılması gerekmektedir.

Kişisel veri işleme sözleşmesi açısından kural olarak yazılılık unsuru bulunmasa bile herhangi bir uyuşmazlık halinde sorumluluğun tespiti ve ispat açısından yazılı olmasında fayda vardır.

Kişisel veri işleme sözleşmesi aslında birçok şirketin ticaret hayatı içerisinde farketmeden sözlü olarak yaptığı bir sözleşmedir. Örneğin bir şirketin, bazı muhasebe hizmetlerini dış kaynaktan temin suretiyle üçüncü bir şirkete yaptırması ve bu kapsamında bütün çalışanlarının kişisel verilerini ilgili şirkete aktarması halinde aslında yazılı olmasa bile taraflar arasında bir kişisel veri işleme sözleşmesi mevcuttur.²⁸⁴

Veri sorumlusu ve veri işleyen arasındaki uyuşmazlıkların çoğunda veri işleyen, veri sorumlusunun talimatları dışında bir veri işleme faaliyeti gerçekleştirmiştir. Bu da dolaylı olarak kişisel verilerin hukuka aykırı olarak işlenmesini önleme yükümlülüğünün ihlali anlamına gelecektir. Bu riski bertaraf etmek amacıyla kural olarak zorunlu olmasa bile veri sorumlusunun veri işleyen ile yazılı olarak kişisel veri işleme sözleşmesi yapması ve veri işlemenin amacı ile

²⁸² Aksi görüşte TAŞTAN, a.g.e., s. 124; TURAN BAŞARA, a.g.e., s. 68

²⁸³ Bkz: s. 120 vd.

²⁸⁴ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması isimli rehberinin 38. sayfasında veri işleyeni, veri sorumlusu ile kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirilen kişi olarak tanımlamıştır.

şartlarını çok net bir şekilde ortaya koyması ve emir-talimatlara uyulduğunun da kontrolünü sağlaması son derece önemlidir.

Kişisel verilerin aktarılmasında bir diğer ihtimal ise KVKK m. 9'da belirtilen kişisel verilerin yurt dışına aktarılmasıdır. Kişisel verilerin yurt dışına aktarılması, yurt içinde aktarımdan daha ağır şartları öngörmektedir. Hemen belirtmek gerekir ki KVKK m. 9/ f. 1 uyarınca kişisel verilerin yurt dışına açık rızaya istinaden aktarılması mümkündür.

Açık rıza söz konusu olmaksızın kişisel verilerin yurt dışına aktarılabilmesi içinse iki ihtimal söz konusudur. Bunlardan birincisi aktarımın dayanağının KVKK m. 5 ya da KVKK m. 6/ f. 3 olması ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunmasıdır. Yeterli koruma bulunan ülkelerin tespitini yapmaya yetkili kurum, Kişisel Verileri Koruma Kurumu'dur.²⁸⁵ Kişisel Verileri Koruma Kurumu ne yazık ki uzun bir süre geçmesine rağmen hala güvenli ülkeler listesi yayınlamamıştır. Bu nedenle kişisel verilerin yurt dışına aktarımında KVKK m. 9/ f. 2, a bendi teoride var olan ancak uygulamada şimdilik kullanılamayacak olan bir hükümdür.

Son ihtimal ise aktarımın dayanağının KVKK m. 5 ya da KVKK m. 6/ f. 3 olması ve aktarım yapılacak ülkenin yeterli korumanın olduğu ülkeler arasında olmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulu'nun izninin bulunmasıdır.

Buna göre öncelikle, kişisel veri aktarımında KVKK'de öngörülen veri işleme şartlarından ilgili olan veri işleme şartına dayanılmalıdır. İkinci aşamada her iki taraf yeterli bir korumayı yazılı olarak taahhüt etmelidir. Son aşamada tarafların yapmış olduğu bu sözleşme Kişisel Verileri Koruma Kurulu'nun bilgisine sunulmalı ve onay alınmalıdır. Bu maddenin detaylarını aşağıda ele alacağız ancak yeri gelmişken belirtmekte fayda var ki kanaatimizce 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında bir veri sorumlusunun tercih ettiği takdirde en çok efor harcaması gereken yükümlülük, KVKK m. 9/ f. 2, b bendinde düzenlenen yükümlülüktür. Zira burada

²⁸⁵ KVKK m. 9/ f. 3 aynen “Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.” şeklindedir.

veri sorumlusu hem aktarım yapacağı üçüncü kişiyi sözleşme yapmaya ikna edebilmeli hem de sözleşmenin yeterli olduğu konusunda Kurulu ikna edebilmelidir.

Belirtmekte fayda var ki KVKK'nin yürürlüğe girdiği tarihten bu tezin kaleme alındığı ana kadar bu maddeye dayanarak onay alan veri sorumlusu sayısı çok azdır. Özellikle onay alabilen şirketlerin büyük ölçekli kurumsal şirketler olduğu göz önüne alındığında kanaatimce bu şartlar Türkiye'de çok az şirketin sağlayabileceği şartlardır. Netice itibarıyla bize göre mevcut şartlar içerisinde bir veri sorumlusunun yurt dışına veri aktarımında dayanabileceği tek makul yöntem açık rıza almaktır. Açık rıza da geri alınabilirliği sebebiyle aktarım sürecinde risk barındırmaktadır. Tüm bu hususlar bir bütün olarak göz önünde bulundurulduğunda kişisel verilerin yurt dışına aktarılması son derece riskli bir alandır.

Kişisel verilerin yurt dışına aktarılması noktasında KVKK m. 9 uyarınca veri sorumlusunun tercih edebileceği üç yöntem bulunmaktadır. Açık rızaya ilişkin daha önce yaptığımız açıklamalar²⁸⁶ aynı şekilde bu bölüm için de geçerlidir. Bir diğer yöntem olan güvenli ülkelerin tercihi ise teoride var olan ancak uygulamada var olmayan bir madde olduğundan bu başlık altında son değinmek istediğimiz nokta KVKK m. 9/ f. 2, b bendidir.²⁸⁷ Bu maddeye dayanılarak yurt dışına veri aktarımı yapılabilmesi için öncelikle aktarımın dayanağı KVKK m. 5 veya KVKK m. 6/ f. 3 olmalıdır.

İkinci aşamada aktarım yapılacak ülke yeterli korumanın bulunmadığı ülkelere birisi olmalıdır. Kurul henüz güvenli ülkeler listesi yayınlamadığı için şu anda herhangi bir ülkenin tercihi halinde bu şart otomatik olarak gerçekleşmiş olacaktır.²⁸⁸

Üçüncü aşamada, Türkiye'deki veri sorumlusu ile yabancı ülkedeki veri sorumlusu yeterli bir korumayı yazılı olarak taahhüt etmelidir. Son aşamada ise bu taahhütnameye Kişisel Verileri Koruma Kurulu tarafından onay verilmiş olmalıdır. Bu

²⁸⁶ Bkz: s. 58 vd.

²⁸⁷ KVKK m. 9/ f. 2 aynen "Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması, b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir." şeklindedir.

²⁸⁸ Kişisel Verileri Koruma Kurumu, **Madde ve Gerekeşi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü**, s. 26, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

aşamaları tamamlamış olan bir veri sorumlusu, KVKK m. 9/ f. 2, b bendi uyarınca aldığı onay kapsamında yurt dışına kişisel veri aktarımı yapabilecektir. Tam da bu noktada, taraflar arasında yapılacak olan taahhütnamenin neleri ihtiva etmesi gerektiği ve Kişisel Verileri Koruma Kurulu’nun bu taahhütname kapsamında taraflardan beklentisinin ne olduğu soruları akla gelebilir.

Öncelikle belirtmek gerekir ki KVKK m. 9/ f. 2, b bendinde geçen “*Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının*” ibaresinden yalnızca her iki tarafın da veri sorumlusu olduğu durumların düzenlendiği anlaşılabılır. Ancak buradaki ilişkinin veri sorumlusu- veri işleyen ilişkisi olması da mümkündür.²⁸⁹ Nitekim Kişisel Verileri Koruma Kurulu, 16.05.2018 tarihinde yayınladığı bir duyuruda²⁹⁰ KVKK m. 9/ f. 2, b bendi kapsamında hazırlanacak taahhütnamelere ilişkin iki ayrı evraka yer vermiş olup evraklardan birisi “veri sorumlusundan veri işleyene aktarım” ismini taşımaktadır. İlâveten, Kişisel Verileri Koruma Kurumu’nun 07.05.2020 tarihli duyurusu da benzer içeriğe sahiptir.²⁹¹ Dolayısıyla KVKK m. 9/ f. 2, b bendi kapsamında bir veri aktarımı, veri sorumlusu- veri sorumlusu şeklinde gerçekleşebileceği gibi veri sorumlusu- veri işleyen şeklinde de gerçekleşebilir.

KVKK m. 9/ f. 2, b bendi kapsamında hazırlanacak olan taahhütnamelerde nelere dikkat edilmesi gerektiği Kurum tarafından duyurulmuş²⁹² ve taahhütnamelerin asgari olarak taşınması gereken unsurlara ilişkin örnek dokümanlar Kurum tarafından paylaşılmıştır.²⁹³ Bu kapsamda, esasa ilişkin dikkat edilmesi gerekenler, aktarımın tarafları arasındaki hukuki ilişkinin doğru bir şekilde tespit edilmesi, taraflar arasındaki hukuki ilişkiyi tevsik edici belgelerin sunulması, taahhütnamede KVKK’de yer alan terminolojinin kullanılması, veri işleme şartının açık rıza olduğu durumlarda taahhütnamede bu hususa yer verilmemesi, muğlak ifadelerden kaçınılması, açık ve

²⁸⁹ DÜLGER, a.g.e., s. 448

²⁹⁰ Kişisel Verileri Koruma Kurumu’nun “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar” isimli ve 16.05.2018 tarihli duyurusu, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁹¹ Kişisel Verileri Koruma Kurumu’nun “Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru” isimli ve 07.05.2020 tarihli duyurusu, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁹² Kişisel Verileri Koruma Kurumu’nun “Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar” isimli ve 16.05.2018 tarihli duyurusu, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁹³ Kişisel Verileri Koruma Kurumu’nun “Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru” isimli ve 07.05.2020 tarihli duyurusu, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

sade bir dil kullanılması, her bir veri kategorisi için ayrı ayrı veri işleme şartının gösterilmesi, aktarılabacak kişisel verinin alıcı tarafından ne şekilde kullanılacağı konusunda açıklayıcı bilgilere yer verilmesi şeklindedir. Bu doğrultuda hazırlanan taahhütnameler Kişisel Verileri Koruma Kurulu tarafından onaylandığı takdirde KVKK m. 9/ f. 2, b bendi kapsamında kişisel verilerin açık rıza aranmaksızın yurt dışına aktarılması mümkün olabilmektedir. Kişisel Verileri Koruma Kurulu tarafından bu doğrultuda verilen kararlardan bazıları duyuru olarak da yayınlanmaktadır.²⁹⁴

C-KİŞİSEL VERİLERE HUKUKA AYKIRI OLARAK ERİŞİLMESİNİ ÖNLEME YÜKÜMLÜLÜĞÜ

Kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğü, KVKK m. 12/ f. 1, b bendinde düzenlenmiştir. Kanun koyucunun veri sorumlusundan bir beklentisi de bünyesinde bulunan kişisel verilerin gerek fiziken gerekse dijital ortamlarda hukuka aykırı ele geçirilmesini önlemeye yönelik teknik ve idari tedbirleri almasıdır. Nitekim KVKK m. 12/ f. 1’de belirtilen üç yükümlülük açısından da madde, idari ve teknik tedbir alma zorunluluğu ile bitmektedir. Veri güvenliğinin temini amacıyla alınması gereken teknik ve idari tedbirlerin neler olduğu KVKK’de düzenlenmemiş olmamakla birlikte konuyla ilgili Kişisel Verileri Koruma Kurulu’nun kararları ve veri güvenliği rehberi²⁹⁵ yol gösterici niteliktedir. Çalışmamızın öznesini Türk ticaret şirketleri oluşturduğu için idari ve teknik tedbirler konusunu şirketler bağlamında ele alacağız.

Bir şirketin alabileceği idari tedbirler konusunda herhangi bir sınırlama bulunmamaktadır. Önemli olan kişisel veri güvenliğinin sağlanmasıdır. Bu kapsamda, mevcut risk ve tehditlerin belirlenmesi ve risk analizi²⁹⁶ yapılması, KVKK kapsamında kurumsal politikalar oluşturulması, kişisel veri işleme sözleşmelerinin yapılması, gizlilik taahhütnamelerinin yapılması, disiplin yönetmeliği oluşturulması, çalışanlara eğitim verilmesi, şirket içi denetimler yapılması örnek verilebilir. Verilen örnekler

²⁹⁴ Amazon Turkey Perakende Hizmetleri Limited Şirketi ve Amazon Turkey Yönetim Destek Hizmetleri Limited Şirketi’nin aldığı izne ilişkin “Taahhütname Başvurusu Hakkında Duyuru” isimli ve 04.03.2021 tarihli duyuru bu şekildedir. Benzer şekilde Turksport Spor Ürünleri Sanayi Ticaret Limited Şirketi (Decathlon Türkiye) tarafından alınan izne ilişkin duyuru da örnek verilebilir. (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁹⁵ Kişisel Verileri Koruma Kurumu, **Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)**, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

²⁹⁶ VOIGT ve VON DEM BUSSCHE, GDPR kapsamında risk analizi yapılırken öncelikle yüksek cezalara sebebiyet verebilecek ihlallerin belirlenmesi ve bunlar üzerine yoğunlaşılması gerektiğini, riskin fazla olduğu süreçlerin tespit edilebilmesi için işyeri bazında genel bir denetimden ziyade departmanlar bazında denetim yapılması gerektiğini belirtmektedir. Daha detaylı açıklamalar için bkz., VOIGT ve VON DEM BUSSCHE, s. 246-247

içerisinde kurumsal politika ve prosedürlerin hazırlanması ve uygulanması, önem arz eden tedbirlerden birisidir.

Bir şirketin KVKK kapsamında belirli politika ve prosedürlere sahip olması son derece önemlidir. Zira belirli süreçler belirli yöntemlere bağlandığı takdirde süreç çok hızlı ilerleyebilecek aksi durumda sürekli bir tereddüt gündeme gelecektir. Örneğin bir şirkette kişisel veri ihlali yaşandığının bir çalışan tarafından tespit edilmesi halinde çalışanın izlemesi gereken yolun ne olduğu, ya da ilgili kişinin fiziken yaptığı KVKK m. 11 kapsamındaki başvurusunun kimlere iletileceği, kimin başvuruyu neticelendireceği, bu süreçte ilgili kişi ile memnuniyete yönelik bir telefon görüşmesi yapılıp yapılmayacağı gibi birçok konunun belirli politika ve prosedürlere bağlanması önem arz etmektedir. Bu sayede, izlenecek yöntem, kimlerin sorumlu olduğu net bir şekilde belirlenmiş olacak ve şirket içi bir eksikliğin gündeme gelmesi durumunda da eksikliğin kimden kaynaklandığı net bir şekilde ortaya çıkacaktır.

Belirtmekte fayda var ki KVKK kapsamında hazırlanması gereken bazı evraklar zaten kanun gereği zorunlu olarak belirtilmiştir. Örneğin aydınlatma metni, kişisel veri saklama ve imha politikası gibi dokümanlar KVKK uyarınca veri sorumlusuna yüklenen yükümlülük gereği bulunması gereken evraklardandır.

Öte yandan zorunlu olmasa bile şirket içerisinde ilgili kişi başvurularının nasıl neticelendirileceğine ilişkin bir prosedür belirlenmesi, veri ihlalinin tespiti halinde nasıl hareket edileceğinin düzenlendiği bir veri ihlal müdahale politikası oluşturulması ya da özel nitelikli kişisel veriler açısından daha hassas bir kategori olduğundan işlenme ve korunmasına yönelik süreçlerin, ek tedbirlerin yer aldığı bir politikanın belirlenmesi veri sorumlusunun menfaatine olacaktır. Hemen belirtmek gerekir ki bu tür kurumsal politikaların en verimli neticeyi verebilmesi için ilgili çalışanların bu evraklardan haberdar olması, ne işe yaradığını bilmesi, yükümlülüklerini anlaması gerekmektedir. Bir şirkette kişisel verilerin güvenliğinin sağlanması, önce çalışanların farkındalığı ile başlamaktadır.

Kişisel verilere hukuka aykırı erişim durumu farklı şekillerde gündeme gelebilir. Örneğin veri sorumlusunun bir ihmalinden, veriye ulaşmaması gereken bir kişi veriye erişmiş olabilir ya da veri sorumlusuna siber saldırı düzenlenmek suretiyle bir saldırı sonucu verilere erişilmiş olabilir. İster fiziki ister dijital ortamda olsun veri sorumlusu her iki alanda da veri güvenliğini sağlamak zorundadır.

Kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğü kapsamında Kişisel Verileri Koruma Kurulu tarafından verilmiş farklı kararlar söz konusudur. Konuya ilişkin kararlarda değerlendirilen noktalardan bazıları; kişisel verilere yetkisiz erişim olması halinde yetkisiz erişimin hızlı bir şekilde tespit edilip edilmediği²⁹⁷, bir veri ihlali meydana gelmeden önce veri sorumlusunun çalışanlarına konuyla ilgili bir eğitim verip vermediği, idari ve teknik tedbirlerin veri ihlalinin önce mi sonra mı alındığı²⁹⁸, kişisel veri içeren panellerin kullanılması halinde bu panellerde erişim yetkilerinin belirlenip belirlenmediği, yetki matrisi bulunup bulunmadığı ve erişim yetkilerinin düzenli olarak kontrol edilip edilmediği²⁹⁹, risk analizi ve log kayıt takibi gibi önlemlerin uygulanıp uygulanmadığı³⁰⁰ şeklindedir.

²⁹⁷ Marriott International Inc. hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.08.2023), kararın ilgili kısmı aynen “Saldırganın web sunucusuna bir komut istemi yükleyerek Starwood ağına girdiğinin tespit edildiği ve web sunucusuna erişimin sağlanmasının ardından, saldırgan tarafından web sunucusuna uzaktan erişim sağlayan bir truva atı (RAT) yüklendiği, saldırganın daha sonra kimlik bilgilerini toplayan ilave araçlar yüklediği ve sonrasında Starwood ağındaki diğer cihazlara erişim sağlayabilmek için kimlik bilgilerini ve iç ağ bağlanabilirliğini kullandığının tespit edilememesinin alınan teknik ve idari tedbirlerin yetersizliğinin göstergesi olduğu, 2014 yılından itibaren mevcut olan yetkisiz erişim ve komut isteminin kurulumunu gösteren web olay günlüklerinin (log kayıtları) olmasına rağmen, olayın tespit edilememesinin Şirket tarafından alınması gereken teknik ve idari tedbirlerin alınmadığının somut bir göstergesi olduğu” şeklindedir.

²⁹⁸ Bir turizm şirketi hakkında Kişisel Verileri Koruma Kurulunun 27.08.2019 tarih ve 2019/255 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “Güvenlik duvarının ihlal gerçekleşikten sonra yenilenmesinin sağlandığı ve güvenlik duvarının güncel durumda bulunmamasının teknik bir eksiklik olduğu, Çalışanların ihlal gerçekleşikten sonra güvenlik eğitiminin sağlandığı ve daha önce böyle bir eğitim almadıkları anlaşılmış olup bu durumun da kişisel veri güvenliği sağlanması ve farkındalığı noktasında idari bir eksikliğin göstergesi olduğu, İhlali gerçekleştiren kişinin önce Şirket içindeki sunuculara erişim sağladığı, daha sonra dikkat çekmemek için Şirketten ayrıldığı ve bir sunucuya yüklediği uzaktan erişim yazılımı ile işlemlerini gerçekleştirdiği, Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının Şirket IT sistemleri tarafından fark edilmemesinin teknik bir eksiklik olduğu, - Sunucu üzerindeki verilerin geri getirilemez şekilde ihlali gerçekleştiren kişi tarafından yok edildiği, Söz konusu olayın Bilgi İşlem Birimine Şirketin diğer birimlerinde çalışanlar tarafından bildirilmesinin Şirketin Bilgi İşlem Biriminin ve Bilgi Sistemlerinin düzgün olarak çalışmadığı ve işlemediğinin bir göstergesi olduğu” şeklindedir.

²⁹⁹ Kişisel Verileri Koruma Kurulu’nun 27.04.2021 tarihli kararına konu olayda müşteri hizmetleri paneline (CRM) hukuka aykırı erişim sağlanmak suretiyle birtakım kişisel veriler hukuka aykırı olarak geçirilmiştir. Kurul kararında, belirtilen panelde yetkilendirme süreçlerinin kontrol edilmemesinden bahisle gerekli tedbirlerin alınmadığına kanaat getirmiştir. Buna göre Kurul, kişisel veri içeren panellerin kullanılması halinde bu panellerde erişim yetkilerinin belirlenmiş olmasını, yetki matrisi bulunmasını ve erişim yetkilerinin düzenli olarak kontrol edilmesini beklemektedir. “Bir e-ticaret sitesi (veri sorumlusu) nezdinde gerçekleşen veri ihlali hakkında yapılan resen inceleme” hakkında Kişisel Verileri Koruma Kurulunun 27/04/2021 tarih ve 2021/427 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “İhlalin veri sorumlusu tarafından kendi tedarikçisi konumunda olan firmanın da bulunduğu tedarikçi grubuna “tüm bildirimlerde arama” yetkisinin verilmesi sonucunda oluştuğunun tespit edildiği, bu durumun yetkisiz erişime ilişkin düzenli kontrolün sağlanmadığının ve yetkilendirme süreçlerinin kontrol edilmeyerek veri ihlali öncesinde veri sorumlusu tarafından ilgili kişiler üzerinde oluşabilecek potansiyel zararları önlemek adına gerekli tedbirlerin alınmadığının göstergesi olduğu” şeklindedir.

