T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETMELERDE KİŞİSEL VERİLERİN KORUNMASINDA İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ ROLÜ: ÖZEL SEKTÖR İŞLETMELERİ ÖRNEK OLAY ÇALIŞMALARI

YÜKSEK LİSANS TEZİ

E. Kübra İNCİROĞLU

İnsan Kaynakları Yönetimi Anabilim Dalı
İnsan Kaynakları Yönetimi Programı

Tez Danışmanı: Öğr. Üyesi Dr. Ercan ÖGE

Haziran, 2019

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETMELERDE KİŞİSEL VERİLERİN KORUNMASINDA İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ ROLÜ: ÖZEL SEKTÖR İŞLETMELERİ ÖRNEK OLAY ÇALIŞMALARI

YÜKSEK LİSANS TEZİ

E. Kübra İNCİROĞLU
(Y1812.190005)

İnsan Kaynakları Yönetimi Anabilim Dalı
İnsan Kaynakları Yönetimi Programı

Tez Danışmanı: Öğr. Üyesi Dr. Ercan ÖGE

Haziran, 2019

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

YÜKSEK LİSANS TEZ ONAY FORMU

Enstitümüz İnsan Kaynakları Yönetimi Anabilim Dalı İnsan Kaynakları Yönetimi Tezli Yüksek Lisans Programı Y1812.190005 numaralı öğrencisi Emine Kübra İNCİROĞLU'nun **"İşletmelerde Kişisel Verilerin İnsan Kaynakları ve Bilgi İşlem Departmanlarının Rolü: Özel Sektör İşletmeleri Örnek Olay Çalışmaları"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 19.06.2019 tarih ve 2019/14 sayılı kararıyla oluşturulan jüri tarafından oybirliği/~~oyçokluğu~~ ile Tezli Yüksek Lisans tezi 09.07.2019 tarihinde kabul edilmiştir.

	Unvan	Adı Soyadı	Üniversite	İmza
		ASIL ÜYELER		
Danışman	Dr. Öğr. Üyesi	Ercan ÖGE	İstanbul Aydın Üniversitesi	
1. Üye	Prof. Dr.	Akın MARŞAP	İstanbul Aydın Üniversitesi	
2. Üye	Dr. Öğr. Üyesi	Erdinç GÜLBAŞ	İstanbul Esenyurt Üniversitesi	
		YEDEK ÜYELER		
1. Üye	Dr. Öğr. Üyesi	Gonca YILDIRIM	İstanbul Aydın Üniversitesi	
2. Üye	Doç. Dr.	Tuğba ALTINTAŞ	Üsküdar Üniversitesi	

ONAY

Prof. Dr. Ragıp Kutay KARACA
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİMİ

Yüksek lisans tezi olarak sunmuş olduğum "İşletmelerde Kişisel Verilerin Korunmasında İnsan Kaynakları Ve Bilgi İşlem Departmanlarının Rolü: Özel Sektör İşletmeleri Örnek Olay Çalışmaları" adlı araştırmanın, bilimsel gelenek ve ahlak kurallarına aykırı düşmeksizin yazıldığını, yararlanılan kaynakların kaynakçada yazılı olanlardan oluştuğunu, bilimsel yazım kurallarına uygun olarak kaynaklara atıf yapıldığını saygılarımla belirtir ve taahhüt ederim. (…/…/2019)

E. Kübra İNCİROĞLU

ÖNSÖZ

İşletmelerde Kişisel Verilerin Korunmasında İnsan Kaynakları ve Bilgi İşlem Departmanlarının Rolüne yönelik özel sektör işletmelerinin bu konuda yaptıkları çalışmaları örnek olay yöntemi ile inceleyerek yaptığım yüksek lisans tez çalışmam sırasında, tez çalışmasının başlangıcından tamamlanmasına kadar geçen tüm süreç içerisinde beni her zaman özveri ve sabırla destekleyen değerli tez danışmanım Öğretim Üyesi Dr. Ercan ÖGE' ye ve bu zorlu süreçlerde benden sevgisini ve yardımlarını hiçbir zaman esirgemeyen sevgili aileme en içten teşekkürlerimi sunuyorum.

Haziran, 2019 **E. Kübra İNCİROĞLU**

İnsan Kaynakları Yöneticisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

AB : Avrupa Birliği
AKT : Aktaran
ASŞ : Avrupa Sosyal Şartı
AY : Anayasa
AYM : Anayasa Mahkemesi
BM : Birleşmiş Milletler
C : Cilt
ÇSGB : Çalışma ve Sosyal Güvenlik Bakanlığı
Danıştay 10D : Danıştay Onuncu Hukuk Dairesi
DLP : Veri Kayıp Önleme
DMK : Devlet Memurları Kanunu
E : Esas
EC : Avrupa Konseyi
GBS : Küresel Konumlama Sistemi
GDPR : Avrupa Birliği Genel Veri Koruma Tüzüğü
ILO : Uluslararası Çalışma Örgütü
IP : İnternet Protokolü
İBYS : İş Sağlığı Bilgi Yönetim Sistemi
İHEB : İnsan Hakları Evrensel Beyannamesi
İSGK : İş Sağlığı ve Güvenliği Kanunu
İşK : İş Kanunu
K : Karar
KHK : Kanun Hükmünde Kararname
KVKK : Kişisel Verileri Koruma Kanunu
M : Madde
MESS : Türkiye Metal Sanayicileri Sendikası
PDKS : Personel Devam Kontrol Sistemi
RG : Resmî Gazete
S : Sayfa
SAP : Sitem Analiz ve Program Geliştirme
SSGSSK : Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
STİSK : Sendikalar ve Toplu İş Sözleşmesi Kanunu
T.C. : Türkiye Cumhuriyeti
TBD : Türkiye Bilişim Derneği
TBK : Türk Borçlar Kanunu
TCK : Türk Ceza Kanunu
TDK : Türk Dil Kurumu
THS : Temel Haklar Sözleşmesi
TÜHİS : Türk Ağır Sanayii ve Hizmet Sektörü Kamu İşverenleri Sendikası
VB : Ve benzeri
VD : Ve diğerleri
VKD : Veri Koruma Direktifi
Y.21HD : Yargıtay Yirmi birinci Hukuk Dairesi

Y.9HD **:** Yargıtay Dokuzuncu Hukuk Dairesi
YCGK **:** Yargıtay Ceza Genel Kurulu
YHGK **:** Yargıtay Hukuk Genel Kurulu

ÇİZELGE LİSTESİ

Sayfa

İŞLETMELERDE KİŞİSEL VERİLERİN KORUNMASINDA İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ ROLÜ: ÖZEL SEKTÖR İŞLETMELERİ ÖRNEK OLAY ÇALIŞMALARI

ÖZET

Kişisel veri, kişiyi belirli ya da belirlenebilir kılan bütün datalar olarak tanımlanmaktadır. Verisi işlenen kişi ister işveren ister iş gören olsun isterse o işyerinin stajyeri ya da müşterisi olsun kişisel veri sahibidir ve verileri, veri sorumlularınca korunmalıdır. İşyeriyle, iş ilişkisi içinde olan herkes bu kapsamda değerlendirilmelidir. İşyerlerinde kişisel veriler ağırlıklı olarak insan kaynakları ve bilgi işlem departmanlarınca işlenmektedir. Çünkü işyerinde, işe alım, işin devamı ve işin sonlanması süreçlerinin yönetimi ve özlük dosyalarının tutulması, performans sisteminin kurulması ve yönetilmesi, iş uyuşmazlıklarının çözümü, işyerinde izin, disiplin, İSG gibi kurulların sağlıklı bir şekilde işletilmesi insan kaynakları departmanın görevleri arasında iken, elektronik ortama aktarılan bu verilerin güvenli bir şekilde saklanması, yedeklenmesi, dış ataklara karşı gerekli teknik tedbirlerinin alınması görevi de bilgi işlem departmanına aittir. İnsan kaynakları ve bilgi işlem görevlileri bir nevi kişilerin o işletmedeki sırdaşı konumundadırlar ve sır saklama yükümlülüğü altındadırlar. Kişilere ait olan kimlik, iletişim, imza, görsel ve işitsel, adres, finans, aile ve yakınlık, sağlık, eğitim, güvenlik ve biyometrik verilerine sahip olmaktadırlar. Kişisel verilerin hukuka uygun olarak işlenmesi ve güvenliğinin sağlanması konusunda veri sorumlusu ile birlikte sorumludurlar. Kamu-özel ayrımı olmaksızın ve sektör farkı gözetilmeksizin kişisel veri işlenen tüm işyerleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda öngörülen yükümlülükleri yerine getirmek zorundadır.

Bu çalışmada da, insan kaynakları ve bilgi işlem departmanlarının işletmelerde kişisel verilerin korunmasındaki rolleri, nasıl önlemler alabileceği ve konunun neresinde oldukları ayrıntılı bir şekilde incelenmiştir. Çalışmada kişisel verilerin mevzuata uygun biçimde saklanması ve korunması noktasında işletmelerde insan kaynakları ve bilgi işlem departmanlarının rolleri, nasıl önlemler alabileceği ve konunun neresinde olduklarının ortaya konulması amacıyla örnek olay yöntemi kullanılmıştır. Bu haliyle çalışma, nitel bir araştırma özelliği taşımaktadır. Bu araştırmada hipotez sunulmaması nedeniyle hipotezlerin testi söz konusu olmadığı gibi, nitel ve tümevarım yöntemi ile yapılan değerlendirmeler bu çalışmanın doğası gereğidir

Anahtar Kelimeler: *Kişisel Verileri Koruma Kanunu, İnsan Kaynakları Departmanı, Bilgi İşlem Departmanı*

THE ROLE OF HUMAN RESOURCES AND INFORMATION TECHNOLOGIES DEPARTMENTS FOR THE PERSONAL DATA PROTECTION: CASE STUDY SAMPLES IN PRIVATE SECTOR BUSİNESS

ABSTRACT

Personal data is defined as the all data which renders the person particular or determinable. The person, whose personal data is processed, can be employer, employee, intern or customer. All these parties have personal data which has to be protected by data responsible. All parties who have business relations with the work place have to be considered in this scope. The personal data are mainly processed by human resources or information Technologies departments of the companies. Because the management of employment and de-employment processes, keeping personnel files, setting up a performance system, solving work incompatibilities and the administration of permission, discipline rules, health and safety councils are the responsibilities of human resources department in a company. Also, the protection and back up of personal data which are converted to electronic environment and taking technical precautions for the cyber-attacks are the responsibilities of information Technologies (IT) departments. In another meaning, the responsible employees in human resources and IT departments are the confidants of the employees and they are obliged to keep the secrets of the employees. The responsible have the identification, contact, signature, visual and audial, address, financial, family, health, education, security and biometric data of the employees. The responsible departments are obliged with the data owner to process the data in line with law and maintain the security of the data. Without any public-private entity or sector based differentiation, whole work places which process personal data have to fulfill their liabilities which are defined in Personal Data Protection Law, 6698.

In this study, the roles of human resources and IT departments for the personal data protection, the precautions to be taken and their positions regarding to the topic have been detailly analysed. The case methodology has been applied in order to reveal the responsibilities of human resources and IT departments for saving and protecting of personal data due to the law. This is a qualitative study with the regarding structure. There are no presented hypothesises in this study. Therefore, the test of hypothesises is not a subject of this study, also the evaluations which are made via qualitative and induction methodologies are to be considered the nature of this study.

Keywords: *Personal Data Protection, Human Resource Department, Technologies (IT) Department*

1. GİRİŞ

1.1 Tezin Konusu

Teknolojinin hızla gelişmesi ve internetin yaygın bir biçimde kullanılmaya başlanmasıyla birlikte kişisel verilerin güvenliğinin sağlanması büyük önem kazanmıştır. Çünkü ekonomik ve sosyal hayata ilişkin birçok konudaki iş ve işlemler elektronik ortamda yapılmaktadır. Hemen her alanda hizmetlerin sunulması aşamasında hizmet alanların kişisel verilerine başvurulmakta ve elde edilen veriler başkalarıyla da paylaşılabilmektedir. Genel hatları ile bakıldığında "mahremiyet" kelimesinin bir karşılığı olan kişisel verilerin 1980'li yıllardan bugüne uluslararası ve ulusal mevzuatlarca korunmaya çalışıldığı bilinmektedir.

Bugün, kişiler yaptıkları hemen her faaliyette kişisel verilerini kullanmak ya da bunların işlenmesine izin vermek durumunda kalmaktadırlar. Ancak kişisel verilerin bu kadar sık kullanılması ve özellikle kolay paylaşılır hale gelmesi çeşitli sorunları da beraberinde getirmektedir. Kişisel verilerin gerçek kişiler için anonim hale gelmesi, bireyin sosyal yaşamını etkileyebileceği gibi dolandırılması ya da izlenebilmesini de mümkün hale getirmektedir. Tüzel kişilerin kişisel verilerinin kullanılması, ticari zorluklara, rekabet ortamında dezavantaja, yatırımcı ve ortaklar ile problemler yaşanmasına neden olabilmektedir.

Kişisel veriler, kişinin kolaylıkla tespit edilmesine neden olabilen her türlü veriyi içerdiğinden kişisel veri kavramı sebebiyle yaşanılacak avantaj ve dezavantajların skalası da oldukça geniştir. Kişisel veriler, Avrupa ülkeleri, Amerika Birleşik Devletleri ve özellikle de son dönemde Türkiye'de oldukça önem kazanan bir konu haline gelmiştir.

7 Nisan 2016 tarihinde Resmi Gazete 'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununun 3 üncü maddesine göre kişisel veriler; kimliği belirlenebilir ya da belirli olan gerçek kişilerle ilişkili bilgiler olarak tanımlanmaktadır. Kişisel veriye örnek olarak bireyin adı, soyadı, doğum tarihi, doğum yeri gibi kişinin kim olduğunu anlamaya yarayan bilgiler olabileceği gibi kişinin ailevi, fiziki,

ekonomik, sosyal ve benzeri özellikleri de kişisel veri kapsamındadır. Gerçek kişilerin açık rızaları olmadan, kendilerine ait verilerin işlenmesi imkansızdır. Kişinin kendisi ile ilişkili verilerin işlenmesine açık rıza göstermesi temel şarttır.

İşletmeler açısından bakıldığında ise verilerin hangi biçimlerde güvenli bir şekilde saklanacağı ya da korunacağı konuları da gizlilik kadar önemlidir. Kişisel verilerin korunması noktasında ise bu çalışmanın eğileceği temel konu ise işletmelerde kişisel verilerin korunması hususunda "İnsan Kaynakları ve Bilgi İşlem Departmanlarının" uygulamaları ve etkilerinin ortaya konulmasıdır. Çalışmada, işe alım sürecinden başlamak üzere, işin devamı süresinde ve işin bitiminde ve akabinde kişisel verilerin hangi ilkeler doğrultusunda işleneceği, nasıl güvenli bir şekilde saklanacağı, saklama sürelerinin hangi kriterlere göre belirleneceği ve saklama süresi dolan verilerin nasıl silineceği, yok edileceği ya da anonim hale getirileceği konularında alınması gereken idari ve teknik tedbirlerin işletmelerin insan kaynakları ve bilgi işlem departmanlarınca nasıl yönetileceği hususları örnek olay çalışmaları ile ortaya konulmuştur. Günümüzde geçerliliğini ve önemini sürekli biçimde artıran kişisel veri ve veri güvenliği konuları işletmelerde de oldukça önemli bir konudur ve ilgili mevzuat ile sınırlandırılmıştır.

1.2 Tezin Amacı

Kişisel verilerin hukuka uygun olarak korunamaması hem yasal açıdan hem de etik değerler bağlamında pek çok sakıncayı beraberinde getirmektedir. Gizliliğin kaybolması, verilerin farklı amaçlarla kullanımı, verilerin değiştirilerek kullanılması ya da kötü niyetle kişisel verilerden istifade edilmesi gibi hususlar kişisel verilerin korunması noktasında karşılaşılan önemli sorunlardan birkaçı olarak bilinmektedir. Bu doğrultuda hem kişisel verilerin güvenliğinin ve gizliliğinin sağlanması, hem de korunması adına işletmelerde atılan adımlar oldukça önemli zorunluluk haline gelmiştir. Bu doğrultuda bu araştırmanın amacı işletmelerde işlenen kişisel verilerin güvenli bir şekilde korunması ve gizliliğinin sağlanması noktasında "İnsan Kaynakları ve Bilgi İşlem Departmanlarının" uygulamalarının ve bu uygulamaların etkilerinin ortaya konulmasıdır. İşverenler istihdam ettikleri çalışanları başta olmak üzere çalışan adayları, stajyerleri, tedarikçileri, alt işveren ve alt işveren çalışanları, müşterileri ile ziyaretçilerinin verilerini işlemektedir. İşlenen kişisel veriler başta kimlik bilgisi olmak üzere, özlük, finans, adres, iletişim, sağlık, biyometrik, yakınlık bilgisi gibi

verileri işlemekte ve bu verilerin korunması, güvenle saklanması ve gizliliğinin sağlanması konusunda özellikle insan kaynakları ve bilgi işlem departmanlarına büyük görevler düşmektedir. Çünkü işyerlerinde ağırlık olarak veri işleme bu iki birim üzerinde yoğunlaşmaktadır. Alınacak idari ve teknik tedbirlerin yasal mevzuat çerçevesinde bu birimlerce yerine getirilmesi gerekmektedir. Bu araştırma, insan kaynakları ve bilgi işlem departmanlarının bugün ve gelecekte bu konu üzerine getirdiği önlem ve faaliyetleri ortaya koyarak gelecekteki çalışmalara ve sektörlere ışık tutmayı amaçlamaktadır.

Bu amaçla, çalışma giriş bölümü dahil beş bölümden oluşmaktadır. Giriş başlığı altında bölümde tezin konusu ve amacı hakkında bilgiler verilmiştir. İkinci bölümde kişisel veri kavramı, veri güvenliği, kişisel veri türleri ve korunmaması durumundaki sakıncalar ile birlikte Türkiye ve Dünya'daki mevzuatın ortaya konulması ile ilgili konular yer almaktadır.. Üçüncü bölümde ise insan kaynakları ve bilgi işlem departmanlarının işletmelerde kişisel verilerin korunması noktası ne tür uygulamalar ortaya koyduğu incelenmiştir. Bu doğrultuda bilgi işlem departmanının, bilgisayar sistemlerinde oluşturduğu veri bankaları, gözetim sağlayacak teknolojilerin entegre edilmesi ve kişisel verilerin korunmasında diğer uygulamaları, insan kaynakları departmanının ise yine veri güvenliği noktasındaki ilkeleri ve sürece dair kattığı unsurlar bu bölüm içerisinde yer almaktadır. Araştırmanın dördüncü bölümünde ise iki farklı sektörden seçilen işletmelere ilişkin örnek olay incelemesi yapılmıştır. Tezin son bölümünde ise tez konusuna ilişkin yapılan örnek olay çalışmaları sonucunda elde edilen bilgiler değerlendirilmiş ve çeşitli öneriler ile çalışma tamamlanmıştır.

1.3 Literatür Araştırması

Çalışmada ağırlıklı olarak bu konuyla ilgili hazırlanmış tez, makale, kitap bölümü ve kitaplardan, işletmelerin web sayfası, resmi gazete ve bu konuda çıkan kanun maddelerinden yararlanılarak literatür taraması yapılmıştır Araştırmada yöntem olarak örnek olay uygulama çalışması kullanılmış, bu kapsamda iki sektörde iki farklı işletme incenmiş, literatür taraması ve görüşme yoluyla elde edilen veriler nitel bir araştırmaya tabi tutulmuştur.