³⁰⁰ Kişisel Verileri Koruma Kurulu’nun 16.06.2020 tarihli kararına konu olayda kişisel verilere hukuka aykırı olarak erişim sağlayan kişi, veri sorumlusunun hem eski çalışanı hem de veri sorumlusunun siber güvenlik desteği aldığı şirketin çalışanıdır. Kurul kararında, ilgili hukuka aykırı erişimin şirket

Öyleyse Kişisel Verileri Koruma Kurumu’nun, veri ihlalinin tespiti halinde şirket içi ilgili birimler arasında hızlı bir raporlama sistemi bulunması, çalışanlara veri güvenliğine yönelik eğitim verilmesi, güvenlik duvarlarının güncel ve kontrol altında tutulması, kişisel veri içeren panellerin kullanılması halinde bu panellerde erişim yetkilerinin önceden belirlenmesi, yetki matrisi oluşturulması ve erişim yetkilerinin düzenli olarak kontrol edilmesi gibi beklentilerinin olduğu söylenebilir. Tam da bu noktada bir teknik tedbir olarak veri sorumlularının belirli periyotlarla sızma testi yaptırmalarının da faydalı olacağı kanaatindeyiz. Zira bu testler ile veri sorumlusu, herhangi bir riski mevcut ise riski ortadan kaldırma imkanına sahip olabilmektedir.

Kişisel Verileri Koruma Kurulu’nun 06.07.2021 tarihli kararına³⁰¹ konu olayda ise fiziken gerçekleşen bir hukuka aykırı erişim söz konusudur. Veri sorumlusu olan bir özel hastanenin işyeri bilgisayarından, bir kişi, ilgili personele fark ettirmeden ekranın fotoğrafını çekmiş, çektiği fotoğrafı bir dava dosyasına sunmuştur. Çektiği fotoğraf boşandığı eşinin yeni doğan oğluna ait doğum belgesine ilişkindir. Kişisel Verileri Koruma Kurulu verdiği kararda, her ne kadar ilgili personele eğitim de verilse, gerekli politika ve prosedürler bulunsun da ihlal meydana geldiği için alınan tedbirlerin yetersiz olduğuna kanaat getirmiştir.

çalışanlarının sisteme girememesi neticesinde fark edilmesinden hareketle veri sorumlusunun sızma testi, risk analizi, log kayıt takibi gibi veri güvenliğini sağlayacak önlemler almadığına kanaat getirmiştir “İlaç sektöründe faaliyet yürüten bir veri sorumlusunun veri ihlali bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 16/06/2020 tarih ve 2020/463 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.08.2023), kararın ilgili kısmı aynen “*Veri sorumlusu, sistemlerine düzenlenen söz konusu saldırıyı şirket çalışanlarının sistemlere erişememesi sonucu tespit ettiği; özel nitelikli kişisel veriler üzerinde çalışan çok uluslu bir şirketin, böylesi saldırılar için sızma testleri ve risk analizleri yapıp tehditleri belirlemesi ve güvenlik açıklarını kapatması ve log kaydı takibi ile veri güvenliğini sağlayacak önlemler alması gerektiği ve bu durumun Kişisel Veri Güvenliği Rehberi 3.2. maddesinde; “Kişisel Veri Güvenliğinin Takibi” başlığı altında; “...güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaaflara karşı korunması için düzenli olarak zaaflar taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir...” ifadelerine aykırılık teşkil ettiği*” şeklindedir.

³⁰¹ “Şikâyetçinin yeni doğan bebeğine ait doğum belgesinde yer alan kişisel verilerin üçüncü kişiler tarafından Özel Hastane olarak faaliyet gösteren veri sorumlusundan hukuka aykırı olarak ele geçirilmesi” hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarihli ve 2021/666 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.08.2023), kararın ilgili kısmı aynen “*Her ne kadar veri sorumlusu tarafından hasta bilgi gizliliği, hasta mahremiyeti, hasta dosyalarının gizliliği, hasta bilgilerinin paylaşılması, hastane dışına çıkarılmaması gerekliliği vb. konularda çalışanlara sürekli eğitimler verildiği ve sürece ilişkin yazılı kurumsal dokümanlar oluşturulduğu ifade edilse de söz konusu olayın meydana geldiği ve kişisel veri ihlaline neden olduğu, Veri sorumlusu hastane tarafından kişisel verilere hukuka aykırı erişimi önlemek adına alınan idari ve teknik tedbirlerin yetersiz kaldığı ve sonuç olarak şikâyetçinin velisi bulunduğu ilgili kişiye ait kişisel verilerin üçüncü kişilerce erişimine neden olduğu*” şeklindedir.

Netice itibariyle, veri sorumlusu yukarıda belirttiğimiz idari tedbirlere ilaveten veri güvenliğinin teminine yönelik yetki kontrolü, yetki matrisi, erişim logları, ağ güvenliği, uygulama güvenliği, sızma testleri yaptırılması, saldırı tespit ve önleme sistemleri kullanılması, veri kaybı önleme yazılımları kullanılması, güvenlik duvarı kullanılması, güncel anti-virüs sistemleri kullanılması gibi teknik anlamda da tedbirlerini almalıdır.

Ç-KİŞİSEL VERİLERİN MUHAFAZASINI SAĞLAMA YÜKÜMLÜLÜĞÜ

Kişisel verilerin muhafazasını sağlama yükümlülüğü KVKK m. 12/ f. 1, c bendinde düzenlenmiştir. Kişisel verilerin muhafazası aslında kişisel verinin bulunduğu ortama yönelik bir düzenlemedir. Kişisel verinin doğru yerde muhafaza edilip edilmediği, yükümlülüğün ifası kapsamında son derece önem arz etmektedir.³⁰² Belirtmekte fayda var ki genellikle bu yükümlülüğün ihlal edildiği durumlarda kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğü de ihlal edilmektedir.

Kişisel verilerin muhafazasını sağlama yükümlülüğünün yerine getirilebilmesi için kişisel verilerin bulunduğu fiziki ve dijital ortamların güvenli olması gerekmektedir. Özellikle dijital ortamlarda muhafazayı sağlama amacıyla uygun güvenlik düzeyinin temini son derece önemlidir. Nitekim Kişisel Verileri Koruma Kurulu bir kararında³⁰³ veri sorumlusu hastaneye ait olan mobil uygulamadan alınan ekran görüntüsünün başka bir cihaz tarafından çekilmesi ve sosyal mecralarda paylaşılması olayında veri sorumlusunun kişisel verilerin muhafazasını sağlama yükümlülüğüne aykırı hareket ettiğine kanaat getirmiştir.

Kişisel Verileri Koruma Kurulu'nun 14.02.2019 tarihli kararına³⁰⁴ konu olayda ise veri sorumlusu teknik servis hizmeti sunan bir firmadır. Firma tarafından sürecin

³⁰² Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi**, s. 12, (www.kvkk.gov.tr), (Erişim: 15.08.2023)

³⁰³ Kişisel Verileri Koruma Kurulu, "Özel Nitelikli Kişisel Verilerin Kanuna Aykırı Şekilde İnternet ve Sosyal Medya Mecralarında Paylaşılması" isimli kararı, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen "*İlgili kişiye ait özel nitelikli kişisel veri olan sağlık raporunun, bir Hastane nezdinde hastaların tedavi sürecinde yer alan hekimler tarafından, veri sorumlusuna ait mobil olarak kullanılan bir uygulamadan alınan ekran görüntüsünün başka bir cihaz tarafından çekilmesi suretiyle internet ve sosyal medya mecralarında paylaşılması ve bu itibarla özel nitelikli bir kişisel verinin sosyal medya aracılığıyla geniş bir kitleye ifşa edilmiş olduğu dikkate alınarak, Kurulca yapılan resen inceleme neticesinde; 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasının (c) bendi kapsamında kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin edemeyen veri sorumlusu hakkında Kanunun 18 inci maddesi uyarınca idari para cezası uygulanmıştır.*" şeklindedir.

³⁰⁴ "Teknik servis hizmeti veren firmanın müşterilerine verdiği form/takip numarasının son hanelerinin değiştirilmesi yoluyla farklı kişilere ait kişisel verilere ulaşıldığı yolunda Kuruma iletilen ihbarın

takip edilebilmesi için her müşteriye bir form numarası verilmekte ve verilen numaradan cihazın durumu sorgulanabilmektedir. Ancak verilen form numaraları birbirlerini takip edecek şekilde verildiğinden ilgili kişiye verilen numaranın bir sonraki veya önceki sayısı girildiğinde başka bir kişiye ait kişisel verilere erişim sağlanabilmektedir. Kurul kararında kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik tedbirlerinin alınmadığı belirterek şirket hakkında idari para cezası yaptırımını uygulamıştır.

Konuyla ilgili ele alacağımız son karar ise Kişisel Verileri Koruma Kurulu’nun 16.01.2020 tarihli kararıdır.³⁰⁵ Karara konu olayda, veri sorumlusu olan banka, kredi kartı teslimat işlemleri için bir firma ile anlaşmıştır. Firma çalışanı, ilgili kişiye ait kredi kartını önce banka sistemlerinde bulunan ilk adrese teslim amaçlı götürmüş, burada kimseye ulaşamayınca sistemde kayıtlı ikinci adrese götürmüştür. Ancak banka sisteminde kayıtlı olan adres ilgili kişinin eski işyeri adresi olup kart da buradaki konu dışı üçüncü bir şahsa teslim edilmiştir. Kurul bu konuya ilişkin kararında dağıtımı yapan kuryenin kartı teslim edeceği kişi bakımından hatalı davrandığını tespit etmiş fakat veri sorumlusu banka olduğu için bankanın kart teslimine ilişkin kişisel verilerin muhafazasını sağlamaya yönelik yeterli tedbirleri almadığına kanaat getirmiştir. Buradan hareketle, veri sorumlusunun dış kaynaktan hizmet temin ettiği süreçlerde dahi verilerin muhafazasını teminen yeterli tedbirlerin alınması gerektiği söylenebilir.

incelenmesi ve ihbara ilişkin alınan Kurul Kararının yerine getirilmemesi hakkında” Kişisel Verileri Koruma Kurulunun 14/02/2019 tarihli ve 2019/23 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “*Veri sorumlusundan alınan bilgide, ilgili internet adresi üzerinden kişilerin servise bıraktıkları cihazları ile ilgili olarak yapılan sorgulamada cihaz sahiplerinin kişisel verilerine erişimin mümkün olmadığına belirtilmesine rağmen yapılan incelemede söz konusu internet sitesinde herhangi bir sorgu numarasının son iki hanesini değiştirmek suretiyle başka cihaz ve sahiplerine ilişkin de sorgulamalar yapılabildiği, söz konusu sorgulamalar neticesinde açılan sayfada yönlendirilen muhtelif linklerin seçilmesi suretiyle de bu kişilere ait isim, soy isim, adres ve sahip oldukları cihaz IMEI numarası bilgilerine erişim sağlanabildiği dikkate alınarak, anılan Şirket tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasına aykırı olarak kişisel verilerin muhafazasının sağlanmasını teminen gerekli idari ve teknik tedbirlerin alınmaması nedeniyle, söz konusu aykırılığın Karar tarihi itibarıyla yapılan sorgulamalarda devam ettiği de göz önünde bulundurulduğunda, veri sorumlusu hakkında Kanunun 18 inci maddesi çerçevesinde 150.000 TL idari para cezası uygulanmasına*” şeklindedir.

³⁰⁵ Bir banka tarafından ilgili kişinin kredi kartının rızası dışında üçüncü kişilere teslim edilmesine ilişkin Kişisel Verileri Koruma Kurulu’nun 16/01/2020 Tarih ve 2020/32 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 15.08.2023), kararın ilgili kısmı aynen “*Somut olay açısından Bankanın kart teslimi sırasında kişisel verilerin muhafazasını sağlamaya yönelik yükümlülükleri doğrultusunda yeterli idari ve teknik tedbirleri almadığı, ilgili kişiye ait verilerin güncelliğini sağlamak açısından yeterli ve makul çabayı göstermediği, değerlendirilmiş olup, bu durumun Kanunun 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği kanaatine varılması nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında Banka hakkında 50.000 TL idari para cezasına hükmedilmesine karar vermiştir.*” şeklindedir.

Kararlara konu olaylardan açıkça anlaşılacağı üzere kişisel verilerin muhafazasını sağlama yükümlülüğü bazen bir ihmalden, bazen hatalı bir işlem, bazen de kontrolsüzlükten kaynaklanabilir. Bu nedenle veri sorumlusu, KVKK kapsamında bir risk tespiti yapmalı ve en ufak risk barındıran noktalar için dahi tedbir almalıdır. Örneğin bir şirkette özlük dosyalarının kilitli dolapta saklanması, çalışan bilgisayarlarında ekran koruyucu kullanılması, çalışan bilgisayarlarının yönünün bekleme salonlarına ya da koridorlara doğru değil duvarlara doğru çevrilmesi bile bu yükümlülüğün yerine getirilmesi kapsamında alınabilecek tedbirlerdendir.

Yeri gelmişken belirtmekte fayda var ki alınacak tedbirlerin seviyesi veri sorumlusunun faaliyette bulunduğu sektör, söz konusu kişisel veri miktarı, kaç kişiye ait kişisel verinin bulunduğu gibi faktörler uyarınca farklılık arz edebilecektir. Örneğin bir bankanın veri merkezine girişte, içeri girecek kişinin içeriye bir teknolojik ekipman yerleştirmesi veya içeriden bir parça alması ihtimaline istinaden ilgili kişinin girişte ve çıkışta tartılması dahi bir tedbir olarak düşünülebilir. Hatırlatmakta fayda var ki eğer veri sorumlusu aldığı tedbir kapsamında kişisel veri işleyecek ise daha önce anlattığımız hususlar uyarınca genel ilkelere dikkat etmeli ve KVKK m. 5 ve KVKK m. 6 hükümlerine uygun hareket etmelidir.

D-VERİ İHLALİ BİLDİRİM YÜKÜMLÜLÜĞÜ

Veri ihlal bildirim yükümlülüğü KVKK m. 12/ f. 5'te düzenlenmiştir.³⁰⁶ Maddede belirtilen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hali aslında KVKK m. 12/ f. 1, b bendinin ihlal edilmesi durumudur. Bu yükümlülük uyarınca kanun koyucu, veri sorumlusunun kendisini ihbar etmesini beklemektedir.³⁰⁷ Böyle bir durumla karşılaşan veri sorumlusu en hızlı sürede Kişisel

³⁰⁶ KVKK m. 12/ f. 5 aynen “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” şeklindedir.

³⁰⁷ Veri ihlal bildirim yükümlülüğü kapsamında gerek KVKK'nin sistematığının gerekse kişisel verilerin korunması anlayışının ülkemizde yeni yeni oturmaya başlaması sebebiyle hatalı olduğu kanaatindeyim. Zira bir veri sorumlusu kendini ihbar ettiğinde Kişisel Verileri Koruma Kurulu tarafından denetlenmenin kapısını aralamış olacak ve her halükarda bir para cezasıyla karşı karşıya kalacaktır. Bu durumda veri sorumlusunun veri ihlaline ilişkin bildirimde bulunması ile bulunmaması arasındaki tek fark bu durumun bir şekilde Kişisel Verileri Koruma Kurumu tarafından tespiti halinde ihlalin bildirilmemesi sebebiyle uygulanacak olan idari para cezasıdır. Çoğu veri sorumlusu da bu riski “Kurum veri ihlali gerçekleştiğini nereden bilecek?” düşüncesiyle göze alarak veri ihlal bildiriminde bulunmamaktadır. Gerçekten de ülkemizde her gün yüzlerce siber saldırı olayı gerçekleşmekte ve birçok veri sorumlusu tarafından kişisel veriler güvenli şekilde muhafaza edilememektedir. Bu noktada Türkiye'deki veri sorumlularının çok küçük bir kısmının veri ihlal bildiriminde bulunduğu da bir gerçektir. Kanaatimizce bu uygulama kişisel verilerin korunmasına fayda sağlamaktan çok zarar vermektedir. Zira veri ihlali meydana gelen durumlarda bu durumu saklayan her veri sorumlusu ihlalden

Verileri Koruma Kurumu'na veri ihlal bildiriminde bulunmalıdır. Akabinde veri ihlalden etkilenen ilgili kişilere de bu durumu bildirmelidir. Burada hedeflenen, ihlalden etkilenen kişilerin ihlalden sonraki süreçte kişisel veri güvenliğini bireysel olarak sağlayabilmesidir.

Maddede belirtilen en kısa süre, Kişisel Verileri Koruma Kurulu tarafından maksimum yetmiş iki saat olacak şekilde yorumlanmaktadır.³⁰⁸ Sürenin başladığı an, veri sorumlusunun veri ihlalini tespit ettiği andır. Belirlenen süre içerisinde veri ihlal bildiriminde bulunmayan veri sorumluları hakkında, KVKK m. 18/ f. 1, b bendi uyarınca Kişisel Verileri Koruma Kurulu'nun idari para cezası yaptırımını uygulama yetkisi vardır.

Veri ihlal bildirimini, ihlalden etkilenen ilgili kişilerin mağduriyetini azaltmak için bazı önemli durumlarda Kişisel Verileri Koruma Kurulu tarafından duyuru olarak yayınlanmaktadır.³⁰⁹ Belirtmek gerekir ki veri ihlali yaşanması halinde şirket tarafından nasıl bir yol izleneceği, Kişisel Verileri Koruma Kurulu'na ihbar bildirimini kim tarafından ne zaman yapılacağı hususlarının düzenlendiği veri ihlali müdahale politikası, bu sürecin en az hasarla atlatılabilmesi için çok faydalı olacaktır. Nitekim Kişisel Verileri Koruma Kurulu da veri ihlali müdahale politikasının gerekliliğine vurgu yapmaktadır.³¹⁰

etkilenen ilgili kişilere zarar vermekte ve savunma imkanı bırakmamaktadır. Veri ihlal bildirimini ile hedeflenen, ilgili kişilerin ihlalden minimum derecede etkilenmesini sağlamak ise veri ihlal bildirimini neticesinde veri sorumlusuna para cezası yaptırımını uygulamak yerine aksine teşvik edici yollar tercih edilmelidir. Veri ihlal bildirim sayılarını arttırmanın ve ilgili kişileri korumanın tek yolu, bu konuda veri sorumlusunu cezalandırmaktan ziyade teşvik etme yolunun tercih edilmesidir. Örneğin veri ihlal bildiriminde bulunan veri sorumluları hakkında yapılacak inceleme neticesinde hükmedilecek idari para cezasının %25 oranında indirilmesi teşvik edici bir davranış olacaktır.

³⁰⁸ Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru, (www.kvkk.gov.tr), (Erişim: 17.08.2023), duyurunun ilgili kısmı aynen “*Kanunun 12 nci maddesinin (5) numaralı fıkrasının “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir....” hükmünde yer alan “en kısa sürede” ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusuna söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşabiliyorsa doğrudan, ulaşamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına*” şeklindedir.

³⁰⁹ Kişisel Verileri Koruma Kurulu'nun web sitesinde yayınlanan “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Dagi Giyim Sanayi ve Ticaret AŞ”, “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Atatürk Üniversitesi”, “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Gulf Sigorta AŞ”, “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – UPS Hızlı Kargo Taşımacılığı AŞ” isimli duyurular örnek verilebilir. (www.kvkk.gov.tr), (Erişim: 17.08.2023)

³¹⁰ Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyuru, (www.kvkk.gov.tr), (Erişim: 17.08.2023)

Kanaatimizce, veri ihlal bildirim yükümlülüğü ve idari yaptırımlara ilişkin mevcut düzenlemeler, veri ihlaline maruz kalan şirketi, ihlal bildiriminde bulunmaya teşvik etmeyip aksine veri ihlalini gizlemeye itmektedir. Bu görüşümüzün temelinde, Kişisel Verileri Koruma Kurulu'nun, gerekçesi ne olursa olsun her veri ihlal bildirimini halinde idari para cezası yaptırım uygulama eğilimi yer almaktadır. Uygulamada veri ihlali ile karşılaşan çoğu veri sorumlusu da bu sebeple kendisini ihbar etmemeyi tercih etmektedir. Bu durumu tersine çevirmenin yolu ise onarıcı adalet yaklaşımının benimsenmesidir. KVKK bir bütün olarak incelendiğinde, veri sorumlusunun Kişisel Verileri Koruma Kurumu ile işbirliği içerisinde hareket etmesinin ve şeffaf davranmasının herhangi bir karşılığı bulunmamaktadır.

Öte yandan, GDPR uyarınca denetim makamı ile gerçekleştirilen işbirliği derecesi, idari para cezasına hükmedilip hükmedilmeyeceği ve hükmedilecekse miktarın tespiti noktasında bir kriter olarak yer almaktadır. Bu düzenleme, veri sorumlusu ile denetim makamı arasındaki ilişkiyi güçlendirecek niteliktedir. Zira burada bir ödüllendirme söz konusudur. KVKK'de ise her halükârda veri sorumlusu hakkında idari yaptırım uygulandığı için veri sorumlusu ihbar bildiriminde bulunmaktan imtina etmektedir. Özellikle, Kişisel Verileri Koruma Kurulu'nun da re'sen denetim yapmak suretiyle ihlal bildiriminde bulunmayan şirketleri tespit etme gibi bir eğilimi söz konusu olmadığı için veri sorumluları bu konuda son derece rahat hareket etmektedir. Bu nedenle, yaptığımız tüm açıklamalar uyarınca veri ihlal bildirimine ilişkin maddenin yeniden ele alınması gerektiği ve ihlale maruz kalan veri sorumlusu ile Kişisel Verileri Koruma Kurumu arasındaki işbirliğinin, yaptırım uygulayıp uygulamama noktasında bir kriter olarak getirilmesi gerektiği kanaatindeyiz.

Ayrıca belirtmek isteriz ki veri ihlal bildirim yükümlülüğüne ilişkin mevcut düzenleme ve Kişisel Verileri Koruma Kurulu'nun konuyla ilgili genel eğilimi göz önünde bulundurulduğunda bir veri sorumlusu için en güvenli yollardan birisi, siber risk sigortası yaptırmaktır. Bu kapsamda, veri sorumlusunun veri ihlal bildirimini sebebiyle karşılaşacağı idari yaptırımın, veri sorumlusunun uğrayacağı itibar kaybının ve veri ihlali nedeniyle ortaya çıkan zararların teminat kapsamına alınması

mümkündür.³¹¹ Bu nedenle siber risk sigortası, veri ihlali riskine karşı veri sorumlusunu güvence altına alan önemli bir araçtır.

Sonuç olarak mevcut düzenleme uyarınca bir veri sorumlusu, veri ihlalinin tespit ettiği andan itibaren hızlı bir şekilde gerekli güvenlik işlemlerini tesis etmeli, yetmiş iki saat içerisinde Kişisel Verileri Koruma Kurumu'na bildirimde bulunmalı ve en kısa süre içerisinde de ihlalden etkilenen ilgili kişileri bilgilendirmelidir.³¹²

IV-İLGİLİ KİŞİLER TARAFINDAN YAPILAN BAŞVURULARIN CEVAPLANMASI YÜKÜMLÜLÜĞÜ

Veri sorumlusunun ilgili kişi tarafından yapılan başvuruları cevaplandırma yükümlülüğü, KVKK m. 11 ve KVKK m. 13 hükmünden doğmaktadır. KVKK m. 11, ilgili kişiye belirli bazı haklar tanımaktadır.³¹³ İlgili kişi, bu haklarını kullanabilmek için öncelikle veri sorumlusuna başvurmalıdır.³¹⁴ Veri sorumlusu da aldığı bu başvuruları cevaplandırmakla yükümlüdür. Nitekim KVKK m. 13/ f. 2 aynen “*Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifiedeki ücret alınabilir.*” şeklinde olup KVKK m. 13/ f. 3 de aynen “*Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.*” şeklindedir.

³¹¹ Sinan ŞEKEROĞLU/ Haşim ÖZÜDOĞRU, **Dijital Dönemin Koruyucuları: Siber Risk Sigortaları**, 4. Uluslararası Sosyal Bilimler Araştırmaları Kongresi, 2019, s. 61 vd.

³¹² Veri ihlal bildirimi, Kişisel Verileri Koruma Kurumu'nun web sitesi üzerinden online olarak da yapılabilmektedir. (<https://ihlalbildirim.kvkk.gov.tr/>)

³¹³ Bu kapsamda ilgili kişi, veri sorumlusuna başvurmak suretiyle KVKK m. 11/ f. 1, a bendi uyarınca kişisel verisinin işlenip işlenmediğini öğrenme, KVKK m. 11/ f. 1, b bendi uyarınca kişisel verileri işlenmişse buna ilişkin bilgi talep etme, KVKK m. 11/ f. 1, c bendi uyarınca kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, KVKK m. 11/ f. 1, ç bendi uyarınca yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, KVKK m. 11/ f. 1, d bendi uyarınca kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, KVKK m. 11/ f. 1, e bendi uyarınca 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, KVKK m. 11/ f. 1, f bendi uyarınca (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, KVKK m. 11/ f. 1, g bendi uyarınca işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, KVKK m. 11/ f. 1, ğ bendi uyarınca kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

³¹⁴ KVKK m. 13/ f. 1 aynen “*İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.*” şeklindedir.

Öyleyse veri sorumlusu, KVKK kapsamında kendisine gelen bir başvuruyu kabul etmek zorunda değildir ancak başvuruyu neticelendirmekle yükümlüdür. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ³¹⁵ m. 6 da veri sorumlusunun bu yükümlülüğünü düzenlemekte olup aynen “*Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.*” şeklindedir.

KVKK uyarınca öngörülen başvuru ve şikayet usulü iki aşamadan oluşmaktadır. İlgili kişi, KVKK kapsamında bir veri sorumlusunu şikayet etmek istiyorsa öncelikle veri sorumlusuna başvuruda bulunmak zorundadır. KVKK m. 14/ f. 2 hükmü aynen “*13 üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.*” şeklinde olup veri sorumlusuna başvuruyu zorunlu kılmaktadır.

Veri sorumlusuna yapılan başvurunun ardından farklı ihtimaller söz konusu olabilir. Birinci ihtimalde veri sorumlusu, ilgili kişinin talebini kabul edebilir. Bu durumda veri sorumlusunun yapması gereken, talep doğrultusunda işlem yapmak ve ilgili kişiyi durum hakkında bilgilendirmektir.

Bazı hallerde talebin kabul edilmesi yine de kişisel verinin işlendiği dönem için hukuka aykırılığı ortadan kaldırmaz. Bu gibi durumlarda ilgili kişinin yine de şikayet hakkı bulunmaktadır. Örneğin ilgili kişi açık rızası olmadığı halde kendisine neden reklam amaçlı SMS gönderildiği konusunda ve hangi veri işleme şartına dayanıldığı konusunda bilgi talep edilebilir ve kendisine bundan sonra SMS gönderilmemesini isteyebilir. Veri sorumlusu da ilgili kişiden özür dileyerek sistemsal bir hata olduğunu belirtebilir ve bundan sonra kendisine SMS gönderilmeyeceğinin taahhüdünü verebilir. Öte yandan talebin kabulü, ilgili kişinin kişisel verilerinin hukuka aykırı olarak işlendiği gerçeğini ortadan kaldırmaz. Bu durumda salt başvuru kabul edildiği gerekçesiyle şikayet yolunun kapandığı söylenemez. İlgili kişi, yine de Kişisel Verileri Koruma Kurumu’na şikayette bulunabilir.

İkinci ihtimalde ise veri sorumlusu ilgili kişinin talebine cevap vermeyebilir. Bu durumda genellikle veri sorumlusu ya KVKK kapsamındaki yükümlülüklerini

³¹⁵ RG., 30356 S., 10.03.2018 T.

bilmemektedir ve böyle bir durumla ilk defa karşılaşmıştır ya da ilgili kişinin yaptığı başvuruyu önemsememektedir. Gerekçe ne olursa olsun bu gibi durumlarda ilgili kişinin Kişisel Verileri Koruma Kurumu'na şikayet yolu açıktır. Nitekim Kişisel Verileri Koruma Kurumu'nun bir kararına konu olayda veri sorumlusu ilgili kişinin talebine cevap vermemiş ancak Kişisel Verileri Koruma Kurumu kendisinden savunma istediği zaman savunma sunmuştur.³¹⁶

Hemen belirtmek gerekir ki Kişisel Verileri Koruma Kurumu'nun sadece veri sorumlusunun yasal süre içerisinde cevap vermemesinden dolayı veri sorumlusu hakkında idari yaptırım uygulama yetkisi yoktur. Nitekim bu konuyu, Kişisel Verileri Koruma Kurulu da bir kararında aynen ifade etmiştir.³¹⁷

Üçüncü bir ihtimal ise veri sorumlusunun başvuruya cevap vermesi ancak cevabın yeterli olmaması ya da çok genel nitelikte olup talebe özgü nitelikte olmamasıdır. Bu durumda da ilgili kişinin Kişisel Verileri Koruma Kurumu'na şikayet hakkı bulunmaktadır. Nitekim Kişisel Verileri Koruma Kurulu'nun bir kararına konu olayda ilgili kişi, veri sorumlusunun kendisine verdiği cevabın yeterli olmadığından bahisle şikayette bulunmuştur.³¹⁸

Bir başka karara konu olayda ise ilgili kişi, kendisine özel bir cevap verilmek yerine çok genel nitelikte, konuya özgülenmemiş bir cevap verildiğinden bahisle şikayette bulunmuştur.³¹⁹ Kişisel Verileri Koruma Kurulu'nun 05.05.2020 tarihli

³¹⁶ “Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu verisini ilgili kişinin açık rızasını almaksızın işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1357 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023)

³¹⁷ “Bir uçak bileti satış firması olan veri sorumlusu hakkındaki şikayetle ilgili” Kişisel Verileri Koruma Kurulunun 06.02.2020 Tarihli ve 2020/86 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), kararın ilgili kısmı aynen “*Kanunun 13 üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 6 ncı maddesinde veri sorumlusunun ilgili kişi başvurularını etkin bir şekilde sonuçlandırma yükümlülüğünün düzenlediği, veri sorumlusu tarafından ilgili kişinin başvurularına cevap verilmemesi ya da cevabın yetersiz bulunması halinde ilgili kişiye Kurula şikayet hakkı tanınmışsa da sadece başvuruya cevap verilmemesi sebebiyle veri sorumlusuna uygulanabilecek bir idari yaptırım türüne Kanunda yer verilmediği*” şeklindedir.

³¹⁸ “Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlemesi” hakkında Kişisel Verileri Koruma Kurulunun 19/01/2023 tarihli ve 2023/86 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023)

³¹⁹ “İlgili kişinin telefon numarasının hastaneden ayrılan doktor tarafından SMS gönderilmesi suretiyle işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 08/09/2022 tarihli ve 2022/923 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), İlgili kişinin taleplerinin özetlendiği bölümün ilgili kısmı aynen “*Konuya ilişkin ilgili doktora ve hastaneye başvurduğu, doktorun cevabında kendisine ait verilerini sağlık durumunun kontrolü amacıyla aldığını belirttiği, hastanenin cevabında ise başvurusuna konu ettiği kişisel verilerine ilişkin özel bilgi vermek yerine genel nitelikte ve konuya özgü olmayan bir cevap verildiği, bu çerçevede taraflardan yeterli bir cevabın alınamadığı*” şeklindedir.

kararına³²⁰ konu olayda ise veri sorumlusu, ilgili kişinin başvurusuna cevap vermiş ancak cevabı doğrudan ilgili kişiye tebliğ etmek yerine resmi yazı şeklinde ilgili kişinin çalıştığı birime göndermiştir. Bu uygulama Kurul tarafından ilgili kişisel verilerin üçüncü kişilerin erişimine sebebiyet vermesi sebebiyle hatalı olarak değerlendirilmiş ve veri sorumlusu hem usulüne uygun cevaplandırma konusunda talimatlandırılmış hem de KVKK m. 12/ f. 1 hükmü ihlal edildiğinden veri sorumlusu hakkında idari para cezası yaptırımını uygulanmıştır.

Dolayısıyla bir şirketin ilgili kişiye vereceği cevap, talep konusuyla ilgili olmalı, genel nitelikte olmamalı, sorulan her bir soruya ayrı ayrı cevabı içermeli, ilgili kişinin anlayabileceği açıklıkta olmalıdır. Ayrıca cevap 30 gün içerisinde verilmelidir. Aksi takdirde ilgili kişi, Kişisel Verileri Koruma Kurumu'na şikayette bulunabilecektir.

Dördüncü bir ihtimal olarak veri sorumlusu ilgili kişinin başvurusunu reddedebilir. Veri sorumlusunun başvuruyu reddi farklı gerekçelerden kaynaklanabilir. Örneğin ilgili kişinin başvurusunda usulen bir eksiklik bulunabilir veya ilgili kişinin başvurusu değerlendirmeye alınıp reddine karar verilmiş olabilir.

Veri sorumlularının en yaygın başvuru ret gerekçeleri arasında ilgili kişinin kimlik teyidinin yapılamaması yer almaktadır. Hemen belirtmek gerekir ki veri sorumlusu açısından kimlik teyidi yapılması son derece kolaydır. Özellikle ilgili kişiden teyit amaçlı istenilecek bilgiler ile kimlik teyidi yapılabilir. Nitekim Kişisel Verileri Koruma Kurulu'nun 07.11.2019 tarihli kararına konu olayda veri sorumlusu, kimlik teyidi yapamadığını, ilgili kişinin başvurusunun Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olmadığını, buradan hareketle

³²⁰ “İlgili kişinin kendisine iletilmesi gereken cevap yazısının veri sorumlusu tarafından resmi yazı şeklinde, çalıştığı birime gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 05/05/2020 tarihli ve 2020/336 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), kararın ilgili kısmı aynen “*Kişisel verilerin işlenmesi faaliyetinin Kanunun 3 üncü maddesinde kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlandığı, bu çerçevede başvuruya konu olayda ilgili kişinin Bilgi Edinme Hakkı Kanunu kapsamında veri sorumlusuna başvurusuna verilen yanıtın, ilgili kişinin çalıştığı birime gönderilmesi suretiyle kişisel verilerinin açıklanmasında Kanunun 5 inci maddesi kapsamında herhangi bir hukuki dayanak söz konusu olmadığından veri sorumlusu tarafından Kanunun 12 inci maddesinin (1) numaralı fıkrası kapsamında kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmadığı kanaatine varıldığı*” şeklindedir.

ilgili kişinin başvurusuna cevap vermediğini savunmuştur. Kurul ise ilgili kişiden alınabilecek bazı cevaplar ile kimlik teyidinin sağlanmasının mümkün olduğu değerlendirmesinde bulunmuş ve konu hakkında veri sorumlusunu talimatlandırmıştır.³²¹ Bu noktada Kişisel Verileri Koruma Kurumu'nun bakış açısının, başvuru evrakı itibarıyla kimlik teyidinin mümkün olmaması halinde salt bu gerekçe ile başvurunun reddedilmemesi veya cevapsız bırakılmaması gerektiği, aksine ilgili kişiden teyit amaçlı bilgi istenilmesi gerektiği yönünde olduğu anlaşılmaktadır.

Ayrıca belirtmekte fayda var ki kimlik teyidi yapabilmek için bazı veri sorumluları kimlik fotokopisi talep edebilmektedir. Bu uygulama son derece sakıncalıdır zira eski kimliklerde kan grubu bilgisi ve din bilgisi gibi özel nitelikli kişisel veriler yer almaktadır. İlgili kişinin kan grubu bilgisi veya din bilgisi, veri sorumlusunun, kimlik teyidi açısından ihtiyaç duymayacağı verilerdir. Nitekim Kişisel Verileri Koruma Kurulu da bir kararında veri sorumlusunun ilgili kişiden kimlik teyidi amaçlı ek bilgi istemesinin mümkün olduğunu ancak kimlik fotokopisi talep edilmesinin KVKK açısından hukuka aykırılığa sebebiyet vereceğini belirtmiştir.³²²

Kurul kararına konu olan bir başka olayda ise ilgili kişinin ad soyadında bir harfi yanlış yazması sebebiyle veri sorumlusu, ilgili kişinin adını kayıtlarında bulamadığı için talebini işleme almamıştır.³²³ Kişisel Verileri Koruma Kurulu bu

³²¹ “Telekomünikasyon sektöründe faaliyet gösteren veri sorumlusu tarafından şikayetçiye, ad ve soyadı benzerliği olan başka bir abonesinin fatura bilgilerinin e-posta yoluyla iletilmesi hakkında” Kişisel Verileri Koruma Kurulunun 07/11/2019 Tarihli ve 2019/333 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023)

³²² “Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu” hakkında Kişisel Verileri Koruma Kurulunun 01.10.2019 Tarihli ve 2019/294 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), Kararın ilgili kısmı aynen “Diğer yandan, veri sorumlusunun, Kanun kapsamındaki başvurusuna cevap verebilmek amacıyla ilgili kişinin kimliğinin teyidi noktasında ek bilgi istemesinin yerinde olduğu değerlendirilmekle birlikte, ilgili kişinin din ve kan grubu gibi özel nitelikli kişisel verilerini de içeren arkalı önlü kimlik görüntüsünün talep edilmesinin, Kanunun “Genel İlkeler” başlıklı 4 üncü maddesinde düzenlenen “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesine uygun olmadığı gibi, Kanunun özel nitelikli kişisel verilerin işlenmesini düzenleyen 6 ncı maddesine de uygun olmadığı, zira veri sorumlusunun da yapığı savunmada, somut olayda çağrı merkezi ekibi tarafından yazılı çalışma kurallarına aykırı şekilde kimlik belgesi talep edildiğini belirterek, olaya ilişkin ikrarda bulunduğu” şeklindedir.

³²³ “İlgili kişinin uluslararası geçerliliği olan bir dil sınavı konusunda Türkiye’deki akredite kuruluş tarafından kişisel verilerinin hukuka aykırı işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 12/08/2021 tarihli ve 2021/799 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), kararın ilgili kısmı aynen “İlgili kişinin Türkiye’deki şirketin sisteminde kayıtlı olduğu ve ilgili kişinin kimliğinin tespit edilebileceği anlaşılmış olduğundan bir harf sebebiyle “...başvurucu ismi kayıtlarımızda bulunmamıştır...” şeklinde ilgili kişiye cevap verilmesinin Tebliğin 6 ncı maddesinde belirtilen dürüstlük kuralına uygun olarak değerlendirilmemesi sebebiyle Kanun kapsamında kendisine yapılan başvurulara cevap verirken 6698 sayılı Kanun ve Tebliğin ilgili hükümlerine uyum konusunda gerekli dikkat ve özeni göstermesi gerektiği konusunda uyarılmasının,” şeklindedir.

durumun hukuka ve dürüstlük kuralına aykırı olduğundan bahisle veri sorumlusunu talimatlandırmıştır.

Esasa ilişkin ret gerekçelerine konu bazı olaylarda ise ilgili kişi, veri sorumlusundan belge talep etmekte fakat bu talebini KVKK m. 11 kapsamında bir talep olarak iletmektedir. Bazı veri sorumluları, bilgi ve belge taleplerinin KVKK m. 11 kapsamında değerlendirilemeyeceğinden bahisle bu tarz başvuruları reddedebilmektedir. Ancak ilgili kişinin talep ettiği belge, eğer ilgili kişinin kişisel verisini ihtiva ediyor ise ve ilgili kişinin talebi de KVKK açısından kabul edilebilir bir talep ise bu belgenin ilgili kişi ile paylaşılması gerekmektedir. Nitekim Kişisel Verileri Kurumu da vermiş olduğu bir kararında veri sorumlusu olan kargo firmasının yukarıda izah olunan doğrultudaki savunmasına itibar etmemiş ve veri sorumlusunu talep doğrultusunda işlem yapması hususunda talimatlandırmıştır.³²⁴

Yeri gelmişken belirtmekte fayda var ki, ne yazık ki bazı kamu kurumları, KVKK m. 11 kapsamında kendilerinden talep olunan ve ilgili kişinin kişisel verilerini ihtiva eden belgeleri, ilgili kişiler ile paylaşmamakta ve hatta paylaşmamalarına gerekçe olarak da KVKK'yi gerekçe sunmaktadır. Özellikle bu durum, idari işlemin iptali davası açmak isteyen ilgili kişinin, ilgili kamu kurumundan iptale dayanak olan belgenin bir nüshasını istemesi durumunda gündeme gelmektedir. Yukarıda atıfta bulunulan karardan açıkça anlaşılacağı üzere eğer ilgili kişinin talep ettiği belge, ilgili kişinin kişisel verilerini içeriyor ise ve talebi de KVKK açısından uygun ise bu belgenin ilgili kişi ile paylaşılması gerekmektedir.

Çok nadir de olsa bazen veri sorumlusunun otuz günlük süresi dolar dolmaz ilgili kişi tarafından şikayette bulunulmakta, fakat veri sorumlusu ilgili kişinin talebine bir veya birkaç gün sonra cevap verebilmektedir. Bu durumda ilgili kişinin başvurusu

³²⁴“Bir kargo firmasında çalışan ilgili kişinin iş akdinin haksız feshedilmesi sonrası özlük dosyası kapsamında yer alan kişisel verilerinin birer suretinin tarafına verilmesi talebine veri sorumlusu tarafından cevap verilmemesi” hakkında Kişisel Verileri Koruma Kurulunun 28/05/2020 tarihli ve 2020/435 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 18.08.2023), kararın ilgili kısmı aynen “İlgili kişinin başvurusunun, Kanunda düzenlenen haklara ilişkin olmadığı ve başvurunun Kanunda düzenlenmeyen bir konu olan belge örneği talebi içerdiği için Kanunun 11 inci maddesi kapsamında karşılanmasının mümkün olmadığı gerekçesiyle veri sorumlusu tarafından 30 günlük yasal süre içerisinde cevaplandırılmadığı dikkate alındığında, ilgili kişiye ait kişisel veri niteliğindeki bilgilerini içeren 30.09.2019 tarihli savunma yazısı ile 18.10.2019 tarihli ve 17.10.2019 tarihli istifa dilekçelerinin birer örneğinin ilgili kişiye verilmesi hususunda Kanunun 15 inci maddesinin (5) numaralı fıkrası kapsamında veri sorumlusunun talimatlandırılmasına, Veri sorumlusunun, ilgili kişiler tarafından Kanun kapsamında yapılan başvurulara yasal süresi içerisinde cevap vermesi noktasında azami dikkat ve özeni göstermesi gerektiği hususunda talimatlandırılmasına karar verilmiştir.” şeklindedir.

açısından herhangi bir problem olmayacaktır. Nitekim Kişisel Verileri Koruma Kurulu da 24.01.2019 tarihli kararında ilgili kişinin, otuz günlük cevap süresinin dolmasıyla birlikte artık ilgili kişinin beklemekle yükümlü olmadığı ve bu sebeple şikayet yoluna başvurabileceğini belirtmiştir.³²⁵

Veri sorumlusunun ilgili kişiye vereceği cevabın taşınması gereken özellikler Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ m. 6/ f. 4'te belirtilmiştir. ³²⁶ Ayrıca ilgili kişinin taleplerine cevap verilirken veri sorumlusu hukuka ve dürüstlük kuralına uygun hareket etmek zorundadır. Tam da bu noktada belirtmekte fayda var ki bazı veri sorumluları tarafından geliştirilmiş, ilgili kişinin başvuru yapmasını engellemeye yönelik uygulamalar söz konusudur. Örneğin bir GSM operatöründen son bir ay içerisinde aradığı kişilerin bilgisini isteyen ilgili kişiye, veri sorumlusu bir e-mail göndermek suretiyle cevap verebilir. Ancak veri sorumlusu bu tarz taleplerin kendi iş yükünü arttıracığından bahisle cevabını yalnızca fiziki olarak iletebileceğini, cevaba konu evrakın 70 sayfa olduğunu, bu durumda 60 TL masrafı³²⁷ olacağını ilgili kişiye iletebilmektedir. Kanaatimizce bu örnekteki uygulama, hukuka ve dürüstlük kuralına aykırı bir uygulamadır. Zira veri sorumlusunun gayesi, ilgili kişinin başvurusunu hızlı ve etkin bir şekilde cevaplandırmaktan ziyade masraf çıkartmak suretiyle gelecek başvuruların önüne geçmek, caydırıcı olmaya çalışmaktır.

Bir başka karşılaşılan örnek de veri sorumlularının web sitesine başvuru formu yüklemeleri ve başvuruyu sadece bu form üzerinden aldıklarını belirtmeleridir. Belirtmek gerekir ki veri sorumlularının başvuru formu oluşturmalarının önünde hiçbir engel yoktur. Öte yandan, başvuruların sadece bu form aracılığıyla yapılması halinde cevap verileceği izlenimi uyandırılması hukuka ve dürüstlük kuralına aykırılık teşkil etmektedir. Zira Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ uyarınca belirtilen usul ve yöntemle her türlü başvuru geçerli bir başvuru olup veri sorumlusunun hazırladığı formların kullanılması zorunluluğu bulunmamaktadır.