2. KİŞİSEL VERİLERİN KORUNMASI ÜZERİNE AÇIKLAMALAR

2.1 Veri ve Bilgi Güvenliği

Latincede "verilen şey" anlamına gelmekte olan veri, İngilizcede ise "data" olarak adlandırılmaktadır. Türkçede ise Latince'deki gerçek ifadesine uygun bir şekilde kullanılmaktadır (Canbek ve Sağıroğlu, 2006:166). Bilgi, enformasyon ve birçok kaynakta veri kavramına yer verilmektedir. Bu kavram söz konusu kaynaklarda farklı anlamlar taşısa dahi benzer anlamlarda kullanılmaktadır. Enformasyon ve bilgi kaynaklarında veri kavramı ham madde anlamına gelen ve tek başına kullanıldığında çok fazla anlam taşımayan bir niteliğe sahiptir (Yılmaz, 2009:98).

Veri kavramı sözlükte ise; araştırmaların, değerlendirmelerin ve tartışmaların temel unsuru, muta; sonuçları gözlemlere ve deneysel çalışmalara dayanan bulgular; kavramların ya da komutların, iletişim, yorum ve işlem süreçlerinde kullanılabilmesi adına geliştirilen gösterimler olarak ifade edilmektedir (TDK, 2019). Veri kavramı enformasyon ve bilginin temelinde yer almaktadır. Bu kavramın tek başına kullanımının bir anlamı olmasa dahi belirli bir amaç doğrultusunda işlevsel bir hale getirilebilmektedir.

Birçok yönden veri güvenliğinin sağlanması önemli bir yere sahiptir. Bu doğrultuda öncelikle kuruluşların malvarlıklarının korunması olarak veri güvenliğinden bahsetmek yerinde olacaktır. Veri güvenliğinin sağlanması ile ilk olarak kuruluşların malvarlıklarının korunması hedeflenmektedir (Canavan, 2001:1-21). Burada malvarlığı ile yalnızca kuruluşa ait mali bilgiler kastedilmemektedir. Kuruluşlara ait donanımlarında ve yazılımların saklanmakta olan tüm bilgiler malvarlığı kapsamında değerlendirilmektedir (Canavan, 2001:1-21).

Veri güvenliğinin sağlanması ile amaçlanan bir diğer konu ise kuruluşların rekabet avantajları elde edebilmesidir. Bu durum özellikle ticaret ve finans alanında faaliyetlerini sürdürmekte olan kuruluşlar için çok daha önemlidir. Veri güvenliği bir kuruluş içerisinde ne kadar geliştirilmişse, tüketiciler tarafından söz konusu kuruluşlar o denli güvenilir olarak değerlendirilmektedir (Canavan, 2001:1-21). Söz konusu

güvenliğin sağlanmasına yönelik olarak ortaya çıkmış kurallar, mevzuatlar ve yasal düzenlemeler bulunmaktadır. Bu duruma bağlı olarak yasal çerçeveler içerisinde varlıklarını sürdürmek isteyen kuruluşların kendi bünyelerinde bilgi güvenliğini sağlaması gerekmektedir (Canavan, 2001:1-21).

Birçok kuruluşun bünyesine saklanmış olan kişisel veriler bulunmaktadır. Bireylere ait özel bilgilerin silinmesi, ele geçirilmesi ya da değiştirilmesi neticesinde olumsuz sonuçlar doğurabilecek durumlar ortaya çıkmaktadır. Ayrıca bir ülkede veri güvenliğinin gelişmiş olması ile refah düzeyinin yüksek olması arasında pozitif bir ilişkinin var olduğu düşünülmektedir.

Kişilere ait verilere yetki sınırlarını aşan kişiler tarafından ulaşılmasının engellenmesi ve söz konusu bilgilerin korunması gizlilik kavramı ile sağlanmaktadır. Kuruluşların sistemlerinde yer alan veriler kişilerin sağlık durumları, felsefi görüşleri, sendika üyelikleri, kimlik bilgileri, adres ve iletişim bilgileri, kredi kartı bilgileri vb. bilgiler olabilmektedir. Kişisel verilerin korunması kadar kurumlara ait verilerin de kullanılması da oldukça önemlidir. Kişisel ya da kurumsal veriler, kasıtlı bir şekilde de ele geçirilebilmektedir. Ancak belirli bir kasıt olmadan dahi çeşitli tedbirsizlikler ve dikkatsizlikler neticesinde yetki sınırı dışında kalan insanlara veri aktarımı yapılabilmektedir (Cole vd., 2005:4-6).

Verilerin korunmasına yönelik geliştirilen güvenlik süreçleri içerisinde üç unsur karşımıza çıkmaktadır. Bunlar; önleme (prevention), tespit (dedection) ve müdahale (response) olarak sıralanmaktadır (Canavan, 2001:1-21). Bilgi güvenliğinin sağlanması açısında güvenlik açıklarının, sistem içerisinde oluşan açıkların, yönetim zaaflarının engellenmesi son derece önemlidir. Saldırı önleme amacı ile birtakım tedbir çalışmalarının yapılmasına karşılık, saldırıların tamamen engellenmesi kimi zaman sağlanamamaktadır. Bu nedenle saldırıların engellenmesi amacı ile yapılan çalışmalar kadar, verilerin tümüne yönelik saldırıların gerçekleşmesi durumunda tespitin sağlanması ve gerekli müdahalelerin yapılması gerekmektedir (Canavan, 2001:1-21).

Bütünlük, genel itibariyle bilgilerin bütününe zarar gelmeksizin doğruluklarının korunmasıdır. Bütünlük, bilgi sistemlerinden beklenen hizmetlerin beklendiği gibi olması ve bilgi sisteminde saklanan verilerin bozulmadan muhafaza edilebilmesi olarak da tanımlanabilir (Adalı, 2016:29-37).

Bütünsel bir ifade ile ortaya çıkan amaçlar üç bölümde değerlendirilmektedir. Bunlar arasında ilk sırada, yetki sınırları dışında kalan kullanıcılar tarafından bilgi değişimlerinin gerçekleştirilmesinin önüne geçmek yer almaktadır (Cole vd., 2005:4-6). Zira yetkisi olmadan bir kullanıcı, sisteme sızarak bilgileri değiştirmek isteyebilmektedir. Bu durum önemli bir güvenlik ihlalini meydana getirmektedir ve bilgi bütünlüğünün sağlanması için öncelik bilgilerin değiştirilmesini engellemek olmalıdır.

Amaçların ikinci sırasında ise, yetki sınırları içerisinde olan kişilerin sistem içerisinde bilgileri değiştirmesinin engellenmesi ve yetki sınırları dışında kalan kişilerin bilgilere ulaşmasını engellemek yer almaktadır (Cole vd., 2005:4-6). Kurum içerisinde yetkisi olmasına karşılık kişiler tarafından kasıtlı ya da kasıt olmadan bilgiler değiştirilebilmektedir. Burada sistem içerisinde geliştirilen değişimleri engelleyecek programların kullanılması önemlidir. Bilgi değişikliğinin yapılacağı zaman sistemde uyarı mekanizmasının çalışması ve kolay bir değişime izin vermemesi veri kayıplarının önüne geçebilmek için yararlı olmaktadır.

Bütünlüğün sağlanmasına yönelik olarak ortaya çıkan son amaç ise, iç ve dış istikrarın sağlanmasıdır (Cole vd., 2005:4-6). Verilerin ve bilgilerin bulunduğu sistemlerin istikrarı, iç istikrar olarak adlandırılmaktadır. Örnek vermek gerekirse, kurum içerisindeki yetkili bir kişinin bilgisayarında veriler korunaklı bir durumda ise, saldırılara maruz kalmıyorsa ya da saldırıların olmasına karşılık verilerin korunması sağlanabiliyorsa iç istikrarın varlığından bahsetmek mümkün olmaktadır.

Kişilerin ya da kurumların bilgi güvenliğinin sağlanabilmesi adına farklı bir işletmeden destek hizmetleri almakta ise, bu işletmelerin veritabanlarında yer alan bilgiler ile gerçek bilgiler arasında uyumun olması durumu ise dış istikrar olarak adlandırılmaktadır (Cole vd., 2005:4-6).

Yetkili kişiler tarafından bilgilere istenildiği zaman, kesintilere maruz kalmadan ulaşabilmesi erişebilirlik olarak açıklanmaktadır. Bilgi sistemleri içerisinde erişebilirlik donanım, bilgisayar ağı ve alınan hizmetler üzerinden değerlendirilmektedir (Adalı, 2016:29-37). Sistem güvenliklerinin devrede olması ve istikrarlı bir işleyişin ortaya çıkması önem arz etmektedir. Zira birçok siber saldırı ardından erişebilirlik noktasında sorunlarla karşılaşılmaktadır. Örneğin, hackerlar tarafından bireylerin yetkili oldukları bilgisayarları kontrol altına alınabilmekte ve bu

kişiler gerek duyduklarında bilgiye erişim sorunları yaşamaktadır. Bu durum ile çoğu zaman Dağıtık Hizmet Engelleme saldırılarında karşılaşılmaktadır. Çünkü bu saldırıların temel amacı erişimin engellenmesidir. En sık olarak karşılaşılan saldırıların başında bunlar gelmektedir. Veri saklama sistemlerinde ortaya çıkan açıklardan yararlanmak suretiyle gerçekleşen bu saldırılarda, yetkisiz kişilerin sisteme müdahale etmesi sonrasında erişebilirliğin engellenmesine yönelik saldırılar gerçekleşmektedir. Bu nedenle sistemlerin düzenli olarak güncellenmesi ve yetkisiz kişiler tarafından kullanılmasının önüne geçilmesi gerekmektedir.