³²⁵ Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı, (www.kvkk.gov.tr), (Erişim: 19.08.2023)

³²⁶ Buna göre, verilen cevapta veri sorumlusunun ya da temsilcisine ilişkin kimlik bilgileri, başvuru kişinin adı ve soyadı, Türkiye Cumhuriyeti vatandaşı ise T.C. kimlik numarası, yabancı ise uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas elektronik posta adresi, telefon ve faks numarası, talep konusu, veri sorumlusunun başvuruya ilişkin başvuruya ilişkin açıklamaların bulunması zorunludur.

³²⁷ Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ m. 7/ f. 1 hükmü aynen “İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.” şeklindedir.

Nitekim Kişisel Verileri Koruma Kurulu verdiği bir kararda bu gibi uygulamaların ilgili kişinin yanlış yönlendirilmesine sebebiyet vereceğini ve bunun da hukuka ve dürüstlük kuralına uygun olmayacağını belirtmiştir.³²⁸

Son olarak belirtmek istediğimiz husus, veri sorumlusu tarafından verilecek cevabın yazılı olması veya elektronik ortamda olması gerektiğidir. KVKK m. 13/ f. 3'te düzenlenen bu husustan anlaşılacağı üzere veri sorumlusunun sözlü olarak cevap vermesi, usule uygun bir cevap yöntemi değildir.

Özellikle uygulamada bazı şirketler, yetkilendirdiği bir personel tarafından ilgili kişiyi aramak suretiyle bilgilendirme yolunu tercih edebilmektedir. Bu uygulama ancak bir ön bilgilendirme olabilir. İlgili kişinin muhakkak ya fiziken yazılı olarak ya da elektronik ortamda bilgilendirilmesi gerekmektedir. Nitekim Kişisel Verileri Koruma Kurulu da vermiş olduğu bir kararda, veri sorumlusu olan banka tarafından ilgili kişinin aranmak suretiyle bilgilendirilmesi durumunun usule uygun olmadığını belirtmiştir.³²⁹

Netice itibarıyla veri sorumluları, kendilerine gelen başvuruları muhakkak ya yazılı olarak ya da elektronik ortamda cevaplandırmalı, cevaplandırma sürecinde hukuka ve dürüstlük kuralına uygun hareket etmeli, cevaplandırma işlemini

³²⁸ “Bir operatör şirketinin, ilgili kişinin internet sitesi üzerinden yapmış olduğu başvurusunu kimlik teyidi yapamadığı gerekçesiyle reddetmesine ilişkin olarak Kurula yapılan başvuru” hakkında Kişisel Verileri Koruma Kurulunun 01/10/2019 Tarihli ve 2019/296 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 19.08.2023), kararın ilgili kısmı aynen “*Şirketçe kimlik teyidi sağlamak amacıyla yalnızca noter kanalı veyahut e-imza ile başvuruda bulunabileceğinin bildirilmesi sonucu Kanun’da ya da Tebliğ’de öngörülme maddi bir külfet getirilmesinin ve ilgili kişinin bu şekilde yanlış yönlendirilmesi suretiyle söz konusu KVKK talep formunu doldurarak usule uygun bir başvuru yapma hakkının engellenmesinin Tebliğ’in 6’ncı maddesinde sayılan hukuka uygunluk ve dürüstlük kuralı ile bağdaşmayacağı dikkate alındığında, Tebliğ hükümlerine uyum konusunda azami dikkat ve özenin gösterilmesi hususunda Şirketin talimatlandırılmasına*” şeklindedir.

³²⁹ “Veri sorumlusu bankanın ilgili kişiye ait kredi kartı ekstresinde yer alan kişisel verileri yanlış e-posta hesabına göndermesi” hakkında Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/78 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 19.08.2023), kararın ilgili kısmı aynen “*Ayrıca ilgili kişinin, veri sorumlusunun Genel Müdürlüğüne konuya ilişkin hem e-posta hem de dilekçe aracılığıyla başvuruda bulunduğu, ancak belirtilen tarihin üzerinden bir ay geçmiş olmasına rağmen kendisine yazılı bir dönüş yapılmadığını iddia ettiği, veri sorumlusunun, başvuru sahibinin, şube personelleri tarafından telefonla aranarak konu hakkında bilgilendirildiğini ifade ettiği görülmekle beraber bu noktada Kanunun “Veri sorumlusuna başvuru” başlıklı 13 üncü maddesinin üçüncü fıkrasında yer alan; “Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.” hükmünden hareketle, ilgili kişinin, veri sorumlusu Banka tarafından telefonla aranmak suretiyle bilgilendirilmesinin Kanunun ilgili hükmü kapsamında usulüne uygun bir bildirim niteliğini haiz olmadığı*” şeklindedir.

mümkünse derhal mümkün değilse en geç otuz gün içerisinde tamamlamalı, talebe ve konuya özgü cevap vermeli, yalın ve basit bir anlatım tercih etmelidir.

V-KURUL KARARLARININ YERİNE GETİRİLMESİ YÜKÜMLÜLÜĞÜ

Kişisel Verileri Koruma Kurulu’nun verdiği kararlara uyma yükümlülüğü *“Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir.”* şeklindeki KVKK m. 15/ f. 5 hükmünden doğmaktadır.

Kişisel Verileri Koruma Kurulu önüne gelen şikayetlerde farklı kararlar verebilir. Bunlardan birincisi, eğer Kişisel Verileri Koruma Kurulu şikayete konu olayda KVKK kapsamında bir hukuka aykırılık tespit etmezse herhangi bir işlem yapılmasına yer olmadığına dair karar verebilir.

İkinci ihtimalde ise önüne gelen olayda KVKK kapsamında bir hukuka aykırılık tespit edebilir. Bu durumda veri sorumlusunu talimatlandırabilir ya da hem idari para cezası uygulayıp hem de talimatlandırabilir. İşte bu durumlarda veri sorumlusunun, Kişisel Verileri Koruma Kurulu’nun vermiş olduğu kararı uygulaması gerekmektedir. Veri sorumlusu KVKK m. 15/ f. 5 gereği kararı gecikmeksizin uygulamak zorundadır. Ancak her halükarda bu süre, kararın veri sorumlusuna tebliğinden itibaren otuz günü geçmemelidir.

Kişisel Verileri Koruma Kurulu vermiş olduğu bir kararda, veri sorumlusunu daha önce ilgili kişilerin başvurularını etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırılması konusunda talimatlandırıldığını ancak buna rağmen veri sorumlusunun, ilgili kişinin KEP üzerinden yaptığı başvuruya cevap vermediğini tespit etmiş ve veri sorumlusunun KVKK m. 15/ f. 5 hükmünü ihlal ettiği gerekçesiyle KVKK m. 18/ f. 1, c bendi uyarınca veri sorumlusu hakkında idari para cezası yaptırımını uygulanmıştır.³³⁰ Yine Kişisel Verileri Koruma Kurulu’nun bir başka

³³⁰ “Bir uçak bileti satış firması olan veri sorumlusu hakkındaki şikayetle ilgili” Kişisel Verileri Koruma Kurulunun 06.02.2020 Tarihli ve 2020/86 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 19.08.2023), kararın ilgili kısmı aynen “*somut olaydaki başvurunun, ilgili kişinin veri sorumlusuna yaptığı ikinci başvuru olduğu, ilk başvuru sonrasındaki şikayet doğrultusunda Kurul tarafından alınan 01/03/2019 tarihli ve 2019/48 sayılı Kararda veri sorumlusunun, Tebliğ kapsamında ilgili kişiler tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri alması hususunda talimatlandırılmasına karar verildiği, Şikayet*

kararında veri sorumlusu olan banka, aydınlatma metninin KVKK'ye uygun hale getirilmesi konusunda talimatlandırılmış ancak buna rağmen istenen uygunluk banka tarafından sağlanmamıştır. Karara konu bu olayda da veri sorumlusu olan banka hakkında idari para cezası yaptırımını uygulanmıştır.³³¹

Ayrıca, Kişisel Verileri Koruma Kurulu'nun 16.10.2018 tarihli bir kararında da veri sorumlusu, gerçekleştireceği imha işlemine ilişkin ilgili kişiyi bilgilendirmesi yönünde talimatlandırılmasına rağmen ilgili kişiyi bilgilendirmediği için Kurul kararını yerine getirmedeğinden bahisle hakkında idari para cezası yaptırımını uygulanmıştır.³³²

dilekçesi ekinde sunulan KEP delilinden veri sorumlusunun ilgili kişinin başvurusunu, kendisine iletilmesinden yedi dakika sonra okuduğunun anlaşıldığı, Kurulun talimatına rağmen ilgili kişinin KEP adresinden yaptığı ikinci başvurusunun cevaplandırılmadığı, başvurunun cevaplandırılmamasının ise veri sorumlusunun savunmasında, yoğunluk sebebiyle gözden kaçtığı şeklinde gerekçelendirildiği, buna göre, veri sorumlusu tarafından başvuruların etkin, hukuka ve dürüstlük kuralına uygun cevaplandırılması için gerekli idari tedbirlerin alınmadığı ve Kurul tarafından verilen talimata uygun davranılmadığı değerlendirilmiş olup, Kanunun 15 inci maddesinin (5) numaralı fıkrası hükümlerine aykırı hareket eden veri sorumlusu hakkında Kanunun 18 inci maddesinin 1 inci fıkrasının (c) bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir.” şeklindedir.

³³¹ Bir Banka Tarafından Kurul Kararı ile Verilen Talimatın Gereğinin Yerine Getirilmemesi Hakkında Kişisel Verileri Koruma Kurulu'nun 08/10/2020 Tarihli ve 2020/765 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 19.08.2023), kararın ilgili kısmı aynen “Aydınlatmanın kişisel verilerin elde edilmesi sırasında ve faaliyet bazı olarak yerine getirilmesi gerektiği talimatına ilişkin olarak tevsik edici belge sunulmamakla birlikte veri sorumlusunun savunma yazısında; kişisel verilerin işleme amacını belirten tek bir aydınlatma metni ile ilgili kişilerin kişisel verilerin elde edilmesi anında bilgilendirildiği ve veri sorumlusunun müşterileri dışındaki gerçek kişiler hakkında gerçekleştirdiği veri işleme faaliyetlerinde ise özel ve ayrı aydınlatma metinleri kullanıldığı ifadelerine yer verilmekle birlikte web sayfasında farklı bankacılık ürünlerine başvuru yapılması sırasında o faaliyete özgü hazırlanmamış genel bir aydınlatma metnine yer verildiği ve bu aydınlatma metninin de Tebliğe uygun olmadığı dikkate alındığında veri sorumlusu tarafından yayımlanan aydınlatma metninin Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak düzenlenmediği ve Kurul Kararı ile verilen talimatın yerine getirilmeyerek Banka tarafından Kanunun 15'inci maddesinin (5) numaralı fıkrasına aykırı hareket edildiği kanaatine varıldığından, veri sorumlusu hakkında Kanunun 18'inci maddesinin (1) numaralı fıkrasının (c) bendi uyarınca 120.000 TL idari para cezası uygulanmasına karar verilmiştir.” şeklindedir.

³³² “Kurul Kararının gereğinin süresi içinde yerine getirilmemesi” hakkında Kişisel Verileri Koruma Kurulunun 16/10/2018 tarihli ve 2018/118 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 19.08.2023), kararın ilgili kısmı aynen “Şikâyetçinin Kurula yapmış olduğu başvurunun incelenmesi neticesinde alınan Kurul Kararı 02.07.2018 tarihinde veri sorumlusuna tebliğ edilmiştir. Bu kapsamda veri sorumlusunun, Kurul Kararı kapsamında 16.08.2018 tarihinde şikâyetçiye bilgi verdiği, bu hususun da 17.08.2018 tarihli yazı ile Kurula bildirildiği görülmekte olup, Şirket tarafından ilgili mevzuat hükümleri çerçevesinde en geç 01.08.2018 tarihinde yapılması gereken işlemin 16.08.2018 tarihinde yapıldığı; diğer yandan şikâyetçinin, veri sorumlusu nezdinde bulunan kişisel verilerinden asgari saklama süresi tamamlanmış olanlarının Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11 inci maddesinin (1) numaralı fıkrası gereğince ilk periyodik imha işleminde, kalanların da yasal saklama yükümlülüğünün dolmasını müteakiben yapılacak periyodik imha işlemi dönemlerinde silinmesine ve gerçekleştirilecek silme işlemleri hakkında Şikâyetçiye bilgi verilmesi ayrıca, söz konusu kişisel verilerin saklama amacı dışında işlenmemesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmiş olmasına rağmen Şirketin şikâyetçiye muhatap 16.08.2018 tarihli yazısında Kurul Kararının bu maddelerine ilişkin herhangi bir açıklamada bulunmadığı tespit edilmiştir. Bu çerçevede kamu kuruluşu olarak değerlendirilen veri sorumlusuna tebliğ edilen Kurul Kararının gereğinin Kanunun 15 inci maddesinin (5) numaralı fıkrasında belirtilen

Sonuç itibariyle, eğer bir veri sorumlusu, Kişisel Verileri Koruma Kurulu tarafından talimatlandırılmışsa veya bir işlemi tesis etmesi ya da etmemesi yönünde karar mevcut ise verilen kararı, talimatı mümkünse derhal mümkün değilse en geç 30 gün içerisinde uygulamakla yükümlüdür. Verilen kararın, talimatın takibatı açısından Kurul tarafından teyit amaçlı bilgi ve belge talep edilmesi mümkündür. Veri sorumlusunun talimatın ya da kararın gereğini yerine getirdiğini tesis ettiği işlemler doğrultusunda ispatlaması gerekecektir.

VI-KİŞİSEL VERİLERİN İMHA EDİLMESİ YÜKÜMLÜLÜĞÜ

Kişisel verilerin imha edilmesi yükümlülüğü KVKK m. 7’de düzenlenmiştir.³³³

Ayrıca, KVKK m. 7/ f. 3 uyarınca Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 28.10.2017 tarihinde 30224 sayılı Resmi Gazete’de yayımlanmış ve 01.01.2018 tarihi itibariyle yürürlüğe girmiştir. Belirtilen yönetmelikte kişisel verilerin imhası yükümlülüğüne ilişkin usul ve esaslara yer verilmiştir.

Çalışmamızda daha önce de bahsettiğimiz üzere³³⁴ kişisel verilerin imhası üç şekilde karşımıza çıkabilir. Bunlar kişisel verilerin silinmesi, kişisel verilerin yok edilmesi ya da kişisel verilerin anonim hale getirilmesidir. Bu yöntemlerden hangisinin tercih edileceği veri sorumlusunun inisiyatifindedir.

Kişisel verilerin imhası yükümlülüğünün temelinde her kişisel verinin bir ömrünün olması yer almaktadır. Kanun koyucu, ömrünü tamamlayan kişisel verilerin imha edilmesini beklemektedir. Peki bir kişisel veri ne zaman ömrünü tamamlamış olacaktır? KVKK m. 7/ f. 1’de geçen ilgili kısım aynen “*Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde*” şeklindedir. Öyleyse veri sorumlusunun kişisel veri işlerken dayanabileceği KVKK m. 5’te veya KVKK m. 6’da yer alan veri işleme

30 günlük yasal süre içerisinde yerine getirilmemesi ve şikayetçiye gönderilen bilgilendirme yazısında Kurul Kararında belirtilen hususlara yer verilmemiş olması nedenleriyle; Şirket hakkında Kanunun 18 inci maddesinin (3) numaralı fıkrası çerçevesinde işlem tesis edilmesine, Şikâyetçinin, Şirket nezdinde saklanmakta olan verileri ile ilgili olarak Kurul Kararı kapsamında yapılacak iş ve işlemler hakkında bilgilendirilmesi hususunda Şirkete talimat verilmesine karar verilmiştir.” şeklindedir.

³³³ KVKK m. 7/ f. 1 aynen “*Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*” şeklindedir.

³³⁴ Bkz: s. 42 vd.

şartlarından birisinin ortadan kalkması halinde artık kişisel veri ömrünü doldurmuş olacak ve veri sorumlusunun da imha yükümlülüğü burada başlayacaktır.

Kişisel verilerin imhasına ilişkin önemli bir nokta da kişisel veri saklama ve imha politikasıdır. Kişisel verilerin korunmasına ilişkin yasal düzenlemelere bakıldığında genellikle veri sorumlusunun oluşturması gereken bir dokümandan açıkça bahsedilmez. Bunun yerine içeriğinde nelerin yer alması gerektiği gibi genel düzenlemelere yer verilir.

Genel yaklaşım bu olmakla birlikte kanun koyucu bazı dokümanlara ayrı bir önem atfetmiştir. Örneğin daha önce ele aldığımız³³⁵ aydınlatma metni bu dokümanlardan biridir. Kişisel verilerin imhası sürecine ilişkin de kanun koyucunun bir diğer önem atfettiği evrak, kişisel veri saklama ve imha politikasıdır.³³⁶ Kişisel veri saklama ve imha politikası oluşturma yükümlülüğü Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 5'te düzenlenmektedir.

Bu yükümlülük, her veri sorumlusu için geçerli olmayan bir yükümlülüktür. Nitekim ilgili madde “*Kanunun 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları*” ibaresi ile başlamaktadır. Öyleyse kişisel veri saklama ve imha politikası oluşturma yükümlülüğü bulunan veri sorumluları, VERBİS kayıt yükümlülüğü bulunan veri sorumlularıdır.³³⁷ Bununla birlikte madde, sadece doküman açısından kimlerin yükümlü olduğunu düzenlemekte olup genel anlamıyla kişisel verilerin imhasına yönelik yükümlülüğü ortadan kaldırmamaktadır. Nitekim aynı maddenin üçüncü fıkrasında bu husus aynı şekilde ifade edilmiştir. Ayrıca maddenin birinci fıkrasında ilgili doküman için “*kişisel veri işleme envanterine uygun olarak*” ibaresine yer verilmiştir.

³³⁵ Bkz: s. 92 vd.

³³⁶ Kişisel veri saklama ve imha politikası tanımı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 4/ f. 1, f bendinde “*Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı ifade eder.*” şeklinde tanımlanmıştır.

³³⁷ Kimlerin VERBİS kayıt yükümlüsü olduğu çalışmamızın “VERBİS Kayıt Yükümlülüğü” başlığı altında detaylıca izah edilmiştir. Bkz: s. 105 vd.

Kişisel veri işleme envanteri, Veri Sorumluları Sicili Hakkında Yönetmelik m. 4/ f. 1, f bendinde tanımlanmıştır.³³⁸ Kişisel veri işleme envanteri, en basit anlatımla bir veri sorumlusunun işlediği kişisel verilerin, veri sorumlusunun uhdesine girdiği andan çıktığı ana kadar olan bütün hareketlerini gösteren çok detaylı bir tablodur.

Kişisel veri işleme envanterinde, Veri Sorumluları Sicili Hakkında Yönetmelik m. 4/ f. 1, f bendi uyarınca kişisel verilerin işlendikleri amaçlar için gerekli olan azami süre bilgisi yer almaktadır. Bu nedenle de kanun koyucu, kişisel veri işleme envanteri ile kişisel veri saklama ve imha politikasının bu noktada örtüşmesini beklemektedir. Hatta bu uyumluluğun içerisine VERBİS kaydını da dahil etmek gerekir. Öyleyse bir veri sorumlusunun işlediği kişisel verileri ne zaman imha edeceğine ilişkin bilgi hem kişisel veri işleme envanterinde hem kişisel veri saklama ve imha politikasında hem de VERBİS kaydında gösterilmeli ve bunların üçü birbiriyle uyumlu olmalıdır.

Hemen belirtmek gerekir ki Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 5/ f. 2 uyarınca, veri sorumlusunun bu politikayı hazırlamış olması tek başına imha yükümlülüğünü yerine getirdiğini göstermemektedir. Ayrıca, kişisel veri saklama ve imha politikasının içermesi gereken asgari unsurlar Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 6’da düzenlenmiştir.³³⁹

Kişisel verilerin imhası iki şekilde gündeme gelebilir. Veri sorumlusu re’sen imha yapıyor olabilir ya da ilgili kişinin veri sorumlusundan kişisel veri imha talebi söz konusu olabilir. Veri sorumlusu ister re’sen imha işlemi gerçekleştirsin isterse ilgili kişinin talebi üzerine imha işlemini gerçekleştirsin Kişisel Verilerin Silinmesi, Yok

³³⁸ Madde aynen “Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter” şeklindedir.

³³⁹ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 6 aynen “Kişisel veri saklama ve imha politikası asgari olarak; a) Kişisel veri saklama ve imha politikasının hazırlanma amacına, b) Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına, c) Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına, ç) Kişisel verilerin saklanması ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya, d) Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere, e) Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere, f) Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına, g) Saklama ve imha sürelerini gösteren tabloya, ğ) Periyodik imha sürelerine, h) Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe ilişkin bilgileri kapsar.” şeklindedir.

Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 7/ f. 3³⁴⁰ uyarınca muhakkak buna ilişkin işlemleri kayıt altına almalı ve bu kayıtları da en az üç yıl süreyle saklamalıdır. Kişisel verilerin re'sen imhası, belirtilen yönetmeliğin 11. maddesinde, ilgili kişinin talebi üzerine silinmesi veya yok edilmesi ise 12. maddesinde düzenlenmiştir.

Kişisel verilerin veri sorumlusu tarafından re'sen imhası durumunda ne zaman ve ne sıklıkla imha yapılacağı ikiye ayrılarak ele alınmıştır. Birinci duruma göre, KVKK m. 11/ f. 1 uyarınca eğer veri sorumlusu, kişisel veri saklama ve imha politikası oluşturmuş ise yükümlülüğünü takip eden ilk periyodik imha³⁴¹ tarihinde imha işlemini gerçekleştirmelidir.

Kanun koyucu burada “kişisel veri saklama ve imha politikası oluşturma yükümlüsü ise” ibaresi yerine “kişisel veri saklama ve imha politikası oluşturmuş ise” ibaresini tercih etmiştir. Buradan hareketle maddenin hem kişisel veri saklama ve imha politikası oluşturma yükümlülüğü altında bulunan veri sorumlularını hem de böyle bir yükümlülüğü bulunmasa bile yine de ilgili politikayı oluşturan veri sorumlularını kapsadığı kanaatindeyiz.

Maddede belirtilen durumu bir örnek ile açıklayalım. Bir veri sorumlusunun, çalışan adaylarının seçme ve yerleştirme süreçlerinde işe kabul etmediği çalışan adaylarının özgeçmişlerini, teslim aldığı tarihten 1 yıl sonra imha ettiğini varsayalım. Aynı zamanda bu şirkete 01.01.2023, 01.02.2023 ve 01.03.2023 tarihinde üç adet özgeçmiş bırakılmış olsun. Buna göre belirtilen özgeçmişlerin ömrü sırasıyla 01.01.2024, 01.02.2024 ve 01.03.2024 tarihlerinde dolacaktır. Veri sorumlusunun kendi bünyesinde bulunan ve kişisel veri ihtiva eden her evrakı günü geldiği anda imha etmesi makul olmayacağından veri sorumlusu bunu periyodik olarak gerçekleştireceği imha dönemlerinde imha edecektir. Örneğin veri sorumlusunun her yıl 10 Ocak, 10 Nisan, 10 Temmuz, 10 Ekim tarihlerini periyodik imha tarihi olarak belirlediğini varsayalım. Öyleyse bu veri sorumlusu 01.01.2024 tarihinde ömrünü dolduracak

³⁴⁰ Madde aynen “*Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.*” şeklindedir.

³⁴¹ Periyodik imha, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 4/ f. 1, 3. bendinde aynen “*Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini ifade eder.*” şeklinde tanımlanmıştır.

kişisel veri için 10 Ocak 2024 tarihinde imha işlemini gerçekleştirecektir. Ayrıca 01.02.2024 tarihinde ömrü dolan kişisel verinin ise en yakın periyodik imha tarihi olan 10 Nisan 2024'te imha edilmesi gerekecektir. Son olarak 01.03.2024 tarihinde ömrü dolacak kişisel verilerin ise yine en yakın tarih olan 10 Nisan 2024 tarihli periyodik imha döneminde imha edilmesi gerekecektir. Açıkça anlaşılacağı üzere bu örneğimizde önemli olan kişisel verinin imha edilmesi gereken tarihin ve en yakın periyodik imha tarihinin tespiti.

Belirtmek gerekir ki Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 11/ f. 2 uyarınca periyodik imhanın zaman aralığı en fazla altı ay olacak şekilde kişisel veri saklama ve imha politikasında belirlenmelidir. Uygulamada da genellikle altı aylık dönemler tercih edilmektedir.

İkinci durum ise kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusunun ne zaman re'sen imha yapması gerekeceğidir. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 11/ f. 3 uyarınca bu kategoride yer alan veri sorumlularının yükümlülüğünün ortaya çıktığı andan itibaren 3 ay içerisinde imha işlemini gerçekleştirmesi gerekecektir. Yukarıda verdiğimiz örneğin aynısını, bu kategoride yer alan veri sorumlusu açısından ele alacak olursak 01.01.2024 tarihinde ömrü dolacak olan özgeçmiş en geç 01.04.2024 tarihinde imha edilebilecektir.

Kişisel verilerin veri sorumlusu tarafından ilgili kişinin talebi üzerine imhası durumunda ne zaman ve ne sıklıkla imha yapılacağı ise Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 12/ f. 1, a bendinde düzenlenmiş olup bu maddede yukarıda izah ettiğimiz şekilde ikili bir ayrıma gidilmemiştir. Buna göre veri sorumlusu eğer talebi kabul ediyor ise ilgili kişinin talebini en geç 30 gün içerisinde yerine getirecektir. Burada öngörülen 30 günlük süre, veri sorumlusunun ilgili kişinin başvurularını cevaplandırması gereken 30 günlük süre ile uyumlu olarak düzenlenmiştir.

Hemen belirtmek gerekir ki veri sorumlusu, ilgili kişinin talebine konu kişisel verileri üçüncü kişilere aktarmış olabilir. Bu durumda Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m.12 / f. 1, b bendi uyarınca veri sorumlusu, veriyi aktardığı üçüncü kişiyi, ilgili kişinin başvurusu kabul ettiği yönünde bilgilendirmeli ve gerekli işlemlerin üçüncü kişi nezdinde de

gerçekleşmesini sağlamalıdır. Örneğin bir veri sorumlusu toplu SMS hizmeti için müşterilerinin telefon adresini üçüncü bir şirket ile paylaşmış ise ve ilgili kişi de artık reklam amaçlı SMS almak istemediğini belirtmiş ise bu talebi alan veri sorumlusu derhal durumu SMS hizmeti sunan firmaya iletmeli ve işlemin gerçekleştirildiğinin teyidini sağlamalıdır.

Kişisel verilerin imhasına ilişkin değinmek istediğimiz son konu, kişisel verilerin imha sürecinde tercih edilebilecek yöntemlerin neler olduğudur. Veri sorumlusu bir imha yöntemi olarak kişisel verilerin silinmesini tercih edebilir.³⁴² Bu yöntemi tercih eden veri sorumlusu önce silinecek veriyi tespit etmeli, veriye erişimi olan kullanıcıları belirlemeli, kullanıcıların nasıl erişim sağladığını belirlemeli ve en nihayetinde silme işlemini gerçekleştirmelidir.³⁴³

Örneğin, bulutta toplanan kişisel veriler açısından bulut sisteminde kişisel veri içeren doküman silinmesi ve aynı zamanda ilgili kullanıcının silinen dokümanı geri getirme yetkisinin de kaldırılması veya kağıt ortamında bulunan kişisel verilerin silinmesi için kişisel veri içeren kısımların sabit mürekkeple karalanması ve görünmez hale getirilmesi, silme işlemine örnek verilebilir.³⁴⁴ Silme işlemi için önemli olan kriter, kişisel verilerin ilgili kullanıcılar³⁴⁵ için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.

İlgili kullanıcı dışındaki kişi/kişiler veya birimin, silinen veriyi tekrar kullanılabilir hale getirebilme yetkisinin bulunması ya da veriye erişebilmesi, veri sorumlusunun silme işlemine hâlel getirmez. Örneğin bulutta depolanan kişisel verilerin silinmesi durumunda bir şirketin bilgi teknolojileri (IT) birimi dışındaki herkesin veriye erişiminin kesilmesi ve verinin bu kişiler açısından tekrar kullanılamaz

³⁴² Kişisel verilerin silinmesi Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 8’de düzenlenmiş olup aynen “(1)Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.” şeklindedir.

³⁴³ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, s. 7, (www.kvkk.gov.tr), (Erişim: 22.08.2023)

³⁴⁴ a.g.e., s. 8

³⁴⁵ İlgili kullanıcı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m.4/ f. 1, b bendinde “İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri ifade eder” şeklinde tanımlanmıştır.

olması durumunda veri sorumlusunun silme işlemini usulüne uygun olarak yerine getirdiğinin kabulü gerekir.

Bir diğer imha yöntemi ise kişisel verilerin yok edilmesidir.³⁴⁶ Kişisel verilerin yok edilmesi yönteminde, silmeden farklı olarak kişisel veriye kimse erişememeli, geri getirmek istese dahi geri getirememeli ve tekrar kullanamamalıdır. Adından da anlaşılacağı üzere kişisel veri gerçek manada yok olmalıdır. Örneğin kişisel veri içeren manyetik bir medyanın de-manyetize edilmesi, CD-DVD gibi araçların kırıldıktan sonra yakılması, fiziki kağıtların kağıt öğütücünden geçirilerek çok küçük parçalara ayrılması bu kapsamda ele alınabilir.³⁴⁷ Hemen belirtmek gerekir ki Kişisel Verileri Koruma Kurumu, arızalanan ya da bakıma gönderilen ve aynı zamanda kişisel veri içeren cihazlar için veri sorumlusunun ekstra önlemler alması gerektiğini belirtmiştir.³⁴⁸

Son ele alacağımız imha yöntemi ise kişisel verilerin anonim hale getirilmesidir. Kişisel verilerin anonim hale getirilmesi Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 10'da düzenlenmiştir.³⁴⁹

Anonim bir veriden bahsedebilmek için verinin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle

³⁴⁶ Kişisel verilerin yok edilmesi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 9'da düzenlenmiş olup aynen “*Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*” şeklindedir.

³⁴⁷ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, s. 12-13, (www.kvkk.gov.tr), (Erişim: 22.08.2023)

³⁴⁸ Kurum tarafından yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'nde, alınması gereken ek önlemler “*Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir: i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a) 'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi, ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi, iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması, gerekir.*” şeklinde ifade edilmiştir.

³⁴⁹ Madde aynen “*(1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. (2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. (3) Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.*” şeklindedir.

ilişkilendirilemeyecek nitelikte olması gerekir. Ayrıca belirtmek gerekir ki Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 10/ f. 2 uyarınca verinin sadece veri sorumlusu nezdinde kimliği belirli veya belirlenebilir bir kişiye ulaşma imkanını ortadan kaldırması yeterli olmaz aynı zamanda kişisel verilerin aktarıldığı alıcı gruplarının da -kişisel veriyi başka verilerle eşleştirme, geri döndürme gibi herhangi bir teknik kullanmak suretiyle dahi- kimliği belirli ya da belirlenebilir bir kişiye ulaşamaması gerekir.

Kişisel verilerin imhası sürecinde kişisel verilerin anonim hale getirilmesini tercih eden veri sorumlusunun genellikle kişisel veri içeren dokümana ihtiyacı bulunmaktadır. Örneğin bir e-ticaret şirketinin pazarlama faaliyetlerini etkin yürütebilmek için her yaş grubundan çok sayıda kişi ile anket yaptığını ve anket sonuçlarının bu şirket tarafından analiz edileceğini varsayalım. Bu veri sorumlusu açısından önemli olan ilgili kişinin kimlik bilgilerinden ziyade tercihleri olduğu için veri sorumlusu bu dokümanı imha etmek istediğinde anonim hale getirme yöntemini seçebilir.

Kişisel Verileri Koruma Kurulu, 10.09.2020 tarihli bir kararında³⁵⁰ veri sorumlusunun, ilgili kişinin telefon numarasını kara listeye alması durumunda ilgili kişisel verinin silindiğinden bahsedilemeyeceği kanaatine varmıştır. Kararda, verinin hala sistemde kayıtlı bir şekilde bulunduğundan bahisle veri sorumlusunun imha yükümlülüğünü yerine getirmediği tespit edilmiştir.

Kurul 22.06.2021 tarihli bir kararında ise veri sorumlusu tarafından, ilgili kişinin cari kart bilgilerinin pasif hale getirilmesini, bu bilgilerin saha personeli tarafından görüntülenemez hale getirilmesini ve saha personeline pasif durumu değiştirme yetkisinin verilmemesini bir bütün olarak ele almış ve bahsedilen yaklaşımı geçerli bir imha olarak ele kabul etmiştir.³⁵¹

³⁵⁰ “İlgili kişinin cep telefonu numarasının, açık rızası olmaksızın bir dernek tarafından reklam içerikli SMS gönderimi için işlenmesi hakkında” Kişisel Verileri Koruma Kurulunun 10/09/2020 tarihli ve 2020/691 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 22.08.2023), kararın ilgili kısmı aynen “Şikayete konu olay bakımından, bahse konu telefon numarasının kara listeye alınmasının hukuka aykırı olarak işlenen kişisel verinin silindiği anlamına gelmediği, hiçbir hukuki sebebe dayanmaksızın işlenen kişisel verinin halihazırda derneğin sistemlerinde kara listeye alınmış bir şekilde bekliyor oluşunun hukuka aykırı durumun devam ettiğini gösterdiği, söz konusu hukuka aykırılığın devam etmemesi adına bahse konu telefon numarasının imha edilmesi gerektiği” şeklindedir.

³⁵¹ “İlgili kişinin internet alışveriş sayfası üzerinden ev adresine teslim talepli olarak vermiş olduğu siparişlerinin veri sorumlusu kargo şirketi tarafından, hiçbir suretle belirtmediği halde işyeri adresine gönderilmesi” hakkında Kişisel Verileri Koruma Kurulunun 22/06/2021 tarihli ve 2021/603 sayılı Karar

Kurul'un, 06.07.2021 tarihli kararına konu olayda ise veri sorumlusu olan banka, ilgili kişiden aldığı imha talebi kapsamında ilgili kişinin kişisel verilerini ilk periyodik imha tarihinde imha edeceğini ilgili kişiye bildirmiştir. Kurul ise konunun re'sen imha yerine talep üzerine imha uyarınca ele alınması gerektiğinin altını çizmiş ve 30 gün geçmiş olmasına rağmen imhanın yapılmaması sebebiyle arada geçen süre için hiçbir veri işleme şartına dayanılmadığından veri sorumlusu hakkında idari para cezası yaptırımını uygulamıştır.³⁵²

Netice itibariyle -zorunlu olmasa bile- kanaatimizce her şirket, kişisel veri saklama ve imha politikası oluşturmalıdır. Bu politika, eğer mevcut ise VERBİS kaydı ve kişisel veri işleme envanteri ile uyumlu olmalıdır. Periyodik imha tarihleri belirlenmiş ise periyodik imha sürelerine dikkat edilmelidir. İlgili kişilerin başvuruları 30 gün içerisinde neticelendirilmelidir. Sürece ilişkin ilgili kişi bilgilendirilmelidir. İmha için veri sorumlusu tarafından en uygun yöntem tercih edilmeli ve usulüne uygun bir imha işlemi gerçekleştirilmelidir.

Özeti, (www.kvkk.gov.tr), (Erişim: 22.08.2023), kararın ilgili kısmı aynen “İlgili kişinin verilerinin silinmesine yönelik talebi ile ilgili olarak, veri sorumlusu tarafından, gönderim esnasında taşıma işini gerçekleştirmek üzere beyan edilmiş olan adresi, adı, soyadı ve irtibat telefon numarasının mevcut kayıtlarından yasal zorunluluk gereği silinmediği, kişisel verilerin korunması ve güvenliğinin azami ölçüde sağlandığı ve işlenen kişisel verilerin taraflar arası hukuki ilişkinin niteliği gözetilerek ve ilgili kanunlarda öngörülen yasal zorunluluk ve zaman aşımı süreleri ve diğer hukuki yükümlülükler dikkate alınarak gereken süre boyunca saklandığı ve akabinde silme, yok etme veya anonim hale getirme yöntemleri gözetilerek imha edildiği, bu çerçevede ilgili kişinin kişisel verilerinin bulunduğu (isim soy isim, adres, iletişim no vb.) veri tabanında kayıtlı bütün cari hesapların pasif hale getirildiği, pasif hale getirilen hesapların sistem kaydı ekran görüntüsünün savunma yazısı ekinde gönderildiği ve pasif hale getirilen cari bilgilerin saha personeli tarafından görüntülenemez, kullanılamaz ve pasif durumu değiştirilemez olduğu” şeklindedir.

³⁵² “İlgili kişinin veri sorumlusu bankaya yaptığı iş başvurusunun olumsuz sonuçlanması sonrası kişisel verilerinin işlenmeye devam etmesi” hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 tarih ve 2021/670 sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 22.08.2023), kararın ilgili kısmı aynen “İş başvurusunun kabul edilmemesi ile birlikte Kanunun 5 inci maddesinde yer alan veri işleme şartlarından herhangi birinin devam etmediği göz önünde bulundurulduğunda her ne kadar veri sorumlusu tarafından Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğinin 11 inci maddesi gereği ilk periyodik imha sürecinde imha talebinin yerine getireceği bilgisi ilgili kişiye verilmiş olsa da verilerin imha talebinin ilgili kişi tarafından Kanunun 7 ve 11 inci maddesi kapsamında veri sorumlusuna yeniden iletildiği, söz konusu imha talebi göz önüne alındığında mezkur Yönetmeliğin 11 inci maddesi kapsamında veri sorumlusu tarafından hazırlanan imha politikasına dayanarak gerçekleştirilecek “resen” imha işleminin söz konusu olamayacağı, aksine aynı Yönetmeliğin 12 inci maddesi kapsamında ilgili kişinin talebi üzerinde imha işleminin gerçekleştirilmesinin gerektiği; bu itibarla da imha işleminin bu madde kapsamında ele alınması gerektiği” şeklindedir.

VII- AYDINLATMA YÜKÜMLÜLÜĞÜNÜN TTK M. 1524 BAĞLAMINDA DEĞERLENDİRİLMESİ

Çalışmamızın bu bölümüne kadar, Türk ticaret şirketlerinin KVKK kapsamındaki yükümlülüklerinin neler olduğunu ve yükümlülüklerin nasıl yerine getirileceğini izah etmeye çalıştık. Bununla birlikte, çalışmamızın öznesini teşkil eden Türk ticaret şirketlerinin uymakla mükellef olduğu kanunlardan birisi de şüphesiz 6102 sayılı Türk Ticaret Kanunu'dur.³⁵³

TTK kapsamında bazı maddeler, KVKK kapsamındaki yükümlülüklerin yerine getirilmesi aşamasında Türk ticaret şirketlerine yol gösterici niteliktedir. Bu nedenle çalışmamızın bu bölümünde TTK-KVKK kesişimine konu olabilecek bazı maddeleri inceleyeceğiz.

İlk ele alacağımız konu, internet sitesine ilişkin yükümlülüklerin düzenlendiği TTK m. 1524'tür.³⁵⁴ TTK m. 1524/ f. 1 uyarınca denetime tabi olan sermaye şirketleri, ticaret siciline tescil tarihinden itibaren üç ay içerisinde bir web sitesi açmak ve sitenin bir bölümünü de kanunen yapılacak duyurulara ayırmak zorundadır.

Maddede belirtilen “kanun” ibaresi sadece TTK'yı değil genel anlamda kanunları ifade etmektedir. Nitekim madde gerekçesinde³⁵⁵ ilgili maddenin genel bir hüküm olduğu, amacın en üst düzeyde şeffaflığı sağlamak olduğu, madde kapsamında

³⁵³ RG., 27846 S., 14.02.2011 T.

³⁵⁴ Madde aynen “(1) 397 nci maddenin dördüncü fıkrası uyarınca denetime tabi olan sermaye şirketleri, kuruluşlarının ticaret siciline tescili tarihinden itibaren üç ay içinde bir internet sitesi açmak ve bu sitenin belirli bir bölümünü şirketçe kanunen yapılması gereken ilanların yayımlanmasına özgülemek zorundadır. İnternet sitesinde yayımlanacak içerikler, bu Kanunda belli bir süre belirtilmiş ise bu süre içinde, belirtilmemiş ise içeriğin dayandığı işlemin veya olgunun gerçekleştiği tarihten, tescil veya ilana bağlandığı durumlarda ise tescil veya ilanın yapıldığı tarihten itibaren en geç beş gün içinde, şirketin kuruluşundan internet sitesi açılıncaya kadar geçen sürede yayımlanması gereken içerikler de bu sitenin açıldığı tarihte siteye konulur. (2) Birinci fıkra öngörülen yükümlülükler uyulmaması, ilgili kararların iptal edilmesinin sebebinin oluşturur, Kanuna aykırılığın tüm sonuçlarının doğmasına yol açar ve kusuru bulunan yöneticiler ile yönetim kurulu üyelerinin sorumluluğuna neden olur. Cezai hükümler saklıdır. (3) İnternet sitesinin bilgi toplumu hizmetlerine ayrılmış bölümü herkesin erişimine açıktır. Erişim hakkının kullanılması, ilgili olmak veya menfaati bulunmak gibi kayıtlarla sınırlandırılmayacağı gibi herhangi bir şarta da bağlanamaz. Bu ilkenin ihlali hâlinde herkes engelin kaldırılması davasını açabilir. (4) İnternet sitesinin bu maddenin amaçlarına özgülenmiş kısmında yayımlanan içeriğin başına tarih ve parantez içinde “yönlendirilmiş mesaj” ibaresi konulur. Bu ibare ancak bu Kanuna ve bu fıkra anılan yönetmeliğe uyulmak suretiyle değiştirilebilir. Özgülenen kısımda yer alan bir mesajın, yönlendirildiği karinedir. Sitenin, bir numara altında tescili ve ilgili diğer hususlar Gümrük ve Ticaret Bakanlığı tarafından bir yönetmelikle düzenlenir. (5) Bu Kanun ve ilgili diğer kanunlarda veya idari düzenlemelerde daha uzun bir süre öngörülmedikçe, şirketin internet sitesine konulan bir içerik, üzerinde bulunan tarihten itibaren en az altı ay süreyle internet sitesinde kalır; aksi hâlde konulmamış sayılır. (6) İnternet sitesiyle ilgili olarak bu Kanunun ilgili maddelerinde ve bu maddede öngörülen düzenlemeler denetime tabi olmayan sermaye şirketleri hakkında uygulanmaz.” şeklindedir.