Bilgi güvenliğinin diğer önemli bileşenleri arasında ise izlenebilirlik, inkar edilemezlik ve güvenirlilik kavramları yer almaktadır. Bilgi sistemleri içerisinde yapılan işlemlerin kimin tarafından, ne zaman yapıldığının izlenebilmesi ve yapılan işlemlerin kayıt altına alınması izlenebilirlik olarak ifade edilmektedir. Sisteme yönelik ortaya çıkması muhtemel saldırıların önüne geçilmesi, hatalı işlemlerin tespit edilmesi ya da saldırı sonrasında tespit çalışmalarının yapılması izlenebilirlik neticesinde gerçekleşmektedir. Özellikle kullanıcı sayılarının fazla olduğu sistemler içerisinde ise kişiler tarafından gerçekleştirilen işlemlerin izlenmesi suretiyle ispatlanması ise inkar edilemezlik kavramı ile açıklanmaktadır. Özellikle internet üzerinden gerçekleştirilen bireysel bankacılık işlemlerinde bireylerin yaptıkları işlemleri inkar edememesi açısından bu kavram önem arz etmektedir (Adalı, 2016:29-37).

Veri saklama işlemlerinin gerçekleştirildiği tüm donanımsal, yazılımsal vb. sistemlere yönelik olarak geliştirilen kuvvetli koruma programları kullanılması ile güvenilirlik kavramı ortaya çıkmaktadır (Adalı, 2016:29-37). Güvenilirliğin sağlanması için sistemlerin düzenli olarak güncellenmesi, ihtiyaç duyulan periyodik bakımların yapılması ve güvenlik derecesi yüksek yöntemlerin tercih edilmesi gerekmektedir. İfade edilen teknik güvenlik kavramlarının haricinde fiziksel olarak da güvenliğin sağlanması önem arz etmektedir. Bu doğrultuda bilgilerin saklandığı donanımlara yetkisiz kişilerin engellenmesi ve yaşanabilecek doğal afetlere karşı fiziksel korumanın sağlanması gerekmektedir (Slay ve Koronios, 2006:130-150). Yangın, fırtına, deprem, volkanik patlama vb. doğal afetler neticesinde verilerin saklandığı sistemlerin muhafaza edilmesi bilgi güvenliği açısından oldukça önemlidir (Slay ve Koronios, 2006:130-150).

2.2 Kişisel Veri Kavramı

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3'üncü maddesi kapsamında kişisel veri; "kimliği belirli ya da belirlenmesi mümkün gerçek kişilere ait her türlü bilgi" olarak ifade edilmiştir (7.4.2016-RG/29677). 6698 sayılı Kanunun gerekçesinde ise kişisel veri kavramına örnek olarak; kişilerin adı, soyadı, doğum yeri ve tarihi, kişilerin ailesine, fiziki durumuna, ekonomik ve sosyal durumuna ait bilgiler gösterilmiştir (6698 sayılı Kişisel Verilerin Korunması Kanunu m.3). Elde edilen bir veri neticesinde kişinin kim olduğunun anlaşılması mümkün hale geliyorsa kişisel veri olarak kabul edilmektedir. Tanım içerisinde yer verilen belirlenebilir ifadesi ile ne anlatılmak istendiği ise kanun gerekçesinde örneklerle ile açıklanmıştır. Bu doğrultuda;

> "*Verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir*." (6698 sayılı Kişisel Verilerin Korunması Kanunu Gerekçesi m.3).

Kişisel veri kavramı ile ilgili olarak yapılan tanımdan yola çıkarak, bir verinin kişisel veri olarak kabul edilmesi için iki unsur bulunmaktadır. Bunlar; söz konusu verinin gerçek bir kişiye ait olması ve bu veri doğrultusunda kişinin belirlenebilir olmasıdır. İlgili kanun gerekçesinde de yer aldığı üzere, bireylerin kişisel, fiziksel, ailevi ve mesleki özelliklerini belirten ve bilgiler ışığında bireylerin diğer insanlardan ayrılmasına yol açan tüm veriler kişisel veri olarak kabul edilmektedir (6698 sayılı Kişisel Verilerin Korunması Kanunu, m.3). Söz konusu veriler kişilerin felsefi görüşlerini, kökenini, sağlık durumunu, cinsel tercihlerini, iletişim bilgilerini, sosyal güvenlik bilgilerini, pasaport bilgilerini, üye olduğu dernek ve sendikaları ve banka bilgilerini de içerebilmektedir (Kişisel Verileri Koruma Kanunu Gerekçesi m.6).

Kanunda yer alan kişisel veri kavramı ile ilgili tanıma bakıldığında kapsamının geniş olduğu görülmektedir. Bir başka ifade ile kişisel veri kavramının içeriğinde hangi unsurların yer aldığı kanun kapsamında yapılan tanım içerisinde tahdidi olarak sayılmamıştır. Bir verinin tanım doğrultusunda değerlendirilmesi neticesinde kişisel veri olup olmadığına karar verilmektedir.

Elektronik haberleşme sektörü içerisinde kişisel verilerin işlenmesi, saklanması ve korunması amacı ile "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelikte" birtakım düzenlemeler yapılmıştır. Söz konusu yönetmelik doğrultusunda; belirli ya da kimliğinin belirlenmesi mümkün olan gerçek ve tüzel kişilere ilişkin tüm bilgiler, kişisel veri olarak kabul edilmektedir (Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, 24/7/2012; RG/28363).

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Yönetmelik arasındaki fark ise Yönetmelikte kanun dışında tüzel kişilere de tanım içerisinde yer verilmesidir. Buradan hareketle düzenlenen yönetmelik doğrultusunda tüzel kişilere ait bilgiler de kişisel veri kapsamında değerlendirilmektedir.

AB ülkeleri adına kişisel verilerin işlenmesine yönelik olarak düzenlenmiş olan Kişisel Veri Koruma Tüzüğü (GDPR) ile KVKK'da yer alan tanımlar arasında paralellik söz konusudur. Bu nedenle kişisel veri olarak, Elektronik Haberleşme Sektörü'ne yönelik olarak hazırlanan yönetmeliğin aksine, KVKK ve GDPR'de yer alan açıklama kabul edilmektedir.

Türkiye'de kişisel verilerin korunması hukukunda temel düzenleme olarak kabul edilen KVKK'nın amacı, kapsamı ve hükümleriyle birlikte değerlendirildiğinde Direktif ile büyük ölçüde paralellik taşımaktadır. Bununla birlikte, KVKK'nın Resmi Gazete'de yayımlanmasından kısa bir süre sonra AB Veri Koruma Reformu kapsamında hazırlanan Kişisel Veri Koruma Tüzüğü (GDPR), Avrupa Parlamentosu tarafından onaylanarak kabul edilmiştir. Söz konusu GDPR ile Direktif'te yer alan hükümlerin modernize edilmesi ve güncellenmesi amaçlanmıştır. Bu çerçevede, KVKK'nın kurgulanmasında GDPR hükümleri değil, o dönemde yürürlükte bulunan Direktif hükümlerinin esas alındığı görülmektedir. Ne var ki, ikincil mevzuat ve Kurul kararlarına bakıldığında, uygulamanın GDPR ile eş düzleme çekildiği de söylenebilecektir.

2.3 Kişisel Veri Türleri

2.3.1 Hassas (özel nitelikli) kişisel veriler

Şahin (2011:80-81), 1995/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi m. 33'te; "verinin asıl sahibinin açık bir şekilde rıza göstermemesi durumunda, kişilerin temel özgürlükleri ya da kişisel mahremiyetinin ihlal edebilme riskini taşıyan verilerin işlenmemesi gerekmektedir" (Lloyd, 2017:169), ifadesi ile hassas kişisel veriler, temel hakları ve özel hayatın gizliliğini ihlal edebilecek nitelikteki veriler olarak ifade edilmiştir (https://ec.europa.eu/info/policies/ justice-and-fundamental-rights_en, Erişim Tarihi: 08.02.2019). Benzer bir yaklaşım AB Veri Koruma Direktifi m. 51'de de görülmektedir. Burada da hassas verilerin daha özel bir koruma sistemi ile muhafaza edilmesi gerektiğinin altı çizilmiştir.

1995/46 EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi m. 8/1'de ise; üye olan devletlerin, kişilerin sağlık durumları, cinsel yaşamları, sendika üyelikleri, dini tercihleri, felsefi görüşleri, siyasi fikirleri, etnik kökenleri ile ilgili verilerin işlenmesinin yasaklanacağı ifade edilerek, hassas kişisel verilere ait tanım içeriğinde yer alan unsurlar üzerinden yapılmıştır. AB Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi m. 9'da da hassas kişisel veriler kapsamına genetik ve sahibinin belirlenebilmesini sağlayan biyometrik veriler de eklenmiştir. AB Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi m. 10'da tüm bunlara ek olarak konu ile ilgili olarak alınması gereken tedbirlerle ilgili de düzenlemeler yapılmıştır. Bu doğrultuda doğrudan ya da dolaylı bir şekilde bireylerin ırkları, etnik kökenler, ten renkleri, siyasi yönelimler, din ve felsefe ile ilgili inançları, sendika üyelikleri, sağlık durumları, cinsel hayatları, bağımlılıkları, almış oldukları mahkumiyetler, genetik ve biyometrik veriler hassas veri olarak kabul edilmektedir ve bunların işlenmesi yasaktır (Lloyd, 2017:170).

Bu kavram bazı ülkelerde farklı isimlerle de kullanılmaktadır. Bunlardan; Hollanda özel kişisel veri kavramını kullanmayı tercih etmekte iken, İngiltere, İsveç ve Yunanistan'da 108 numaralı sözleşme kapsamında özellikli veri kategorileri olarak kullanılmaktadır. Türkiye'de hazırlanmış olan KVKK doğrultusunda ise özel nitelikli kişisel veriler ifadesi hassas kişisel veriler için tercih edilmektedir. Bu konunun

değerlendirilmesi aşamasında mukayeseli hukukta tercih edilmesinden dolayı hassas kişisel veriler kavramı kullanılmaktadır.

Yukarıda yer verilen tanımlarda da görüldüğü gibi hassas kişisel veriler; kapsamında temel hak ve hürriyetlerin yer aldığı konuların yer alması nedeni ile daha özel bir korumaya gereksinim duyulmaktadır (Şahin, 2011:82). Bu nedenle 1995/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi ve Avrupa Konseyi'nin Ocak 1981 tarih ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmesi m.6 kapsamında özel koruma altındadır. Hassas kişisel veriler, AB Kişisel Verilerin İşlenmesi Ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi m. 9'da da düzenlenmiş ve söz konusu madde 1995/EC VKD m. 8'i temel almıştır.