³⁵⁵ Türk Ticaret Kanunu Madde Gerekçesi, (<https://www.lexpera.com.tr/mevzuat/gerekceler/turk-ticaret-kanunu-madde-gerekceleri/1>), (Erişim: 21.08.2023)

akla ilk gelenin bilgi, belge ve raporlar olmakla birlikte bunların sınırlı sayıda olmadığı, web sitesine bilgi toplumu bağlamında her şeyin konulabileceği, web sitesine konulması gereken bir içeriğin konulmaması halinde yönetim kurulunun görevini yerine getirmemesinin tüm sonuçlarının doğacağı belirtilmiştir.³⁵⁶

Madde gerekçesinde yer alan şeffaflık vurgusu son derece önemlidir. Zira her ne kadar KVKK'de "şeffaflık" ya da "hesap verilebilirlik" ismiyle bir ilke açıkça yer almasa da Kişisel Verileri Koruma Kurumu bu ilkelere ayrı bir önem atfetmektedir.³⁵⁷ Nitekim Kurul bir kararında hesap verilebilirlik ilkesine atıfta bulunmuştur.³⁵⁸

Netice itibarıyla hem TTK m. 1524 / f. 1 hem de Kişisel Verileri Koruma Kurumu'nun genel yaklaşımı uyarınca şirketlerden bir şeffaflık beklenmektedir. TTK m. 1524 / f. 1 uyarınca şeffaflığın sağlanması adına her türlü evraka web sitesinde yer verilebilir. Bu evrakları KVKK kapsamındakilere indirgeyecek olursak çerez aydınlatma metni, ziyaretçi aydınlatma metni gibi evraklar örnek verilebilir. Elbette evrak türü açısından bir sınırlama olmamakla birlikte TTK m. 1524 kapsamında web sitesinde yayınlanacak evraklar daha çok ilgili kişiyi aydınlatmaya yönelik metinlerden oluşacaktır. Bu nedenle TTK m. 1524 hükmü,

³⁵⁶ Madde gerekçesinin ilgili kısmı aynen "Bu maddede, "Elektronik işlemler ve bilgi toplumu hizmetleri" başlığı altında elektronik işlemler ve bilgi toplumu hizmetlerine ilişkin hükümler toplu olarak yer almaktadır. Bu genel hüküm dışında 1524 üncü madde bir genel hükümdür. Tasarının çeşitli hükümlerinde web sitesine konulacak içeriğe ilişkin düzenlemelere yer verilmiştir. Web sitesi ile ilgili düzenleme, gelişmelere açıktır. Pek de uzak olmayan bir gelecekte yapılacak değişikliklerle söz konusu başlık altında yer alan düzenlemelerin genişleyebileceği düşünülmüştür. Çünkü alan çok dinamik ve bu konudaki uluslararası çalışmalar çok yoğundur. Birinci fıkra: Hüküm, en üst düzeyde şeffaflığın sağlanması amacıyla öngörülmüştür. Web sitesinin, şirketle ilgili bilgilere, şirketin yaptığı açıklamalara, çağrılara, beyanlara ve hazırladığı belgelere, raporlara, finansal tablolara, sorulan sorulara verilen cevaplara, herkesin en kolay şekilde ulaşabildiği, en güvenilir şeffaflığı en üst düzeyde sağlayan araç olduğu düşüncesinden hareket edilmiştir. Hükümün internet tekniğine uydurulması bazı güçlüklerle sebep olabilir. Hükümün öngördüğü web sitesi düzeni şöyle açıklanabilir: (a) Her sermaye şirketi bir web sitesi alacaktır. (b) Web sitesine bilgi toplumu bağlamında "herşey" konulabilir. "Herşey" şeffaflık ile tanımlanır ve anlam kazanır. Hükümde ilk akla gelen bilgiler, belgeler, raporlar, tablolar, çağrılar vs. (kısaca: "İçerik") yer almıştır. Bunlar sınırlı sayı (numerus clausus) değildir. İçeriğin web sitesine konulması için web sitesinin bir bölümü 1524 üncü maddenin amaç ve işlevlerine özgülenmelidir. Özgüleme olgusu "özülemenin yapılmış olduğu" ikinci fıkra da belirtildiği üzere web sitesinin tescili değildir. Sicile kaydın kurucu niteliği bulunmayıp, özgüleme açıklayıcıdır; kamuya özgülemenin bildirilmesidir. İstenen özgülemenin sicile kaydedilmesi, sicilde özel bir numara verilmesidir. Bu sicil numarası değildir. Ancak, kanun bunu bir hükme bağlamamıştır, idarî düzenlemelere bırakmıştır. Böylece web sitesi içinde bir bölüm ayrılması gerçekleşmiş, ilân edilmiş ve resmîleşmiş olacaktır. Web sitesine konulması gereken bir içerik konulmamışsa, hukuka aykırılığın ve yönetim kurulunun görevini yerine getirmemesinin tüm sonuçları doğar. Meselâ: genel kurulun kararı iptal edilir, yönetim kurulu sorumlu tutulur, gereğinde işlem geçerlik kazanmayabilir." şeklindedir.

³⁵⁷ KAYA, a.g.e., s. 1889

³⁵⁸ "Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru" Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, (www.kvkk.gov.tr), (Erişim: 21.08.2023)

madde kapsamına giren bir Türk ticaret şirketinin aydınlatma yükümlülüğünü nasıl yerine getireceği noktasında bir yol göstericidir.

TTK m. 1524/ f. 2 aynen “*Birinci fıkra da öngörülen yükümlülükler e uyulmaması, ilgili kararların iptal edilmesinin sebebini oluşturur, Kanuna aykırılığın tüm sonuçlarının doğmasına yol açar ve kusuru bulunan yöneticiler ile yönetim kurulu üyelerinin sorumluluğuna neden olur. Cezai hükümler saklıdır.*” şeklindedir. İlk izlenimde maddede yalnızca TTK kapsamındaki bir sorumluluğun incelendiği düşünülebilir. Öte yandan madde gerekçesinde “*Web sitesine konulması gereken bir içerik konulmamışsa, hukuka aykırılığın ve yönetim kurulunun görevini yerine getirmemesinin tüm sonuçları doğar.*” açıklaması yer almaktadır.

Web sitesine konulması gereken içerik TTK kapsamındaki bir içerik olabileceği gibi KVKK kapsamındaki bir içerik de olabilir. Kanaatimizce, hem TTK m. 1524 hem de madde gerekçesi bir bütün olarak değerlendirildiğinde eğer veri sorumlusu

TTK m. 1524 kapsamında değerlendirilen şirketlerdense ve web sitesinde çerez aydınlatma metni, ziyaretçi aydınlatma metni, e-bülten aydınlatma gibi web sitesinde yayınlanması gereken evraklara³⁵⁹ yer vermemişse, yönetim kurulu üyelerinin sorumluluğu söz konusu olabilecektir.

VIII- KİŞİSEL VERİLERİN İŞLENMESİ VE İMHASI SÜREÇLERİNİN TTK M. 64 VE TTK M. 82 BAĞLAMINDA DEĞERLENDİRİLMESİ

Defter tutma ve envanter üst başlığını taşıyan TTK m. 64 hükmü, her tacir için uygulama alanı bulan ve tutulması gereken kayıtlara ilişkin detayların düzenlendiği bir maddedir. Saklama ve ibraz üst başlığını taşıyan TTK m. 82 hükmü ise saklamakla yükümlü olunan belgelerin ne kadar süre ile saklanması gerektiğini ve sürenin hesaplanma şeklini düzenlemektedir.

Belirtilen maddeler, Türk ticaret şirketleri açısından kişisel verilerin korunması kapsamında önemli maddelerdir. Zira maddede sayılan belgeler içerisinde şüphesiz ki

³⁵⁹ Veri sorumlusunun faaliyet gösterdiği sektör ve işlemek istediği kişisel veriler uyarınca web sitesinde yayınlaması gereken belge sayısı farklılık arz edebilir. Bu belgeler sınırlı sayıda değildir. Öte yandan, bir web sitesi sadece bilgilendirme amaçlı olsa dahi en azından zorunlu çerezler kullanıldığından ve ziyaretçilerin IP adresi işlenebileceğinden çerez aydınlatma metni ve ziyaretçi aydınlatma metni bulunmalıdır.

birçok kişisel veri yer almaktadır. Dolayısıyla, TTK m. 64 ve TTK m. 82 hükmü bir bütün olarak değerlendirildiğinde, bir Türk ticaret şirketinin hangi belgeyi ne kadar süre ile ve ne surette saklaması gerektiğinin cevabı ortaya çıkmaktadır. Bunun doğal bir sonucu olarak, bu kapsamda yer alan belgelerdeki kişisel verilerin ne kadar süre ile ve ne surette saklaması gerektiğinin cevabı da ortaya çıkmaktadır.

Bu noktada özellikle, “İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme” ilkesi gündeme gelmektedir. Daha önce de izah edildiği³⁶⁰ üzere anılan ilke uyarınca veri sorumlusu öncelikle bir kişisel veriyi işlemesi için mevzuatta bir süre öngörülüp öngörülmediğini araştırmalı, şayet bir süre var ise kişisel veriyi o süre kadar işlemelidir. Öte yandan, bir süre öngörülmemiş ise veri sorumlusu, kişisel veriyi işleyeceği süreci, amacı ve kişisel veriye olan ihtiyacının ne kadar sürede ortadan kalkacağını belirlemeli ve makul bir süre tayin etmelidir.

TTK m. 82/ f. 5 hükmü aynen “*Birinci fıkranın (a) ilâ (d) bentlerinde öngörülen belgeler on yıl saklanır.*” şeklindedir. Atıfta bulunulan a bendinde bahsi geçen belgeler aynen “*Ticari defterlerini, envanterleri, açılış bilançolarını, ara bilançolarını, finansal tablolarını, yıllık faaliyet raporlarını, topluluk finansal tablolarını ve yıllık faaliyet raporlarını ve bu belgelerin anlaşılabilirliğini kolaylaştıracak çalışma talimatları ile diğer organizasyon belgelerini*” şeklinde ve d bendinde bahsi geçen belgeler de aynen “*64 üncü maddenin birinci fıkrasına göre yapılan kayıtların dayandığı belgeleri*” şeklinde sayılmıştır. Açıkça görüleceği üzere bu belgelerin saklanma süresi kanunda 10 yıl olarak düzenlenmiştir.

Buna göre bir Türk ticaret şirketi, hem TTK m. 64 ve m. 82 kapsamındaki yükümlülüğünü ifa edebilmek hem de KVKK’de yer alan “İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme” ilkesine uygun bir veri işleme faaliyetinde bulunmak için maddede anılan evrakları 10 yıl süre ile saklamalıdır. 10 yıllık sürenin hesabında ise “*Saklama süresi, ticari defterlere son kaydın yapıldığı, envanterin çıkarıldığı, ara bilançonun düzenlendiği, yılsonu finansal tablolarının hazırlandığı ve konsolide finansal tabloların hazırlandığı, ticari yazışmaların yapıldığı veya muhasebe belgelerinin olduğu takvim yılının bitişiyle başlar.*” şeklindeki TTK m. 82/ f. 6 hükmü göz önünde bulundurulmalıdır.

³⁶⁰ Bkz: s. 56

IX- VERİ İHLALİ BİLDİRİM YÜKÜMLÜLÜĞÜNÜN TTK M. 82/ F. 7 BAĞLAMINDA DEĞERLENDİRİLMESİ

Defter ve belgelerin zıyânı düzenleyen TTK m. 82/ f. 7 hükmü aynen “*Bir tacirin saklamakla yükümlü olduğu defterler ve belgeler; yangın, su baskını veya yer sarsıntısı gibi bir afet veya hırsızlık sebebiyle ve kanuni saklama süresi içinde ziyaa uğrarsa tacir zıyâı öğrendiği tarihten itibaren otuz gün içinde ticari işletmesinin bulunduğu yer yetkili mahkemesinden kendisine bir belge verilmesini isteyebilir. Bu dava hasımsız açılır. Mahkeme gerekli gördüğü delillerin toplanmasını da emredebilir.*” şeklindedir. Öte yandan, veri ihlal bildiriminde bulunma yükümlülüğünü düzenleyen KVKK m. 12/ f. 5 hükmü aynen “*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.*” şeklindedir.

Daha önce açıklandığı üzere³⁶¹ bir veri sorumlusu, kişisel verilerin güvenliğine yönelik her türlü teknik ve idari tedbiri almakla yükümlüdür. Kanun dışı yollarla kişisel verilerin başkaları tarafından ele geçirilmesi durumunda ise veri sorumlusu kendisini, Kişisel Verileri Koruma Kurumu’na ihbar etmekle yükümlüdür. Veri ihlal bildirim yükümlülüğü olarak adlandırılan bu yükümlülük uyarınca kanun koyucu, veri sorumlusunun kendisini ihbar etmesini bir yükümlülük olarak getirmiştir.

Her iki maddenin kesişim noktası ise TTK m. 82/ f. 7 hükmünde geçen “hırsızlık” unsurudur. Takdir olunacağı üzere hırsızlık, KVKK m. 12/ f. 5’te geçen “*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi*” unsurunun görünüm biçimlerinden birisidir. TTK m. 82/ f. 7 kapsamında hırsızlığa konu olan bir evrak, tacirin saklamakla yükümlü olduğu defter veya belgelerden birisi olabilir. Bu belgelerde ilgili kişiye ait birtakım kişisel verilerin de bulunma ihtimali mevcuttur. Dolayısıyla ihtimaller içerisinde kişisel veri içeren birtakım evrakın çalınması durumu bulunmaktadır.

Daha önce de açıkladığımız üzere³⁶² veri ihlal bildiriminde bulunulması için veri sorumlusuna tanınan süre 72 saattir. TTK m. 82/ f. 7 kapsamında dava açmak

³⁶¹ Bkz: s. 111 vd.

³⁶² Bkz: s. 129-130

isteyen bir Türk ticaret şirketine tanınan süre ise 30 gündür. Böyle bir hırsızlık durumuyla karşılaşan veri sorumlusunun yapması gereken, 72 saat içerisinde veri ihlal bildiriminde bulunmak ve dilerse TTK m. 82/ f. 7 hükmünce kendisine tanınan dava hakkını kullanmaktır. Öte yandan, farklı ihtimaller de söz konusu olabilir. Örneğin bir Türk ticaret şirketi, kişisel veri ihtivan eden bir belgenin hırsızlığa konu olması sebebiyle TTK m. 82/ f. 7 kapsamında bir dava açmış ancak veri ihlal bildiriminde bulunmamış olabilir. Bu durumda, ilgili Türk ticaret şirketi hakkında, Kişisel Verileri Koruma Kurumu'na 72 saatlik süre içerisinde veri ihlal bildiriminde bulunmaması gerekçesiyle idari para cezası yaptırımını uygulanabilir.

Netice itibariyle, eğer bir Türk ticaret şirketi, hırsızlık gerekçesiyle TTK m. 82/ f. 7 kapsamında bir dava açmış ise ve davaya konu evrak da kişisel veri ihtiva eden bir evrak ise muhakkak 72 saatlik süre içerisinde veri ihlal bildiriminde bulunmalıdır. Aksi takdirde, dava dilekçesinde olayın gerçekleşme şekli, günü, saati ve hırsızlık konusu evrak bilgileri doğrudan davacının kendisi tarafından Mahkemenin bilgisine sunulmuş olacaktır. Bu bilgiler neticesinde, ilgili Türk ticaret şirketinin 72 saatlik süre içerisinde veri ihlal bildiriminde bulunup bulunmadığı rahatlıkla tespit olunabilecek ve idari yaptırım uygulanabilecektir.

X- KVK KAPSAMINDAKİ YÜKÜMLÜLÜKLERİNİ YERİNE GETİRMEYEN TÜRK TİCARET ŞİRKETİNİN EYLEMLERİNİN TTK M. 55/ F. 1/ E BENDİ UYARINCA HAKSIZ REKABET BAĞLAMINDA İNCELENMESİ

Rekabet, piyasadaki rakiplerin müşteriyi kendi mal ve/veya hizmetlerine çekme yarışıdır.³⁶³ Piyasalarda rekabet ortamının adil bir şekilde tesisi, tüketicinin kaliteli ve uygun fiyatlı ürün ve hizmetlere erişiminin sağlanması, tüketicinin takdir yetkisine sahip olacağı bir ortamın oluşturulması oldukça önemlidir. Kişisel verilerin korunması hukukunun temelinde de en basit anlatımla özel hayatın gizliliği yer almaktadır.

Haksız rekabet hukuku ve kişisel verilerin korunması hukukunun kesişim noktalarından birisi de kişisel verilerdir. Kişisel veriler, ekonomik bir değere sahip olduğundan hukuka aykırı kullanılması halinde haksız rekabet teşkil edebilecek

³⁶³ Deniz AÇIKGÖZ, **Çalışanın Haksız Rekabet Eylemleri ve Tazminat Sorumluluğu** – Ticaret Hukuku Monografileri, Ankara: Seçkin Yayıncılık, 2023, s. 21.

eylemlerin ve sonuçların ortaya çıkabilmesi mümkündür. İlaveten, KVKK kapsamında öngörülen yükümlülüklerin yerine getirilmesi şüphesiz ki belirli bir bütçeyi gerektirmektedir. Bu doğrultuda, KVKK kapsamında hiçbir yükümlülüğünü yerine getirmeyen bir ticaret şirketi, piyasadaki rakiplerine oranla belirli bir bütçe fazlasıyla yarışa başlamaktadır. Bu nedenle çalışmamızın bu bölümünde, KVKK kapsamında hiçbir yükümlülüğünü yerine getirmeyen bir şirketin bu davranışının haksız rekabet teşkil edip etmeyeceğini inceleyeceğiz.

Haksız rekabete ilişkin hükümler, TTK m. 54 ve devamında düzenlenmiştir. TTK m. 54/ f. 1 aynen “*Haksız rekabete ilişkin bu Kısım hükümlerinin amacı, bütün katılanların menfaatine, dürüst ve bozulmamış rekabetin sağlanmasıdır.*” şeklinde olup aynı maddenin 2. fıkrası da “*Rakipler arasında veya tedarik edenlerle müşteriler arasındaki ilişkileri etkileyen aldatıcı veya dürüstlük kuralına diğer şekillerdeki aykırı davranışlar ile ticari uygulamalar haksız ve hukuka aykırıdır.*” şeklindedir. O halde haksız rekabetten söz edebilmek için haksız rekabette bulunan kişinin kusuru, bu rekabetten yarar sağlaması ya da karşı tarafın zarara uğraması gerekmemektedir.³⁶⁴ Açıkça anlaşılabacağı üzere haksız rekabete ilişkin hükümlerin temel noktalarından birisi de dürüstlük kuralıdır.³⁶⁵ Hatırlatmakta fayda var ki dürüstlük kuralı, kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerden de birisidir.

Dürüstlük kuralına aykırı olan ticari davranışların neler olabileceği TTK m. 55’te sayılmıştır. Madde içerisinde birçok ticari davranış örneğine yer verilmeyle birlikte bazı örnekler kişisel verilerin korunması-haksız rekabet ilişkisinde ön plana çıkmaktadır. TTK m. 55/ f. 1/ e bendi de bunlardan birisidir.

Öncelikle ele acağımız husus, bir Türk ticaret şirketinin KVKK kapsamında kendisine yüklenen yükümlülüklerden hiçbirini yerine getirmemesinin haksız rekabet teşkil etme ihtimalinin olup olmadığıdır. Türk ticaret şirketlerinin KVKK kapsamında yerine getirmesi gereken yükümlülükler arasında aydınlatma yükümlülüğü, VERBİS kayıt yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından

³⁶⁴ AÇIKGÖZ, a.g.e., s. 21.; Füsün NOMER ERTAN, **Haksız Rekabet Hukuku**, İstanbul: Oniki Levha Yayıncılık, 2016, s. 99.

³⁶⁵ Nitekim TTK m. 55’in gerekçesinin üçüncü paragrafında dürüstlük kuralının önemine “Dürüst davranma kuralı ise artık haksız rekabetin tanınmasında (teşhisinde) belirleyicidir. Hukuka uygun ve bozulmamış rekabet ortamında (ortamın her zaman piyasa olması şart değildir) tüm katılanlar piyasanın tüm aktörlerinin dürüst davranış kurallarına göre hareket edeceğine güvenir ve güvenmek hakkını haizdir. Dürüstlük kuralını ihlâl eden bu güvene aykırı hareket edilmiş olur. Bu da haksız rekabet oluşturur.” yer verilmiştir. (<https://www.lexpera.com.tr/mevzuat/gerekceler/turk-ticaret-kanunu-madde-gerekceleri/1>) (Erişim Tarihi: 03.10.2023)

yapılan başvuruların cevaplanması yükümlülüğü, kurul kararlarının yerine getirilmesi yükümlülüğü, kişisel verilerin imha edilmesi yükümlülüğü gibi yükümlülükleri bulunmaktadır.

Türk ticaret şirketleri tarafından KVKK kapsamındaki yükümlülüklerin yerine getirilmesi amacıyla hem dijital ortamda hem de fiziksel ortamda birçok evrak hazırlanmakta, kanuna uyumluluk kapsamında gerekli güncellemeler yapılmaktadır. Hazırlanan evraklar kapsamında bazen ilgili kişiden imza atılması istenmekte, bazı durumlarda ise bir kutucuğa tıklayarak onay vermesi beklenmektedir. Her iki ihtimalde de Türk ticaret şirketi, ilgili kişinin önüne okunması ve neticelendirilmesi gereken bir metin sunmaktadır. İşte tam da bu noktada ilgili kişinin davranışsal eğilimlerinin haksız rekabet kapsamında incelenmesi gerekmektedir.

Yapılan bir araştırmada,³⁶⁶ 5.124 katılımcıya, gizlilik politikalarını okuma durumları sorulmuştur. Katılımcıların %26'sı gizlilik politikalarını hiçbir zaman okumadığını, %27'si nadiren okuduğunu, %23'ü bazen okuduğunu belirtmiştir. Dolayısıyla araştırmaya göre okuyucuların genel eğiliminin bu tarz evrakları okumamak yönünde olduğunu söylemek yanlış olmaz.

Türkiye özelinde konuyu ele alacak olursak, kişisel verilerin korunmasına yönelik düzenlemeler daha öncesinde de bulunmakla birlikte yukarıda açıkladığımız yükümlülükler veri sorumlusuna 2016 yılında KVKK ile birlikte yüklenmiştir. Dolayısıyla çerez politikaları, aydınlatma metinleri, gizlilik politikaları gibi metinlerin yaygınlaşmasında KVKK'nin etkisi yadsınamaz. Hal böyle olunca, gerek dijital gerekse fiziksel ortamda hazırlanan ve okuyucunun bilgisine sunulan çoğu hukuki metin, aslında ülkemiz için çok yenidir. Yukarıda ele aldığımız araştırmadan da çıkarılacağı üzere, bu tarz metinlerin ilgili kişiye sunulması çoğu zaman ilgili kişi nezdinde rahatsız edici karşılanmaktadır. Kanaatimce bu tarz hukuki metinlere bakış açısı, ilgili kişi nezdinde, veri sorumlusu tarafından KVKK kapsamındaki bir yükümlülüğünün yerine getirildiği veya en azından yerine getirilmeye çalışıldığı şeklinde olmaktansa “imzalanması gereken bir evrak” veya “işleme devam edebilmek için işaretlenmesi gereken bir kutucuk” şeklinde ele alınmaktadır.

³⁶⁶ B.H.M. Custers/ Simone van der Hof/ B. Schermer, **Privacy expectations of social media users: The role of informed consent in privacy policies**. *Policy & Internet*, 2014, 6(3), s. 280

Netice itibariyle tüketici, anlaşılması zor, son derece uzun ve ağır bir dille yazılmış hukuki metinlerle karşılaştığı takdirde okumama eğilimi içerisinde. Bu nedenle, KVKK kapsamındaki yükümlülüklerini tam anlamıyla yerine getirmeye gayret gösteren bir Türk ticaret şirketi ile hiçbir yükümlülüğünü yerine getirmeyen bir Türk ticaret şirketi kıyaslandığında ortaya ciddi farklar çıkabilir.

Bu kapsamda, uyumluluğu sağlamaya gayret gösteren bir Türk ticaret şirketinin elinde ilgili kişinin bilgisine sunulması gereken açık rıza metni, aydınlatma metni, gizlilik taahhütnamesi gibi evraklar bulunmaktayken sektördeki rakibi olan diğer firmanın elinde bu formatta hiçbir evrak bulunmayabilir. İlaveten, uyumluluğa gayret gösteren şirket, teknik tedbirlerin sağlanması için bir firmadan, hukuki yükümlülüklerin yerine getirilmesi içinse bir hukuk bürosundan danışmanlık hizmeti almış olabilir ve harcamalarının belirli bir kalemini de KVKK kapsamındaki uyumluluğunun sağlanması oluşturabilir. Öte yandan sektördeki diğer rakibinde böyle bir maliyet kalemi hiçbir zaman olmayacaktır.

Her iki şirket kıyaslandığında, kanaatimce tüketici nezdinde ikinci şirket, birinci şirkete nazaran işine daha çok odaklanan, evrak işleriyle tüketiciyi yormayan, tüketiciye herhangi bir metin imzalamak zorunda bırakmayan bir şirket olarak değerlendirilebilecektir. Ek olarak, ikinci şirketin KVKK kapsamında bir maliyet kalemi olmayacağı için, ürününü veya hizmetini fiyatlandırma noktasında bu da belirleyici bir etken olabilecek ve tüketicinin tercihini etkileyebilecektir. Dolayısıyla olaya sadece ticari açıdan bakılacak olursa, tüketiciyi elinde tutabilmek, evrak işleriyle uğraşmamak, bütçeyi daha farklı alanlarda kullanabilmek için ikinci şirketin davranışı cazip gibi görünmektedir.

Öte yandan, KVKK kapsamında hiçbir yükümlülüğünü yerine getirmemiş olan şirket açık bir şekilde KVKK'ye aykırı birçok işlem gerçekleştirmiş olacaktır. İşte bu durumda kanaatimizce *“İş şartlarına uymamak; özellikle kanun veya sözleşmeyle, rakilere de yüklenmiş olan veya bir meslek dalında veya çevrede olağan olan iş şartlarına uymayanlar dürüstlüğe aykırı davranmış olur.”* şeklindeki TTK m. 55/ f. 1/ e bendi uyarınca haksız rekabet konusu gündeme gelebilir.³⁶⁷

³⁶⁷ Kanaatimizce İş şartı kavramı ile anlatılmak istenen herhangi bir mevzuata aykırılık yahut sözleşmeye aykırılık durumudur. Benzer değerlendirme için bkz: AÇIKGÖZ, a.g.e., s. 49

Maddeden anlaşılacağı üzere iş şartlarına uymamanın haksız rekabet teşkil edebilmesi için ortada bir iş şartı bulunmalı, taraflara arasında rakiplik ilişkisi bulunmalı ve iş şartlarına uyulmamış olmalıdır.

KVKK kapsamında, Türk ticaret şirketlerine belirli yükümlülükler yüklendiğinden maddede geçen “kanun ile rakiplere de yüklenmiş olan iş şartları” unsuru gerçekleşmiş olacaktır. Ayrıca, yukarıda örneğimizde izah ettiğimiz şekilde bir Türk ticaret şirketinin KVKK kapsamındaki yükümlülüklerini yerine getirmemesi “iş şartlarına uymama” olarak nitelendirilebilecektir. Bunun neticesinde de somut olayın özellikleri göz önünde bulundurulmakla birlikte TTK m. 56 vd. hükümlerinin tatbik imkânı doğabilecektir.

XI- KVKK KAPSAMINDAKİ SORUMLULUĞUN TESPİTİNDE TTK M. 366/ F. 2 VE TTK M.375 HÜKÜMLERİNİN ETKİSİ

Bir şirket nezdinde, KVKK kapsamında hukuka aykırılık olarak nitelendirilebilecek herhangi bir ihlal meydana geldiğinde, bu ihlal tamamen bir çalışanın kusurlu davranışından kaynaklansa dahi Kişisel Verileri Koruma Kurumu tarafından hükmedilecek idari para cezasının muhatabı veri sorumlusu olan şirkettir.

İdari para cezası yaptırımını alan bir şirket, eğer şartları mevcut ise çalışanına rücu edebilmektedir. Çalışmamızın bu bölümünde tartışmaya açacağımız konu ise, bir şirket nezdinde meydana gelen KVKK kapsamındaki hukuka aykırı ya da eksik/ hatalı uygulamalarda şirket yetkililerinin 6102 sayılı Türk Ticaret Kanunu³⁶⁸ m. 375 bağlamında sorumluluğunun olup olmadığı ve varsa kusur oranının neye göre belirleneceğidir.

Yönetim kurulunun devredilemez ve vazgeçilemez görev ve yetkileri TTK m. 375’te düzenlenmiştir. KVKK bağlamında ele almak istediğimiz kısım ise “Yönetimle görevli kişilerin, özellikle kanunlara, esas sözleşmeye, iç yönergelere ve yönetim kurulunun yazılı talimatlarına uygun hareket edip etmediklerinin üst gözetimi” şeklindeki TTK m. 375/ f. 1, e bendidir.

Maddeye göre yönetimle görevli kişilerin kanunlara, yönetim kurulunun yazılı talimatlarına uygun hareket edip etmediğinin üst gözetimi yönetim kurulunun

³⁶⁸ RG., 27846 S., 14.02.2011 T.

devredilemez ve vazgeçilemez bir görevidir. O halde yönetim kurulu, yönetimle görevlendirdiği kişi, komisyon, komite gibi yapıları denetlemek zorundadır.³⁶⁹

Maddede geçen kanun kavramı genel anlamda kullanıldığından KVKK da bu kapsam içerisinde. Öyleyse yönetim kurulunun bir görevi de yönetimle görevli kişilerin KVKK'ye uygun hareket edip etmediğinin ve KVKK uyarınca verilen yazılı talimatlara uygun davranıp davranmadığının üst gözetimini sağlamaktır.³⁷⁰ Dolayısıyla yönetim kurulu, her ne kadar bir kontrol makamı olmasa da şirketin KVKK'ye uyumluluğunun sağlanabilmesi için altyapıyı hazırlaması gereken organdır.

KVKK uyum süreçleri için şirket içerisinde bir “kişisel verileri koruma komitesi” kurulması mümkündür. Yönetim kurulunun genel manada gözetleme ve denetim yükümlülüğünün ifası için profesyonel kişilerden oluşan komitelerden istifade edilebilmektedir.³⁷¹ Uygulamada sıklıkla karşılaşılan durum da KVKK uyum süreci için şirket içerisinde bir komite kurulmasıdır. Aslında bu komiteler TTK m. 366/ f. 2'nin verdiği yetkiye dayanarak kurulmaktadır. Belirtmek gerekir ki yönetim kurulunun böyle bir komite kurma zorunluluğu bulunmamaktadır.³⁷² Bununla birlikte, bazı şirketlerin ciddi derecede büyük ve karmaşık yapıya sahip olması, çok sayıda yöneticinin görev yapması ve bu alanın tamamının yönetim kurulu tarafından kontrolünün mümkün olmaması sebebiyle büyük yapıya sahip şirketlerde sıklıkla denetim komitelerine rastlanmaktadır.³⁷³

Kanaatimizce, TTK m. 375/ f. 1, e bendi uyarınca eğer veri sorumlusu olan şirket KVKK uyumluluğu kapsamında hiçbir çalışma yürütmemiş, KVKK

³⁶⁹ Hakan ÇEBİ, **Şirketler Hukuku**, Ankara: Seçkin Yayıncılık, 2020, s. 171

³⁷⁰ Madde gerekçesinde e bendinde yer alan üst gözetim kavramı hakkında aynen “Üst gözetim ile kastedilen hem kuramsal açıdan hem de işletme iktisadi yönünden gerekli olan işlerin akışının gözetimidir. Yoksa, yönetim kurulu bir kontrol ve denetim organı değildir. Üst gözetimin normatif niteliği hükmün bizzat kendisinden anlaşılmaktadır.” ifadelerine yer verilmiştir. (<https://www.lexpera.com.tr/mevzuat/gerekciler/turk-ticaret-kanunu-madde-gerekceleri/1>) (Erişim: 06.11.2023)

³⁷¹ Şaban KAYIHAN, **6102 Sayılı Yeni Türk Ticaret Kanunu'na Göre Anonim Şirketlerde Üst Gözetim**, Ankara, 2011, s. 133

³⁷² Bazı anonim şirketlerin çok büyük yapıda olabilmesi sebebiyle şirketin menfaatini gerektiren bazı durumlarda denetim komitesi kurulması gerektiği ve aksi takdirde gerekli özen ve tedbirin gösterilmemesi sebebiyle yönetim kurulunun sorumluluğunun gündeme gelebileceği hakkındaki görüş için: Mustafa İsmail KAYA, “Anonim Şirket Yönetim Kurulunun Denetim ve Gözetim Görevi”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 16, Özel Sayı 2014, s. 3269

³⁷³ Hasan PULAŞLI, Türk Ticaret Kanunu Tasarısı'na Göre Anonim Şirket Yönetim Kurulu Üyelerinin Özen Yükümlülüğü ve Müteselsil Sorumluluğu, **Banka ve Ticaret Hukuku Dergisi**, 2009, Cilt: 25, Sayı: 1, s. 41

kapsamındaki yükümlülüklerini yerine getirmemiş, adeta böyle bir kanun yokmuş gibi hareket etmişse artık yönetim kurulu üyelerinin sorumluluğu gündeme gelecektir.

Öte yandan, yönetim kurulu KVKK kapsamında uyumluluğun sağlanması için bir adım atmış olabilir. Örneğin dışarıdan profesyonel bir destek almayı tercih edebilir veya şirket bünyesinde bu konuyla ilgilenecek bir ekip kurmuş olabilir. Yönetim kurulunun bir ekip kurması ya da dışarıdan destek alması KVKK uyumluluğu kapsamında atılmış bir adım olsa da tek başına yükümlülüklerin yerine getirildiği anlamına gelmez. Kanaatimizce yönetim kurulundan beklenen, yükümlülüklerin yerine getirilip getirilmediği konusunda komiteye veya destek aldığı ekibe yazılı talimatlarda bulunması, süreci takip etmesi, yükümlülüklerin yerine getirilmediği noktalarda eksikliklerin giderilmesi için müdahale etmesi, özetle uyumluluğun sağlanması için asgari özeni göstermesidir.

Hemen belirtmek gerekir ki elbette yönetim kurulunun bir kanuna uyumluluk çalışmalarının istenildiği gibi gidip gitmediğini anlayabilmesi mümkün değildir. Öte yandan, çalışanlara eğitim verilip verilmediği, gerekli dokümanların hazırlanıp hazırlanmadığı, dokümanların şirket içerisinde hayata geçirilmesi noktasında herhangi bir çalışma yapıp yapılmadığı, çalışmanın gerçekten mi yapıldığı yoksa kağıt üzerinde mi kaldığı, yükümlülüklerin tamamının yerine getirilip getirilmediği gibi konular yönetim kurulunun rahatlıkla idrak edebileceği konulardır. Örnek olarak belirttiğimiz bu gibi durumların ihmal edilmesi halinde yönetim kurulu üyelerinin de sorumluluğunun gündeme geleceği kanaatindeyiz.

Özetlemek gerekirse, yönetim kurulunun sorumluluğunun KVKK bağlamında incelendiği durumlarda ikili bir ayırım yapmak suretiyle konuyu ele almak gerekir. Birinci ihtimalde, KVKK uyumluluğu konusunda komite kurulmamış ve aksiyon doğrudan şirket tarafından alınıyor olabilir. Bu durumda yönetim kurulunun somut olaya yaklaşımını detaylıca incelemek gerekir. Örneğin yönetim kurulu, KVKK kapsamındaki yükümlülüklerin yerine getirilmesi noktasında hiçbir adım atmaz, adeta kanun yokmuş gibi hareket ederse sorumluluğunun doğacağı noktasında hiçbir tereddüt bulunmamaktadır. Bununla birlikte, yönetim kurulu tarafından KVKK uyumluluğunun sağlanabilmesi ve yükümlülüklerin yerine getirilmesi için belirli adımlar atılmış olabilir. Şirket dışı profesyonel bir ekipten destek alınması veya şirketin kendi içerisinde birtakım çalışmalar yapması bu bağlamda ele alınabilir. Bu noktada dikkat edilmesi gerekenler hususların başında yönetim kurulunun devam eden

işlerle ilgili bilgi sahibi olmaya gayret gösterip göstermediği yer almaktadır. Özellikle yönetim kurulu, çalışanlara eğitim verilir verilmeyeceği, gerekli dokümanların hazırlanıp hazırlanmadığı, dokümanların şirket içerisinde hayata geçirilmesi noktasında herhangi bir çalışma yapıp yapılmadığı, çalışmanın gerçekten mi yapıldığı yoksa kağıt üzerinde mi kaldığı, yükümlülüklerin tamamının yerine getirilip getirilmediği konularında bilgi sahibi olmaya gayret göstermelidir. Bir diğer dikkat edilmesi gereken nokta yönetim kurulunun konuyla ilgili emir ve talimatlarda bulunması ve yazılı bir raporlama talep etmesidir. Bu yaklaşım da yönetim kurulunun hem yükümlülüklerin ifası noktasında aktif davrandığını hem de şirketin risk ve tehditlerini belirleme konusunda hassasiyet gösterdiğini ispatlamaktadır. Ayrıca, yapılan raporlamaların analiz edilmesi, raporlama doğrultusunda ihtiyaçların karşılanması, eksikliklerin giderilmesi, ele alınması gereken bir diğer kriterdir. Netice itibarıyla hem yukarıda izah olunmaya çalışılan kriterler uyarınca hem de yönetim kurulunun sorumluluğuna ilişkin genel düzenlemeler uyarınca KVKK kapsamındaki yükümlülüklerin yerine getirilmesinde yönetim kurulunun sorumluluğu her somut olayın özelliklerine göre ayrıca değerlendirilmelidir.

İkinci ihtimalde, KVKK uyumluluğunun sağlanabilmesi için bir komite kurulmuş olabilir. Burada dikkat edilmesi gereken ilk husus, yönetim kurulunun komite üyelerini seçerken gerekli dikkat ve özeni gösterip göstermediğidir. Her somut olayın özelliğine göre ayrıca değerlendirilecek olan bu husus uyarınca eğer yönetim kurulu, komite üyelerini seçerken gerekli dikkat ve özeni göstermemiş ise sorumluluğu gündeme gelebilecektir. Belirtmek gerekir ki komitenin kurulmuş olması, yönetim kurulunun sorumluluğunun ortadan kalktığı anlamına gelmeyecektir. Zira üst gözetim yükümlülüğü, yönetim kurulunun devredilemez görev ve yetkilerindendir. Bu nedenle, bir önceki paragrafta yaptığımız açıklamalar, yönetim kurulunun üst gözetim yükümlülüğünün ifası bakımından da geçerlidir.

Tam da bu noktada ele alınması gereken bir diğer düzenleme, TTK m. 553/ f. 3 hükmüdür.³⁷⁴ Hüküm aynen “*Hiç kimse kontrolü dışında kalan, kanuna veya esas sözleşmeye aykırılıklar veya yolsuzluklar sebebiyle sorumlu tutulamaz; bu sorumlu olmama durumu gözetim ve özen yükümü gerekçe gösterilerek*

³⁷⁴ Doktrinde TTK m. 553 / f.3 hükmü, TTK m. 375’e aykırı olduğu, gözetim yükümlülüğünü faydasız hale getirdiği gerekçesi ile eleştirilmiştir. Daha detaylı açıklama için bkz. ÇEBİ, a.g.e., s. 223.

geçersiz kılınamaz.” şeklindedir.³⁷⁵ Buradan hareketle, yönetim kurulunun KVKK kapsamında uyumluluğu sağlamak için gerekli tüm gözetimi ve özeni göstermesinin zorunlu olduğu ancak yönetim kurulundan kaynaklanmayan ve yönetim kurulunun kontrolü dışında gerçekleşen aksaklıklarda yönetim kurulunun sorumluluğundan söz edilemeyeceği düşünülebilir. Belirtmek gerekir ki kontrol alanının dışında kalması ile kastedilen normal şartlarda ilgili durumun öngörülme ihtimalinin bulunmaması, tahmin edilemeyecek derecede olması, müdahale edilse bile önlenmesinin mümkün olmamasıdır.³⁷⁶

Sonuç olarak yönetim kurulunun KVKK kapsamında uyumluluğu sağlamak için gerekli tüm gözetimi ve özeni göstermesi zorunludur. İzah ettiğimiz açıklamalar doğrultusunda bazı hallerde yönetim kurulu üyelerinin sorumluluğunun gündeme geleceği ve veri sorumlusu olan şirketin, yönetim kurulu üyelerine kusurları oranında rücu edebileceği kanaatindeyiz.

³⁷⁵ Hüküm gerekçesinde, yönetim kurulu üyelerinin insan üstü bir efor göstermesinin, dolayısı ile şirketteki her durumdan haber olmamasının olağan olduğu belirtilmiştir. Gerekçe aynen “Üçüncü fıkra yönetim organının, organsal işlevi ister kanuna göre devredilmiş olsun, ister organın kendisinde kalsın üyelerin gözetim yükümlerini tanımakta, ancak bu yükümün kontrol dışında kalan olgu ve konularda bulunmadığını hükme bağlamaktadır. Bu hüküm yönetim ile görevli kişilerin bu arada yönetim kurulu üyelerinin uygun nedensellik bağının veya kusurlarının yokluğu halinde, soyut bir gözetim (nezaret) görevi anlayışına dayanılarak sorumlu tutulmalarına engel olmak amacıyla öngörülmüştür. Çünkü, uygulamada yönetim kurulu üyelerinin insan takatinin üstünde bir gözetim anlayışıyla şirketteki her türlü kanuna veya esas sözleşmeye aykırılıktan sorumlu tutuldukları gözlemlenmiştir.” şeklindedir.

³⁷⁶ Ünal TEKİNALP, *Sermaye Ortaklıklarının Yeni Hukuku*, 3. Bası, İstanbul, 2013, s. 384

SONUÇ

Kişisel Verilerin Korunması Kanunu ile veri sorumlusuna getirilen yükümlülükler arasında aydınlatma yükümlülüğü, VERBİS kayıt yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından yapılan başvuruların cevaplanması yükümlülüğü, kurul kararlarının yerine getirilmesi yükümlülüğü ve kişisel verilerin imha edilmesi yükümlülüğü yer almaktadır.

Çalışmamızda, sıklıkla atıfta bulunduğumuz Kişisel Verileri Koruma Kurulu kararları uyarınca Türk ticaret şirketlerinden beklenenlere ilişkin bazı sonuçlar elde ettik. Özellikle Kişisel Verileri Koruma Kurulu’nun bir Türk ticaret şirketinden kanunda açıkça yer almamakla birlikte “aktif özen yükümlülüğü” ismiyle bir özen yükümlülüğü beklentisinin oluştuğu elde ettiğimiz ilk çıkarımlardandır.

Ayrıca temel manada Kişisel Verileri Koruma Kurulu’nun kişisel verilere hukuka aykırı erişimi önleme yükümlülüğü kapsamında bir Türk ticaret şirketinde ne şekilde olursa olsun bir verinin şirket dışına çıkması halinde idari yaptırım uyguladığı kanaatine vardık. Bu durumlarda, ister veri sorumlusunun ihmalinden kaynaklı olsun, ister veri sorumlusu her şeyi yapmasına rağmen ihlal meydana gelsin isterse tamamen bir işçiden kaynaklansın her halükârda veri sorumlusu hakkında idari yaptırım uygulandığı sonucuna vardık. Öyleyse Kişisel Verileri Koruma Kurulu’nun kişisel verilere hukuka aykırı erişimin engellenmesi kapsamında bir Türk ticaret şirketinden beklentisinin verinin, veri sorumlusunun kontrolü dışında dışarı çıkış yollarının imkânsız hale getirilmesi yönünde olduğunu söylemek yanlış olmaz. Nitekim çalışmamızda belirttiğimiz bir kararda bir çalışanın bir anlık dalgınlığından faydalanmak suretiyle gizlice çalışan bilgisayarından fotoğraf çekilmesi durumunda dahi bu yükümlülüğün ihlal edildiğine kanaat getirilmiştir. Öyleyse Kişisel Verileri Koruma Kurulu, bu yükümlülük açısından asgari değil maksimum seviyede bir güvenlik beklentisi içerisindedir. Bu beklentisi de hem kişisel veri içeren fiziki ortamları hem de dijital ortamları kapsamaktadır.

Bir diğ er ele aldığımız konu ise VERBİS kayıt yükümlülüğüdür. Bu konuyla ilgili sadece çalışma kapsamında değil aynı zamanda uygulamaya da yönelik bazı eleştirilerde bulunmak isteriz. Kişisel Verileri Koruma Kurumu kanaatimizce VERBİS kayıt yükümlülüğünü Türkiye’deki veri sorumlularına, özellikle ticaret şirketlerine çok yanlış ve hatalı bir şekilde tanıtmıştır. Türkiye’de faaliyet gösteren birçok şirket ne yazık ki Kişisel Verilerin Korunması Kanunu’nu VERBİS kayıt yükümlülüğünden ibaret zannetmektedir. Hatta bazı veri sorumluları, VERBİS için kullanıcı adı ve şifre temin ettiğinde artık her şeyi bitirdiği düşüncesine kapılmaktadır. Burada bir iletişim eksikliği olduğu kanaatindeyiz. Zira Türkiye’de ticaret şirketlerinin yıllardan beri süregelen bir alışkanlığı söz konusudur. Bir şirket için ilk defa bir yükümlülük meydana geldiğinde şirket eğer varsa hemen meslek odasına bu konuyu sormakta, aynı sektörde faaliyet gösteren diğ er şirketlerden bilgi almakta, muhasebecisine dahi konuyu sormakta ancak ne yazık ki varsa en son avukatına sormaktadır. Hal böyle olunca ilk bilgi kaynağı meslek odaları haline gelmektedir. Bu nedenle Kişisel Verileri Koruma Kurulu’nun her meslek odasıyla tek tek görüşerek VERBİS kayıt yükümlülüğünü daha basit bir biçimde anlatmasının daha sağlıklı bir yöntem olabileceği düşüncesindeyiz.