1995/46/EC VKD m. 8/1'de ise içeriğinde ırka, etnik kökene, düşünce özgürlüğüne ve genel sağlık durumuna ilişkin veriler, hassas kişisel veriler grubu içerisinde değerlendirilmektedir. 1995/46/EC VKD'de hassas kişisel veriler tahditli bir ifade ile aktarılmakla birlikte m. 8/5'te "üye olan devletler, hukuk davalarında alınmış olan kararlar ya da idari müeyyidelere dair verilerin de resmi makamların kontrolü altında işlenmesi sağlanabilmektedir" ifadesi ile hassas kişisel verilen korunmasına yönelik bir düzenleme gerçekleştirilmiştir (Lloyd, 2017:787). AB VKD m. 9'da ise hassas kişisel verilerin sayılması sırasında biyometrik ve genetik verilerden söz edilmiş, bireylerin almış oldukları mahkumiyetler ve güvenlik tedbirleri ile ilgili olarak verilerden m. 10'da ayrı olarak söz edilmiş ve yetkili mercilerin kontrolü altında olmak şartı ile veriler her kime ait ise bu kimselerin temel hak ve özgürlüklerinin ihlal edilmemesine dikkat edilerek verilerin işlenebileceği belirtilmiştir. 108 nolu Sözleşme m. 6'da ise, kişilerin ırkı, siyasi görüşü, dini tercihi, inançları, sağlık durumları, cinsel hayatları ve mahkumiyetleri ile ilgili veriler hassas kişisel veriler olarak değerlendirilmiştir.

Mukayeseli hukuk alanında yukarıda ifade edilenlere benzer niteliklere sahip olan veriler hassas kişisel veriler olarak değerlendirilmektedir. Fakat konu ile ilgili olarak farklı yaklaşımlarda ortaya çıkmaktadır. Örnek vermek gerekirse Polonya, İzlanda, Estonya ve Bulgaristan'da genetik bilgiler hassas veri olarak kabul edilmektedir. Slovenya, Slovakya, Çekya'da biyometrik bilgiler hassas veri olarak değerlendirilmekte iken, İtalya'da kişilerin dernek üyelikleri bu sınıf içerisinde yer

almaktadır. Finlandiya'da kişilerin sosyal refah gereksinimler, kişilerin yaralanmaları ve almış oldukları destekler hassas veri kapsamında yer almakta, Danimarka, Finlandiya, Yunanistan, Hollanda, Portekiz ve Fransa'da ise kişilere ait mali veriler kişisel veri olarak kabul edilmektedir. İngiltere'de ise farkı olarak kişilerin işlemiş oldukları suçlar gibi işledikleri iddia edilen suçlar ve bu suçlara yönelik olarak gerçekleşen kovuşturma süreçleri ve akabinde alınan kararlar hassas kişisel veriler olarak kabul edilmektedir (Jay, 2007:786; https://ec.europa.eu/info/policies/justice-and-fundamental-rights_en, Erişim Tarihi: 09.02.2019).

6698 sayılı KVKK m. 6'da ise; bireylere ait olan etnik köken, siyasi eğilimler, felsefi düşünceler, dini tercihleri, giyim tarzları, üye oldukları dernek ya da vakıflar, biyometrik ve genetik verileri, genel sağlık durumları, cinsel yaşamları, almış oldukları cezalar ve mahkumiyetler özel nitelikli kişisel veri olarak adlandırılmaktadır. Bireylerin etnik kökenlerinin ve ırksal bilgilerinin hassas veriler kapsamında değerlendirilmesinin temel nedeni, yakın geçmişte yaşanan ırkçı saldırılar ve bu sorunların zaman zaman ortaya çıkmaya devam etmesi neticesinde meydana gelen tepkilerdir (Şahin, 2011:81-82). Benzer bir şekilde birtakım gerilimlerin önüne geçebilmek adına bireylerin düşüncelerinin, dini tercihlerinin, siyasi yönelimlerinin de özel bir korumaya alınmasına gereksinim duyulmuştur (Jay, 2007:790). Zira söz konusu verilerin korunamaması durumunda veri sahipleri birtakım olumsuzluklarla karşılaşabilmektedir. Kanun kapsamında yer almakta olan sağlık durumunun içeriğinde ise birçok ülkede farklı unsurlar dahil edilmektedir. Örnek vermek gerekirse; Estonya'da bireylerin özür durumları, Polonya'da bağımlılıkları, İzlanda'da bireylerin ilaç kullanımları bu grup içerisinde değerlendirilmektedir (Özdemir, 2009:64).

Hassas kişisel verilere örnek olarak ise; işveren tarafından iş görenin sendika bilgilerine dair yapmış olduğu kayıtlar, dini inancı doğrultusunda uçak yolculuğunda yemek tercihi yapan yolcunun tercih kaydı, bireyin hastanede hangi ameliyatı olduğuna dair oluşturulan kayıt, kişilerin daha önceki bağımlılıkları gösterilebilmektedir (Özdemir, 2009:55). Kimi durumlarda verilerin hassas kişisel veriler içerisinde yer alıp almadığı ise rahatlıkla belirlenememektedir. Bu duruma örnek olarak politik bir yönü ve tarafı olduğu düşünülen bir derginin üyelerinin isimlerini internet sitesinde paylaşması siyasi görüşler üzerinde kişisel verilerin korunmasının ihlal edildiğini gösterebilmektedir.

1995/46/EC VKD m. 8 doğrultusunda hassas verilerin işlenmesi yasaklanmıştır. Bu durum benzer bir şekilde AB VKD'de ve birçok ulusal koruma kanununda da yer almaktadır. Hassas kişisel veriler sadece birtakım ufak istisnaların geçerli olması durumunda işlenebilmektedir.

1995/46/EC VKD, kimi durumlarda hassas verilerin işlenmesine müsaade etmektedir. Ancak unutulmaması gereken ana konu, işlenmesine istisnai şekilde müsaade edilen kişisel verilerin özel koruma altında kalmaya devam etmesi gerektiğidir. Ancak özel korumaya dair m. 8'de ifade edilen özel koruma hususları göz ardı edilmek zorunda kalmaktadır (Özdemir, 2009:58). Örnek vermek gerekirse, verinin sahibinin açık bir şekilde rızası 1995/46/EC VKD'nin koruma unsurları ile uygun olma gereksiniminin ortadan kalkmasına neden olmamakta; yalnızca 1995/46/EC VKD m. 8/1'de yer alan kesin işlem yasağını ortadan kaldırmaktadır.

6698 sayılı KVKK'nın 6'ncı madde gerekçesinde de hangi hallerde rıza aranmaksızın özel nitelikli kişisel verilerin işleneceği örnekler verilerek açıklanmıştır. Buna göre, "Maddenin dördüncü fıkrasında tahdidi olarak sayılan şartların varlığı halinde, yeterli önlem alınması şartı baki kalmak kaydıyla ilgili kişinin açık rızası aranmaksızın özel nitelikli kişisel verilerin işlenmesine imkân tanınmaktadır.

Madde gerekçesine göre, ilgili kişinin rızası olmasa bile, kanunlarda açıkça öngörülen hallerde özel nitelikli kişisel veriler işlenebilecektir. Örneğin, askerlik yapacak kişilerin bazı özel sağlık bilgilerinin ilgili kanun hükümleri uyarınca işlenmesi, yine hastanelerin, eczanelerin ya da Sosyal Güvenlik Kurumunun hastalarla ilgili veri işlemesi bu kapsamda değerlendirilecektir.

Aynı madde gerekçesinde, siyasi parti, vakıf, dernek veya sendika gibi kâr amacı gütmeyen kuruluş ya da oluşumlar tarafından, özel nitelikli kişisel verilerden bazılarının işlenebilmesi düzenlenmektedir. Buna göre, bu kuruluş ve oluşumlar, kendi üye ve mensuplarının özel nitelikli verilerini, kuruluş amaçlarına ve tabi oldukları mevzuata uygun, faaliyet alanlarıyla tahditli ve üçüncü kişilere açıklanmamak kaydıyla işleyebileceklerdir. Örneğin, bir siyasi partinin veya sendikanın üyelerine ilişkin kimlik ve iletişim bilgilerini, fıkrada belirtilen şartlarla tutması, bu bent kapsamında değerlendirilecektir. Bu kuruluşlar, sadece kendi faaliyet alanlarıyla tahditli olarak özel nitelikli veri işleyebileceklerdir. Örneğin, bir sendika, kendi faaliyet alanına ve amacına ilişkin olarak sadece sendika üyeliğiyle ilgili verileri

işleyebilecektir. Buna karşın üyelerin sağlık veya din ya da mezhebine yönelik kişisel verileri, faaliyet alanıyla ve amacıyla ilgisi olmaması sebebiyle işleyemeyecektir.

Bununla birlikte, ilgili kişinin kendisi tarafından kamuoyuna açıklanmış olan özel nitelikli kişisel verileri işlenebilecektir. Zira ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir.

Ayrıca, özel niteliği olan kişisel verilerin, bir hakkın tesisi, kullanılması veya korunması için işlenmesinin zorunlu olması hali düzenlenmektedir. Örneğin, bir işverenin, engelli çalıştırma zorunluluğu kapsamında, işyerinde, bu statüde çalıştırdığı kişilere ilişkin rapor ve belgeleri işlemesi bu kapsamda değerlendirilecektir. Yine engelli bir kişinin özel tüketim vergisinden muaf özel donanımlı araç almak hakkından yararlanabilmesi için, engelliliğine ilişkin sağlık raporlarının vergi dairesi tarafından edinilmesi ve işlenmesi de bu bent kapsamında değerlendirilecektir.

Son olarak da özel nitelikli verilerin; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi düzenlenmektedir. Bu bağlamda, Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun bu madde gerekçesinde yazılı amaçlarla tuttukları veriler ve kayıtlar bu kapsamda değerlendirilecektir."