Öte yandan VERBİS, kendi içerisinde de kanaatimizce birçok soru işaretini barındırmaktadır. Örneğin bir şirketin VERBİS kaydını alanında uzman beş farklı kişinin yapması halinde beş farklı kayıt ortaya çıkmaktadır. Öte yandan, hukuki olan biricik ve tektir. Bu konuda tekdüzeliğin sağlanamamasının en büyük nedeni, VERBİS’te yer alan kişisel veri işleme amaçlarının neyi ifade ettiğini açıklayan yol gösterici bir kaynak olmamasıdır. Örneğin bir kişisel veri işleme amacından iki kişi birbirinden tamamen farklı şeyi algılayabilmektedir. Kanaatimizce, VERBİS’te gösterilen bir kişisel veri işleme amacının eksik veya fazla seçilmesinden dolayı Kişisel Verileri Koruma Kurulu’nun salt bu gerekçeyle yaptırım uygulayabilme yetkisi yoktur.

Ayrıca belirtmek isteriz ki VERBİS kayıt yükümlülüğüne ilişkin son kayıt tarihlerinin sürekli ertelenmesi, birçok şirket tarafından bunun önemslenmediği, sürekli erteleneceği, ertelenmese de kimseye cezai yaptırım uygulanmayacağı, sadece şikayet edilen şirketlerin sorun yaşayabileceği aksi durumda hiçbir şey olmayacağı görüşünün oluşmasına sebebiyet vermiştir. Netice itibariyle Kişisel Verileri Koruma Kurulu’nun

çok acilen bir iletişim stratejisi geliştirmek suretiyle VERBİS kayıt yükümlülüğüne ilişkin bu kötü imajı ortadan kaldırması gerekmektedir.

Konuyla ilgili belirtmek istediğimiz son husus da VERBİS kayıt yükümlülüğünün yıllık mali bilanço ve işçi sayısı gibi faktörlere bağlanmasıdır. Örneğin mali bilançosu çok düşük, çalışan sayısı da ellinin altında olan ve ana faaliyet konusu da özel nitelikli kişisel veri işlemek olmayan bir şirketin işlediği kişisel veriler daha mı değersizdir? Bu şirket VERBİS açısından neden sistemin dışında tutulmaktadır? Kanaatimizce VERBİS ya tamamen kaldırılmalı ya da herkes bunun içerisine dahil edilmelidir. Buradaki temel yaklaşımın şeffaflığı sağlamak olduğu vurgulanmaktadır. Çalışan sayısı ya da mali bilanço toplamı gibi kriterler şeffaflık karşısında çok ilginç kriterlerdir. Bu nedenle ilgili kriterlerin acilen değiştirilmesi gerekmektedir.

Çalışma kapsamında ele aldığımız ve ulaştığımız bir diğer sonuç ise kişisel verilerin aktarılmasına ilişkindir. Özellikle kişisel verilerin yurtdışına aktarılmasına ilişkin maddenin acilen değiştirilmesi gerektiği kanaatindeyiz. Zira kanun koyucu bu madde ile üç yol öngörmektedir ancak bu yollardan sadece açık rıza yöntemi uygulamada makul olmaktadır. Açık rızanın geri alınabilirliği her zaman mümkün olduğundan ve açık rıza da hizmet şartına bağlanamayacağından bu gibi durumları yaşayan binlerce veri sorumlusu eli kolu bağlı durumdadır. Bu nedenle madde ihtiyacı karşılar nitelikte değildir. Kişisel verilerin yurt dışına aktarılmasında kapsamın genişletilmesi gerekmektedir.

Veri ihlali bildirim yükümlülüğünde ise kanun koyucunun doğru bir yöntem tercih etmediği kanaatindeyiz. Zira kanun ile öngörülen sistem uyarınca veri sorumlusunun kendi kendisini ihbar etmesi beklenmektedir. Kendisini ihbar eden veri sorumlusu ise her türlü idari para cezası yaptırımını ile karşı karşıya kalmaktadır. Öyleyse kamuoyuna yansıma ihtimali olmayan bir veri sorumlusu neden kendisini ihbar etsin sorusu akla gelmektedir. Bu soru işaretini gidermek için veri sorumlusuna uygulanacak idari yaptırımda mutlak surette belirli bir oranda indirim yapılması gerektiği kanaatindeyiz. Zira mevcut yaklaşım ile hiçbir veri sorumlusu kendisini ihbar etmek istemez ve etmemektedir. Kişisel Verileri Koruma Kurulu tarafından yayınlanan veri ihlal bildirim sayısı-her ihlalin yayınlanmadığı bilinmekle birlikte- makul kabul edilemeyecek düzeyde düşüktür. Öyleyse birçok şirket bu yükümlülüğü ihlal etmeyi

tercih etmektedir. Bu nedenle de cezalandırıcı değil teşvik edici bir model tercih edilmeli ve cezada indirim modeli tercih edilmelidir.

KVKK bir bütün olarak incelendiğinde, veri sorumlusunun Kişisel Verileri Koruma Kurumu ile işbirliği içerisinde hareket etmesinin ve şeffaf davranmasının herhangi bir karşılığı bulunmamaktadır. Bu noktada referans olarak GDPR ele alınabilir. GDPR uyarınca denetim makamı ile gerçekleştirilen işbirliği derecesi, idari para cezasına hükmedilip hükmedilmeyeceği ve hükmedilecekse miktarın tespiti noktasında bir kriter olarak yer almaktadır. Bu düzenleme, veri sorumlusu ile denetim makamı arasındaki ilişkiyi güçlendirecek niteliktedir. KVKK’de ise her halükârda veri sorumlusu hakkında idari yaptırım uygulandığı için veri sorumlusu ihbar bildiriminde bulunmaktan imtina etmektedir. Özellikle, Kişisel Verileri Koruma Kurulu’nun da re’sen denetim yapmak suretiyle ihlal bildiriminde bulunmayan şirketleri tespit etme gibi bir eğilimi söz konusu olmadığı için veri sorumluları bu konuda son derece rahat hareket etmektedir. Bu nedenle, yaptığımız veri ihlal bildirimine ilişkin maddenin yeniden ele alınması gerektiği ve ihlale maruz kalan veri sorumlusu ile Kişisel Verileri Koruma Kurumu arasındaki işbirliğinin, yaptırım uygulayıp uygulamama noktasında bir kriter olarak getirilmesi gerektiği kanaatindeyiz.

Ayrıca belirtmek gerekir ki gerek doktrinde gerekse Kişisel Verileri Koruma Kurulu kararlarına konu olaylarda ortak yaklaşım, veri sorumlusunun tüm süreçlerinde genel ilkelere dikkat etmesi gerektiğidir. Özellikle her şirket, kendi ihtiyaçları doğrultusunda ölçülülüğe ve kişisel verileri işleyeceği sürelerle son derece dikkat etmelidir. Bu bağlamda imha yükümlülüğünü hiçbir surette ihmal etmemeli, periyodik imhaları kurumsal bir kültür haline getirmelidir. Nasıl ki her şirket ay sonu geldiğinde belirli sigorta ödemelerinin ve vergi ödemelerinin vaktinin geldiğini biliyorsa her belirlenen dönem yaklaştığında da kişisel veri imha edeceğini, bunun vaktinin yaklaştığını bilmelidir.

Kanunda bazı yükümlülüklerin yerine getirilmesi nispeten daha kolaydır. Kanaatimizce ilgili kişinin başvurularının cevaplanması yükümlülüğü ve kurul kararlarının yerine getirilmesi yükümlülüğü böyledir. Gerek kanun koyucunun gerekse Kişisel Verileri Koruma Kurulu’nun burada beklentisi çok nettir. Bazı yükümlülükler ise nispeten daha zordur. Kanaatimizce beklentiye karşılamanın en zor olduğu yükümlülük, kişisel veri güvenliğine ilişkin yükümlülüklerdir. Zira burada bırakılacak en ufak bir boşluk dahi ihlale sebebiyet verebilecek cinstendir. Bu nedenle

kanaatimizce Türk ticaret şirketlerinin veri güvenliğine yönelik yükümlülüklerine ayrıca dikkat etmesi gereklidir. Kişisel Verilerin Korunması Kanunu kapsamında bir Türk ticaret şirketinin uyumluluğu sağlaması için kanaatimizce aynı anda hem bir avukat hem de alana çok hakim bir bilişim güvenliği uzmanıyla çalışılması faydalı olacaktır. Zira kanunda belirtilen yükümlülükler tek taraflı yükümlülükler değildir. Disiplinler arası ortak bir çalışmanın sonucunda uyumluluk ancak sağlanabilir. Bu nedenle hiçbir bölümün ihmal edilmemesi gerekir.

Her şirket açısından kanun kapsamındaki ihtiyaçlar farklıdır. Bu ihtiyaç ve gerekliliklerin çok iyi tespit edilmesi gerekmektedir. Örneğin tüm Türkiye’de bilinen bir e-ticaret şirketinin ihtiyaçları ve bu şirketten beklenenler ile bir saç ekim merkezinden beklenenler farklılık arz edecektir. Dolayısıyla bir şirketin ihtiyacını ve eksikliklerini en iyi bilen, o şirketin yöneticileridir. Kanun kapsamında temel bir eğitim alan yöneticiler ve departman yetkilileri, çok rahatlıkla şirketin zayıf taraflarını, nerede problem yaşayabileceklerini tespit edebilirler ve risk analizi yapabilirler. Bu nedenle, yükümlülüklerin yerine getirilmesi noktasında şirket yetkililerine büyük görevler düşmektedir. Bazı alanlar çok belirgin bazı alanlar ise gözden kaçabilecek niteliktedir. Özellikle veri güvenliği konusunda Kişisel Verileri Koruma Kurulu’nun yaklaşımı göz önünde bulundurulduğunda hiçbir alanda boşluk bırakılmamalıdır.

Son elde ettiğimiz sonuç ise şirket yöneticilerinin ve yönetim kurulunun bu yükümlülükler kapsamında önemli bir rolü olduğu ve bazı durumlarda sorumluluklarının gündeme geleceğidir. Konuyla ilgili çalışmalar incelendiğinde genellikle konu rücuya geldiğinde hep bir örnek olarak şirketin çalışanına rücu etmesi verilir. Öte yandan, nasıl ki bir çalışana kusuru oranında rücu etmek mümkün ise bir yöneticiyi de belirli şartların dahilinde rücu edebilmek mümkün olmalıdır. Çalışmamızın en sonunda da bu kanaate yer verilmiş ve detaylıca ele alınmıştır.

KAYNAKÇA

AÇIKGÖZ, Deniz Çalışanın Haksız Rekabet Eylemleri ve Tazminat Sorumluluğu – Ticaret Hukuku Monografileri, Ankara: Seçkin Yayıncılık, 2023

AKİPEK, Jale G./ **AKINTÜRK**, Turgut/ **ATEŞ KARAMAN**, Derya, Türk Medeni Hukuku, Başlangıç Hükümleri, Kişiler Hukuku, C. I, 8. Bası, İstanbul, 2011

AKKURT, Sinan Sami, “Açık Rıza”, iç. Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik; Ankara, 2023, s. 155-187

AKSOY, Hüseyin CAN, Kişisel Verilerin Korunması, Yayınlanmış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, 2008

AKSOY, Hüseyin CAN, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, 1. Bası, Ankara, Çakmak Yayınevi, 2010

ALTINDERE, Murat, Kişisel Verilerin Korunması Hukuku ve Uygulaması. 1.Basım, Ankara, Adalet Yayınevi, s. 47-51

ARAL, Fahrettin/ **AYRANCI**, Hasan, Borçlar Hukuku Özel Borç İlişkileri, 9. Baskı, Ankara, 2012

ARPACI, Abdulkadir, Kişiler Hukuku (Gerçek Kişiler), 2. Bası, İstanbul, 2000

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 4/2007 on the Consept of Personal Data, 01248/07/EN, WP 136

ARTICLE 29 DATA PROTECTION WORKING PARTY, No 203 (2013), Opinion 03/2013 on purpose limitation

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14 EN, WP 217

AVCI BRAUN, Cihan, “Kişisel Verilerin İşlenmesinde Rıza”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S.1, 2018, s.13-35

BAŞALP, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, 2009

BAŞALP, Nilgün, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 21, Sayı 1, 2015, s. 77-105

BAYKAL, Sanem /**GÖÇMEN**, İlke, “Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi”, Prof. Dr. Erdal Onar’a Armağan, Ankara, 2013, s. 317-365

BİNARK, Mutlu: “Habeas Data Kavramı ve Kavramın Kişisel Verilerin Korunması Tartışmalarına Katkısı”, Kültür ve İletişim Dergisi, Eylül 2015- Şubat 2016, C. 18, S. 36, s. 196-207

BYGRAVE, Lee A./**TOSONİ**, Luca “Article 4(13) Genetic Data”, iç. The EU General Data Protection Regulation (GDPR), A Commentary (Ed. Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY), Croydon : Oxford University Press, 2020, s. 196-207

CANBAY, Yavuz, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik; Ankara, 2023, s.319-342

CUSTERS, B.H.M. / **Van der Hof**, Simone/ **SCHERMER**, B., Privacy expectations of social media users: The role of informed consent in privacy policies. Policy & Internet, 2014, 6(3), s. 268-295

ÇEBİ, Hakan, Şirketler Hukuku, Ankara: Seçkin Yayıncılık, 2020

ÇEKİN, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul, On İki Levha Yayıncılık, 2020 (ÇEKİN)

ÇEKİN, Mesut Serdar, “6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 74, Sayı 2, 2016, s. 630-644

ÇEKİN, Mesut Serdar /**BERKTAŞ**, Ahmet Esad /**AKINCI**, M. Furkan Veri Hukuku, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2023

ÇELİK, Nuri/ **CANIKLIOĞLU**, Nurşen/ **CANBOLAT**, Talat, İş Hukuku Dersleri, Beta Yayınevi İstanbul, 2020,

DEVELİOĞLU, Murat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017

DURAL Mustafa/ **ÖĞÜZ**, Tufan, Türk Özel Hukuku, C. II, Kişiler Hukuku, 12. Bası, İstanbul, 2012,

DÜLGER, Murat Volkan, Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul, Hukuk Akademisi, 2020

GÜNAL, Ayşe Nida/ **ÜSTÜN**, Yasin İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak “Meşru Menfaat”, Kişisel Verileri Koruma Dergisi. Cilt:4, Sayı: 2, 2022, s. 1-18

KAYA, Mehmet Bedii, İstanbul Hukuk Mecmuası, “Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verilebilirlik İlkesi”, 78 (4), 2020, s. 1859-1897

KAYA, Mustafa İsmail, “Anonim Şirket Yönetim Kurulunun Denetim ve Gözetim Görevi”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 16, Özel Sayı 2014, s. 3261-3286

KAYIHAN, Şaban, 6102 Sayılı Yeni Türk Ticaret Kanunu’na Göre Anonim Şirketlerde Üst Gözetim, Ankara, 2011

KESER BERBER, Leyla/ **ATABEY**, Ayça / **MERT**, Melis, E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, Kişisel Verileri Koruma Dergisi, Cilt: 1, Sayı: 2, 2019, s. 66-74

KÜZECİ, Elif, “Kişisel Verilerin Korunması Hakkı”, iç. Kişisel Verilerin Korunmasına Akademik Bakış- KVKK Akademi Derleme Çalışması (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik: Ankara 2023, s. 19-65 (KÜZECİ)

KÜZECİ, Elif, Kişisel Verilerin Korunması, İstanbul, On İki Levha Yayınları, 2021

LAMBERT, Paul B., Understanding the New European Data Protection Rules, Florida: CRC Press, 2018

LYNSKEY, Orla, The Foundations of EU Data Protection Law, Oxford University Press, 2015

MONDSCHIEIN, Christopher F. / **MONDA**, Casimo “The EU’s General Data Protection Regulation (GDPR) in a Research Context”, Fundamentals of Clinical Data Science (Ed: Pieter Kubben · Michel Dumontier Andre Dekker)

MILLER, Arthur R. The Assault on Privacy, Computers, Data Banks, and Dossiers, ABD: The University of Michigan Press, 1971

OĞUZMAN, M. Kemal/ **SELİÇİ**, Özer/ **OKTAY-ÖZDEMİR**, Saibe, Kişiler Hukuku, 14. Bası, İstanbul, Filiz Kitabevi, Ekim 2014

NOMER ERTAN, Füsün, Haksız Rekabet Hukuku, İstanbul: On iki Levha Yayıncılık, 2016

OĞUZMAN, M. Kemal/ **BARLAS**, Nami, Medeni Hukuk Dersleri, İstanbul, 2011

ÖZDEMİR, Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara: Seçkin, 2009

ÖZKAN, Oğulcan, Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara, 2020

ÖZSUNAY, Ergun, Gerçek Kişilerin Hukuki Durumu, İstanbul, 1979

PULAŞLI, Hasan, Türk Ticaret Kanunu Tasarısı’na Göre Anonim Şirket Yönetim Kurulu Üyelerinin Özen Yükümlülüğü ve Müteselsil Sorumluluğu, Banka ve Ticaret Hukuku Dergisi, 2009, Cilt: 25, Sayı: 1, s. 27-63

SCHWARTZ, Paul M./ **EIFER**, Karl-Nikolaus, Transatlantic Data Privacy, Kasım 2017, 106 Georgetown Law Journal, 2017;115. UC Berkeley Public Law Research Paper

ŞEKEROĞLU, Sinan/ **ÖZÜDOĞRU**, Haşim, Dijital Dönemin Koruyucuları: Siber Risk Sigortaları, 4. Uluslararası Sosyal Bilimler Araştırmaları Kongresi, 2019, s. 55-64

TAŞTAN, Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul, On İki Levha Yayıncılık, 2017

TEKİNALP, Ünal, Sermaye Ortaklıklarının Yeni Hukuku, 3. Bası, İstanbul, 2013

TINNEFIELD, Christian/ **HANSSEN**, Henrik, “Mobile Health in the EU (Part 2): Personal Data and Sensitive Information in Health Businesses”, <https://www.engage.hoganlovells.com/knowledgeservices/news/mobile-health-in-the-eu-part-2-personal-data-and-sensitive-information-in-mhealth-businesses>

TOSONI, Luca/ **BYGRAVE**, Lee A., “Article 4(2) Processing”, iç. The EU General Data Protection Regulation (GDPR), A Commentary (Ed. Christopher KUNER, Lee A. BYGRAVE, Christopher DOCKSEY), Croydon : Oxford University, 2020, s. 116-123.

TURAN BAŞARA, Gamze, Uyuşmazlık Mahkemesi Dergisi, “Kişisel Veri İşleme Sözleşmesi”, Yıl: 8, Sayı: 16, Aralık 2020, s. 57-90

UÇAK, Murat, Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası, Kişisel Verileri Koruma Dergisi, Cilt: 3, Sayı:1, 2020, s. 41-60

UNCULAR, Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara, Seçkin Yayıncılık, 2014

ÜSTÜN, Yasin/ **GÜNAL**, Ayşe Nida, İş İlişkilerinde Bazı Yaygın Uygulamaların Kişisel Verilerin Korunması Kanunu Kapsamında Değerlendirilmesi, Kişisel Verileri Koruma Dergisi, Cilt:2, Sayı:2, 2020, s. 61-74.

VOIGT, Paul/**VON DEM BUSSCHE**, Axel, The EU General Data Protection Regulation (GDPR), A Practical Guide, Cham: Springer, 2017

YILDIZ, Esra Tekil, İnternet Üzerinde Kişisel Verilerin Korunması, Prof. Dr. Fahiman Tekil’in Anısına Armağan, İstanbul, 2003

YILDIZ, Ünal., (2022). Habeas Data Kavramı ve Arjantin Örneği, Kişisel Verileri Koruma Dergisi. 4(1), 1-13

YÜCEDAĞ, Nafiye, “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, iç. Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması (Ed. AKSOY, Pınar Çağlayan / AKSOY, Hüseyin Can), Ütopya Grafik; Ankara, 2023, s.135-155 (YÜCEDAĞ)

YÜCEDAĞ, Nafiye, Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 75 Sayı 2, s. 765-789

ZEVKLİLER, Aydın/ **ACABEY**, Mehmet Beşir/ **GÖKYAYLA**, K. Emre, Medeni Hukuk (Giriş-Başlangıç Hükümleri-Kişiler Hukuku-Aile Hukuku), Ankara, 2000

ZEVKLİLER, Aydın / **GÖKYAYLA**, K. Emre, Borçlar Hukuku Özel Borç İlişkileri, 15. Baskı, Ankara, 2015

ELEKTRONİK KAYNAKLAR:

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Verilerin Korunması Kanunu ve Uygulaması Rehberi, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları No 1, Ankara, Aralık 2019, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları No: 3, Ankara, 2019

KİŞİSEL VERİLERİ KORUMA KURUMU, Çocukların Kişisel Verilerinin Korunması “Ürün ve Hizmet Geliştirenler Tarafından Dikkat Edilmesi Gerekenler”, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Sorularla VERBİS, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, KVKK Yayınları, Mart 2019, Ankara, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Özel Nitelikli Kişisel Verilerin İşlenme Şartları Rehberi, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Açık Rıza Rehberi, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Veri Sorumluları Sicili Rehberi, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Örneklerle Kişisel Verilerin Korunması, KVKK Yayınları No: 29, Ankara, Haziran 2019, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Veri İşleme Envanteri Hazırlama Rehberi, KVKK Yayınları No: 30, (www.kvkk.gov.tr),

KİŞİSEL VERİLERİ KORUMA KURUMU, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan 2019, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Verilerin İşlenme Şartları, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, (www.kvkk.gov.tr)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), (www.kvkk.gov.tr)

CEVRİMİÇİ KAYNAKLAR:

<https://www.resmigazete.gov.tr/>

<https://www.kvkk.gov.tr/>

<https://www.lexpera.com.tr/>

<https://eur-lex.europa.eu/homepage.html>

<https://dergipark.org.tr/tr/>

<https://kararlarbilgibankasi.anayasa.gov.tr/>

<https://www.coe.int/en/web/data-protection/convention108/modernised>

<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyenum=223>

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

ÖZGEÇMİŞ



TEZ ONAY SAYFASI

Üniversite : T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü : SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı : Yasin ÜSTÜN
Tez Başlığı : 6698 Sayılı Kişisel Verilerin Korunması Kanunu
Uyarınca Türk Ticaret Şirketlerinin Yükümlülükleri
Savunma Tarihi : 11/12/2023
Danışman : Prof. Dr. Mehmet ERDEM

JÜRİ ÜYELERİ:

Prof. Dr. Mehmet ERDEM	İmza
Dr. Öğretim Üyesi Sedef KOÇ TANGÜN	İmza
Doç. Dr. Mehmet Bedii KAYA	İmza

Prof. Dr. Ulun AKTURAN
Enstitü Müdürü