2.3.2 Hassas olmayan (genel nitelikli) veriler

Yukarıda hassas kişisel veriler başlığı içerisinde yer almayan, ele geçirilmesi durumunda herhangi bir mağduriyete neden olmayan, kişilerin ayrımcılık tehlikesi ile karşılaşmasına neden olmayan veriler ise hassas olmayan kişisel veriler olarak değerlendirilmektedir (Özdemir, 2009:69; Şahin, 2011:65).

Örnek vermek gerekirse kişilerin isimleri ya da cep telefonu numaraları çoğu zaman hassas olmayan veriler arasında gösterilmektedir. Bu verilerin işlenmesi, direktifler ve KVKK'da yer alan özel hükümler doğrultusunda değil, genel hukuka uygunluk nedenleri kapsamı içerisinde işlenebilmektedir. Aslına bakıldığında KVKK, hassas ve hassas olmayan verilerin işlenmesine ilişkin unsurlar arasındaki ayrımı asgari seviyelere indirmiş olsa da teorik olarak böyle bir ayrım yapılmaktadır.

2.4 Kişisel Verilerin Korunması

Çalışmanın temelinde yer alan konunun kişisel verilerin korunması olduğundan, kavramın genel yapısı gereği içerisinde çeşitli birçok konu yer alabilmekte ve kapsam çalışmanın türüne göre daha da fazla genişleyebilmektedir. Kişisel verilerin korunmasına yönelik olarak hem ulusal hem de uluslararası boyutta gerçekleştirilen yasal düzenlemeler oldukça önemlidir. Özellikle AB bünyesinde ortaya çıkan birtakım yasal düzenlemeler kavrama dair yaklaşımlarımı anlamlandırmaktadır.

Hukuk disiplini içerisinde, korunmasına gereksinim duyulduğu düşünülen maddi ve manevi birçok unsur yazılı olarak hazırlanan düzenlemelerle garanti altına alınmaya çalışılmaktadır. Küresel ölçekte teknolojide ve iletişim sistemlerinde yaşanan gelişmelere paralel olarak kişisel verilere erişim çok daha kolay bir hal almıştır. Bu durumda kişisel verilerin kullanılmasındaki amaçlara göre sınıflandırılması neticesinde olası mağduriyetlerin önüne geçilmeye çalışılmış ancak kimi zaman ise ortaya çıkan bazı suiistimaller bireyleri çeşitli olumsuzluklarla karşı karşıya bırakmıştır. Kişisel verilerin usulüne uygun olarak kullanılmamaya başlaması ile birlikte bireylerin temel hak ve özgürlüklerinin ihlal edilmeye başlaması ve bu durumun zaman içerisinde bireyler adına önemli bir tehdit unsuru haline gelmesi küresel ölçekte bireyleri, devletleri, sivil toplum kuruluşlarını, işletmeleri, çok uluslu örgütleri harekete geçmeye zorlamıştır. Bu hareketler doğrultusunda kişisel verilerin korunmasına yönelik yasal düzenlemeler yapılmaya başlanmıştır. Ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun çıkarılmış olması ve Kanun ile belirlenen tarihlerin geçmesiyle birlikte öngörülen yükümlülüklerin de tamamının yürürlüğe girmesi ile kişisel verileri koruma hukukunun uygulamaya yönelik güncel sorunları ön plana çıkmıştır. Ancak bu hukuk dalının altında insan hakları ve temek hak ve özgürler içinde değerlendirilen "kişisel verinin korunmasını isteme hakkı" yatmaktadır (Dülger, 2018:72)

Kavram ile ilgili olarak karşılaşılan ayrım hatalarının başında; verilerin korunması ve verilerle ilişkili olan kişilerin korunması gelmektedir. Bu alanda yapılan hukuki çalışmaların temelinde kişisel hakların korunması yer almaktadır ancak bu düzenlemelerle verilerle ilişkili olan kişilerin korunması amaçlanmaktadır. Bu doğrultuda salt bir şekilde verilerin korunması, hukuk düzeni içerisinde bir araç olarak değerlendirilmektedir. Verilerin korunmasına yönelik olarak gerçekleştirilen

çalışmalar, yasal çerçeve dışında kalan ve daha teknolojik düzenlemeleri içeren bir yapıya sahiptir (Gola ve Schomerus'dan akt. Küzeci, 2010:13).

1982 Anayasası incelendiğinde aslında birçok temel hak ve özgürlüğün kişisel verilerle ilgili olduğu görülmektedir. Bakıldığında anayasada yer alan; özel hayatın gizliliği, haberleşme özgürlüğü, din ve vicdan özgürlüğü, düşünce ve kanaat özgürlüğü vb. birçok hakkın doğrudan kişisel verilerle bağlantı içerisinde olduğu anlaşılmaktadır. Anayasanın 22 nci maddesinde yer alan haberleşme özgürlüğü ile ilgili düzenlemelerle birlikte kişilerin, kişisel veri olma özelliği taşıyan bilgileri anayasal güvence altına alınmıştır (Civelek, 2011:141). Benzer bir şekilde kişisel verilerin korunmasına dair doğrudan olmasa dahi, dolaylı olarak Avrupa İnsan Hakları Sözleşmesinin 8 inci maddesinde özel hayatın gizliliği ile ilgili olarak yapılan düzenlemeler, kişisel verilerin korunmasına atıfta bulunmaktadır. Kimi zaman bu düzenleme üzerinden Avrupa İnsan Hakları Mahkemesi tarafından kişisel verilerin korunması ile ilişkili kararlar verilmektedir (TBD, 2008:21). Kişisel veriler kapsamı içerisinde yer alan birçok veri, bireylerin özel yaşamları ile ilişki içerisinde ve bu verilerin bireylerin en mahrem olarak değerlendirdikleri bilgileri dahi açığa çıkarma riskini taşımaktadır. Böyle bir durum içerisinde kişisel veriler, doğal olarak özel hayatın bir parçası olarak değerlendirilmektedir.

Kişisel verilerin korunması ile birlikte özel hayatın gizliliği, Anayasanın 20 nci maddesinde güvence altına alınmıştır. Özellikle teknolojinin gelişimi ile birlikte hak ve hürriyetlerin müdahaleye daha açık bir hale gelmesi, kişisel verilerin korunmasını hukuki bir problem olarak ortaya çıkartmıştır. Bu durum ise bu konuda yasal düzenlemelerin yapılmasını zorunlu kılmıştır. 12 Eylül 2010 tarihinde yapılan halkoylaması sonucu kabul edilen 5982 sayılı Kanun'la yapılan Anayasa değişikliği ile Anayasanın 20 nci maddesine ilave bir fıkra eklenerek kişisel veriler; Özel hayatın gizliliği ve korunması hakkı" kapsamında Anayasal güvenceye kavuşmuştur. Söz konusu fıkrada; *"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."(AY. m.20)* hükmüne yer verilmiştir.

Sözü edilen Anayasa hükmü doğrultusunda;

- Herkes, kişisel verilerinin korunmasını isteme hakkına sahiptir.
- Bu anlamda bireyler temel olarak, kendileri ile ilgili kişisel verilerin ilgisiz üçüncü kişilerin eline geçmemesi konusunda gerekli tedbirlerin alınmasını isteme hakkına sahiptirler.
- 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. Bu anlamda bireyler, hangi amaçla hangi kişisel verilerinin kullanıldığını öğrenme hakkına sahip olduğu gibi söz konusu kişisel verilerde herhangi bir yanlışlık bulunması halinde bu durumun düzeltilmesini ya da verilerinin silinmesini isteme hakkına da sahiptirler.
- Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Yasal bir düzenleme bulunmaması ya da bireyin kendisine ait kişisel verilerin işlenmesi yönünde açık bir irade beyanının olmaması durumunda kişisel verilerin işlenebilmesi mümkün değildir.

Anayasanın 20'nci maddesinin 3'üncü fıkrasında kişisel verilerin korunması öngörülmektedir. Ayrıca kişisel verilerin hukuka aykırı olarak işlenmesi, Anayasanın 17'nci maddesi ile güvence altına alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı ile Anayasanın 20 ve 22'nci maddelerinde düzenlenen özel hayatın gizliliği ve korunması hakkının ihlali anlamına da gelmektedir.

Anayasanın 20'nci maddesinin 3'üncü fıkrasında, kişisel verilerin ancak bireyin açık rızası veya kanunda öngörülen hallerde işlenebileceği, kişisel verilerin nasıl korunacağına ilişkin esas ve usullerin kanunla düzenleneceği ifade edilmiştir. Anayasa hükmünde, kanunla öngörülen hallerde kişisel verilerin işlenebileceği belirtilmesine rağmen, özel sınırlama sebeplerine yer verilmediği görülmektedir.

Anayasada öngörülen hüküm gereğince 26 Aralık 2014 tarihinde "Kişisel Verilerin Korunması Kanunu Tasarısı" TBMM Başkanlığına sunulmuştur. Tasarı, 24 Mart 2016 tarihinde kanunlaşmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete 'de yayımlanarak yürürlüğe girmiş, böylece kişisel verilerin korunması için gerekli hukuksal altyapı tamamlanmıştır.

2.5 Veri Güvenliğini Sağlamada Temel İlkeler

Dünya genelinde kabul gören bir yaklaşım doğrultusunda bilginin güvenliğinin sağlanabilmesi adına aşağıda belirtilen şartların sağlanması gerekmektedir;

- Önem seviyesi ve hassasiyeti yüksek verilerin arzulanmayan bir şekilde yetki sınırları dışında kalan insanların erişimine açık olmaması gerekmektedir ve gerekli bilgiler yalnızca yetkili kişiler tarafından erişilebilir olmalıdır (Confidentiality-Gizlilik).
- Veri sahibi haricinde bilginin değiştirilmesinin ya da silinmesinin engellenmesi gerekmektedir (Integrity – Bütünlük).
- Veriler ya da veri sistemlerinin kullanımında sürekliliğin sağlanması gerekmektedir (Availability – Sürekli Kullanılabilirlik).
- Kullanıcılara dair kimlik doğrulama sistemlerinin geliştirilmesi gerekmektedir (Authentication).

Veri güvenliğinin sağlanması konulu araştırmalar sonucunda, yalnızca teknoloji temelli önlem girişimleri ile iş süreçleri içerisinde yukarıda da ifade edilen güvenlik unsurlarının sağlanması mümkün görülmemektedir. Veri güvenliğinin sağlanması ile iş süreçlerinin tam bir koordinasyon içerisinde yürütülmesi gerekmekte ve kurumlarda bilgi güvenliğinin sağlanmasına yönelik bir kültürün oluşturulmasına özen gösterilmesi gerekmektedir (Ersoy, 2007:3).

Sanal ortamlarda gerçekleştirilen işlemlerin sayıca ve türce artış göstermesi, kişisel verilerin korunması ve gizlilik kavramının hayata geçirilmesi noktasında birtakım yenilikçi sistemlerin geliştirilmesi zorunluluğunu ortaya çıkarmaktadır. Günümüzde kişisel verilerin kurumların sistemlerine işlenmesi ve bu verilerin elektronik ortamlarda kullanılması zorunlu hale gelmiştir. Ancak bu durumda kişilerin haklarının korunmasına yönelik daha çok çaba sarf edilmesi gerekmektedir (Ersoy, 2007:4).

2.6 Verilerin Korunmamasının Sakıncaları

Gerçek ve tüzel kişilere ait verilerin korunmaması ve bilgilerin gizli tutulamaması neticesinde ortaya çıkacak olumsuzlukların ve mağduriyetlerin tek bir cümle üzerinden açıklanması mümkün değildir. Bu doğrultuda ortaya çıkması muhtemel zararlar alt başlıklar içerisinde değerlendirilmiştir.

2.6.1 Gizliliğin kaybolması

Gizliliğin ihlal edilmesi, bireylere ait özel belgelerin, verilerin, bilgilerin yetki sınırların dışarısında kalan bir başka birey ya da kurum tarafından ele geçirilmesi, ya da hukuksal olmayan yöntemlerle saklanması anlamına gelmektedir.

Gerçek ya da tüzel kişilere ilişkin, gizli kalması gerekli olan bir bilginin üçüncü şahıslar tarafından öğrenilmesi, ilk etapta çok fazla risk taşımayan bir durum olarak değerlendirilebilmektedir. Fakat bu durum, tahmin edildiğinden çok daha büyük zararlara yol açabilmektedir. Örnek vermek gerekirse, bir kişinin kredi ya da banka kartı bilgilerinin gizli tutulması gerekmektedir. Bu bilgilerin kötü niyetli üçüncü kişilerin eline geçmesi kişileri maddi olarak zarara uğratabilmektedir (Adalı, 2016:6). Yine ilgili kişinin e devlet şifresinin ele geçirilerek onun adına birtakım iş ve işlem yaparak maddi ve manevi zararlara yol açılabilmektedir.

2.6.2 Bilginin başka amaçlarla kullanımı

Bireylere ait kişisel bilgilerin toplanmasının ardından farklı amaçlar için kullanılması, bilgi sahibinin rahatsızlık duymasına neden olabilmektedir. Örnek vermek gerekirse, ikamet edilen adrese ait bilgilerin toplanması neticesinde, bu bilgilerin mağaza sahiplerine verilmesi sonrasında satış temsilcilerinin kişileri araması, evine gelmesi, adresine kataloglar göndermesi adres sahibini rahatsız edebilmektedir (Adalı, 2016:6). Ya da iletişim amacıyla AVM deki mağazalarca talep edilen telefon numaralarının bilahare reklam amaçlı olarak kullanılması ilgili kişileri rahatsız edebilmektedir.

2.6.3 Bilginin değiştirilmesi

Bilgi erişiminin sağlanması, sonrasında bilgilerin değiştirilmesi riskini ortaya çıkarmaktadır. Sistem içerisinde bilgilerin değiştirilmesi ise bireylere ve kurumlara birtakım zararlar verebilmektedir. Örnek vermek gerekirse emniyet birimlerinde sabıkalı olarak görülen bir kişinin bu kaydının sabıkasız olarak değiştirilmesi kurumlara ve bireylere zarar verebilmektedir. Finansal kurumlarda ise bu durumun sonuçları çok daha ağır olabilmektedir (Adalı, 2016:6). Aynı şekilde sahte diploma ile iş başvurusu yapan kişinin kurumlara ve kişilere verebileceği zararlar da bu yönde değerlendirilmelidir.

2.6.4 Bilginin kötü niyetle kullanılması

Gerçek ya da tüzel bir kişi ile ilgili olarak gizlilik içerisinde saklanması gerekli olan bilgilerin paylaşılması kişilerin ya da kurumların zarara uğramasına neden olabilmektedir. Gizli kalması gereken bir bilginin, kötü niyetli üçüncü kişilerin eline geçmesi sonrasında bilgi sahibi olan kişi tehdit edilebilmekte, şantaj yolu ile kişi üzerinden birtakım menfaatler elde edilebilmektedir. Örneğin kişinin resimlerinin ya da ses kaydının onun izni olmadan sosyal medyada aleyhine hüküm doğuracak biçimde yayımlanması ilgili kişiye maddi ve manevi zararlar verebilecektir. Bu duruma ek olarak küresel ticaret ortamı içerisinde rekabet şartlarının gün geçtikçe ağırlaştığı günümüzde ticari bilgilerin gizli tutulmaması, işletmelerin önemli zararlarla karşı karşıya kalmasına neden olabilmektedir. Benzer bir durum ulusal güvenlik içinde geçerli olmaktadır (Adalı, 2016:7).

3. İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ KİŞİSEL VERİLERİN KORUNMASINDAKİ ROLÜ

3.1 Bilgi İşlem Departmanlarının Kişisel Verilerin Korunmasındaki İşlevi ve Rolü

3.1.1. Bilgi işlem departmanlarında kişisel veri edinimi ve işlenmesi

Bilgi İşlem departmanları, elde edilen verilerin işlenmesi ve korunmasına yönelik mevcut yöntem ve teknikler doğrultusunda çeşitli uygulamalar gerçekleştirmektedir. Bilgi işlem departmanları tarafından yasalara aykırı veri işleme faaliyetlerinin engellenmesi amacı ile çeşitli sistemler oluşturulmakta, oluşturulan sistemlerin gözetim ve denetim etkinliklerini gerçekleştirmek üzere yetkili çalışanlar belirlenmekte ve sürecin geneline dair temel prensipler ortaya konulmaktadır. Bunlara ek olarak bilgi işlem departmanları tarafından teknik sebeplere bağlı olarak ortaya çıkabilecek muhtemel güncellemeleri takip ederek sistemin işleyişine dair güncellemelerin yapılması gerekmektedir. Bilgi işlem departmanları tarafından verilerin toplanması, işlenmesi, silinmesi gibi işlemlere dair donanım, yazılım altyapısı ve yönetim şeması oluşturulmaktadır. Bu yapıların işleyişinin izlenmesi, denetim süreçleri, gerekli güncellemelerin yapılması, teknik donanımın sürdürülebilir durumda bulundurulması bu departmanın önemli misyonlarından biridir. Bilgi işlem departmanlarının veri edinimi ve işleme konusunda kullandığı araçlar ve yöntemler kısaca bu başlıkta incelenmiştir.

3.1.1.1 Bilgisayar ve merkezi veri bankaları

Bilgisayar teknolojilerinde ve teknolojinin genelinde meydana gelen şey öncelikle, işlerin yapılabilirlik seviyesinin etkilemesidir. Teknolojiden doğan imkanlar ile veri toplama işlemleri, verilerin depolanması, verilerin ilişkilendirilmesi çok daha hızlı ve kolay bir şekilde yürütülmeye başlanmıştır (Miller, 1971:216). Bu durumda ise dönemin bir gerçeğinin de üzerinde durmak gerekmektedir.

İlk ortaya çıktığı dönemlerde bilgisayar, bugünkü kullanımından çok daha farklı niteliklere sahipti. Kullanımı oldukça zor, geniş bir hacme sahip bu cihazlar, maliyetlerinin de yüksek olmasının bir sonucu olarak yalnızca çok büyük ölçekli işletmeler ve devletler tarafından kullanılabilmekteydi (Henderson, 2006:13). Daha farklı bir ifade ile kullanımının çok yaygın olmaması nedeni ile bilgisayarların kontrolü merkezi güçlerinde elinde bulunmaktaydı. Bu durumun doğal bir sonu olarak ise söz konusu teknolojinin kullanımında doğan bir çekince unsurunu meydana getirmekteydi.

Söz konusu çekincelerin ortaya çıkmasının temel nedeni ise, verilerin yalnızca merkezi birimlerde toplanıyor olmasıdır. Bu süreç içerisinde veri toplamanın çok daha hızlı gerçekleşmesi ile birlikte veri ambarları ortaya çıkmaya başlamıştır (Çölkesen vd., 2006:879-883). Ancak bu süreç içerisinde veri miktarının hızlı bir şekilde artması neticesinde işe yarayacak verilere ulaşmak gittikçe zorlaşmaktadır. Bu zorlukların üstesinden gelebilmek adına yürütülen çalışmalar neticesinde ise "veri madenciliği" kavramı ortaya çıkmıştır. Bu kavram üzerinden birbiri ile bağlantılı olmayan veriler arasında beklenmedik ilişkiler ortaya çıkmaya başlamıştır (Cadaoux, 1998:68).

Birçok devlet tarafından, özellikle bürokratlar tarafından 1960 ve 1970'li yıllara gelindiğinde dağınık bir şekilde bulunan verilerin tek bir merkezde toplanmasının oldukça faydalı olacağı görülmüştür. Bu durumun ortaya çıkmasında hiç kuşku yoktur ki bilişim teknolojilerinde yaşanana gelişmeler etkili olmuştur (Bennett, 1992:49-53). Bu dönem içerisinde tartışmalarla birlikte hayata geçirilen vatandaşlık numaraları, kişisel verilerin korunmasına yönelik endişelerin de yüksek bir sesle dile getirilmesine yol açmıştır. Bu sürecin devamında soru işaretlerinin artmasına neden olan bir diğer uygulama ise otomatik nüfus sayımlarının gerçekleştirilmesidir (Bennett, 1992:49-53).

Bu gelişmelere kamu kesiminden doğan duyarlılıkların temelinde, özel hayatın gizliliğin ihlal edileceğine dair endişeler ve çoğul demokratik toplum anlayışının zarar görmesi korkusu yer almaktadır. Bu dönemde yaşanan gelişmelerle ile birlikte, bireylere ait bilgiler çevrelerinde gelen aktarımlar ve kurumların tozlu arşivlerinden çıkarılan bilgiler üzerinden bilgisayar ortamlarına taşınmaya başlamıştır. Bu doğrultuda ise dönem içerisinde birçok düşünür, hukukçu ve yazarlar, bilgisayar kullanımından kaynaklanabilecek sorunların üzerine yoğunlaşmışlardır (Solove, 2004:15).

Fakat teknolojide yaşanan gelişmeler hızlanarak devam etmiş ve bilgisayar kullanımının yaygınlaşması da paralel bir şekilde hızlanmıştır. Bu durumda bilgisayarlarda saklanmakta olan kişisel verilerin korunması çok daha önemli bir hale gelmiştir. Bu durumun ortaya çıkmasının nedenlerinin başında, toplanmakta olan veri sayısının hızlı bir artış göstermesidir. Yenilikçi teknolojiler üzerinden ortaya çıkan dört temel unsur veri sayısının artışında etkili olmuştur (Cate, 1997:14-16):

- Bilginin ortaya çıkarılması, işlenmesi, yayılması ve saklanması gelişmeler neticesinde çok daha kolay bir şekilde yürütülmektedir.
- Bu işlemlerin gerçekleştirilmesi, elektronikleşmenin bir sonucu olarak çok daha düşük maliyetlerle ortaya çıkmaya başlamıştır.
- Günümüz bilgi çağı içerisinde bilgiler, elektronik ortamda saklanmaları ile birlikte çok daha kıymetli bir hale gelmişlerdir. Zira bilgilere yönelik işlemler çok daha kolay yapılmaya başlanmıştır.
- Bilgisayar sistemleri ve ağların mevcut özellikleri doğrultusunda bilgi varlığının gelişmesine katkı sağlanmaktadır (Cadaoux, 1998:114).

Günümüzde en önemli gözetim aracı olarak ise, elde edilen verilen korunması, veriler arasında ilişkilendirmelerin yapılması, işleme süreçlerinin izlenmesi ve pazarlanabilir olmasını sağlaması nedeni ile bilgisayarlar olarak gösterilmektedir. Veri kapsamının içerisinde DNA kodlar, görsel veriler, işitsel veriler yer alıyor olsa da gözetlemenin sağlanmasına yönelik olarak geliştirilen teknolojilerin temelinde de bilgisayar yer almaktadır. Gözetleme kavramının merkezinde bilişim teknolojilerinin yer almasındaki neden olarak ise bilgisayar teknolojilerinin büyümesi ve kapsamının genişlemesi gösterilebilmektedir. Bu anlamda yürütülen gözetleme etkinlikleri ise verimlilik artışlarının sağlanması ve sıradan işlemlerin yerine getirilmesi açısından da modern yaşamın bir gerekliği olarak değerlendirilmektedir (Lyon, 2006:13).

İşletmelerin bünyesinde kurulan bilgi işlem departmanları ile beraber, devlet kontrolünde yer alan veri tabanları haricinde, içeriklerinde kredi kartı ve telefon verilerinin yer aldığı ticari özelliklere sahip veri tabanlarının kullanılması ile bireylerin bir araya getirildiği bütünsellik ifade eden profillerin meydana getirilmesi mümkün hale gelmiştir. Öyle ki, bu yönteme olan yönelim her gün biraz daha artmaktadır. Günümüzde, bilgimiz dahilinde olsun ya da olması bilgisayar sistemleri içerisinde rakamlarla formüle edilmiş benlikler, sistem içerisindeki genel resmin gittikçe büyümesine yol açmaktadır.

Bize ait en ayrıntılı aktarımının gerçekleştiği resmin ortaya çıkmasında kamu ve özel sektör arasında ortaya çıkan bilgi akışı da oldukça dikkat çekicidir. Daniel J. Solove, "dijital siciller"in ortaya çıkışında üç farklı bilgi akışının etkili olduğunu ifade etmektedir. Bu doğrultuda edinilmekte olan veriler (Solove, 2004:3):

- Özel sektör kuruluşları arasında,
- Kamu sektöründen özel sektöre,
- Özel sektörden kamu sektörüne sürekli bir akış halindedir.

Bilgisayar sistemleri olmadan rahatlıkla ulaşılamayacak birçok veriye, gelişen gözetim sistemleri erişebilmek çok daha kolay hale gelmiştir. Bunlar arasında; bireylerin mali durumları, sağlık durumları, tüketim eğilimleri, davranış biçimleri, eğitim durumları, etnik kökenleri, sağlık yardımlarından yararlanılan durumlar, suç oluşturan faaliyetler vb. birçok unsur yer almaktadır. Bu durum yeni teknolojilerin kullanılması ile gözetim kapasitelerinde artışların meydana geldiğini göstermektedir. Özellikle internet teknolojisinin gelişmesi, birbirinden konum ve görev bakımında uzak kuruluşların veri tabanlarına ulaşmasına ve karşılaştırmalarda bulunmasına olanak sağlamaktadır (Lyon, 2006:120). Gelişen veri saklama ve işleme kapasitesine karşılık ortaya çıkan bir gerçek ise, kişisel verilerin korunmasının sanal ortamda gerçeğe kıyasla çok daha zor olmasıdır (Bellia vd., 2003:605).

3.1.1.2 Gözetim sağlayan yeni teknolojiler

Verilerin izlenmesi, gözetlenmesi ve toplanması teknolojide yaşanan gelişmeler neticesinde birçok aracın kullanımı ile gerçekleştirilebilir hale gelmiştir. Bu durum, bilgi çağı içerisinde kişisel verilerin korunması hakkının çiğnendiği eylemlerin tanımlanmasının çok daha zor hale gelmesine yol açmaktadır (Tansuğ, 2006:536). Bu alanda uzmanlaşmış kurumlar tarafından gelişmiş araçların kullanılması ile bireylerin izlemelerin hedefinde yer aldığı endişelerinin artması, daha önceleri istisna olarak değerlendirilen izleme durumunun bir kural biçimine dönüştüğünü göstermektedir (Lyon, 2006:16).

Teknolojik gelişmeler neticesinde geliştirilen yeni araçlar ile kişisel verilerin toplanması mümkün olduğu gibi, daha önceleri farkına varılmayan yeni ve önemli bilgilerde gün yüzüne çıkarılmaktadır. Bu durumun en belirgin örneklerinden biri "DKA" verileri olarak gösterilmektedir (King ve Stansfield, 1997:95). Genler insanlar tarafından taşınmakta olan en geniş veri hazneleri olarak kabul edilmektedir

(DiMartino, 2005:20). "DKA"nın içeriğinde gen parçaları bulunmaktadır. Genler üzerinden elde edilen veriler, bireyin farklılığını ortaya koyan tüm unsurları kapsadığı için ve buna ek olarak akrabalarına ilişkin bilgileri de içeriği için kişisel verilen korunması hukuku içerisinde oldukça önemli bir yere sahiptir.

Geliştirilen birçok yeni araba modelinde, hız, sürüş ve direksiyon tutuşuna dair birçok bilgi kayıt altına alınmakta ve bu araçların birçoğunda GPS bulunmaktadır. Yeni arabaların bu özellikleri ise sunmuş oldukları imkanlar doğrultusunda birtakım tartışmaları beraberinde getirmektedir. Kullanım açısından birçok kolaylık sağlayan bu arabalar, öte yandan bireylerin alışkanlıklarına dair birçok bilgiyi de kayıt altına almaktadır. Bu doğrultuda söz konu araçların kullanıcılarının, kendilerine ait hangi bilgilerin sistem içerisinde kaydedildiğini bilmesi gerekmektedir ve bu durum aynı zamanda kullanıcıların doğal hakkıdır (MacRonin, 2008). Benzer bir durum cep telefonları üzerinden de karşımıza çıkmaktadır. Günün her anında insanları erişilebilir kılan cep telefonları, servis sağlayıcıları üzerinden bireylerin yer ve zaman bilgilerine ulaşabilmek mümkün olmaktadır (Koops vd., 2009:9). Araba kullanıcılarına benzer bir şekilde cep telefonu kullanıcılarının da kendilerine dair elde edilen bilgilerin kullanım amaçlarını bilme hakkının olması gerekmektedir.

Kullanımı sürekli yaygınlaşmakta olan ve kapsamında araçları sürekli gelişen teknoloji ile yeni bir gözetim türünün ortaya çıktığını ifade etmek mümkündür. Gözetim türünün farklılaşan yapısı, daha önceleri bu denli belirgin olmayan özelliklere sahip olmasından kaynaklanmaktadır. Gary T. Marx (1988:217-219)'a göre yeni gözetim türünün farklılaşan özellikleri aşağıdaki gibidir:

- Daha yoğun ve daha yaygındır.
- Emek yoğunluğuna değil, sermaye yoğunluğuna bağlıdır,
- Merkezileştirilmiş kendini denetlemeyi içerir,
- Görünmezdir ya da görünürlüğü düşüktür,
- Belirli bireyleri hedeflemekten çok herkes şüpheli durumundadır,
- İrade dışıdır,

Bunlara ek olarak Marx tarafından, söz konusu yeni gözetimin devlete ait güç unsurları üzerindeki geleneksel tekeli içerisinde kaynağına ulaştığı öne sürülmektedir. Bu doğrultuda zorlamadan ziyade yönlendirmeler, hapishane kurumları yerine kullanılan çipler, kelepçeler yerine ise tutukluların uzaktan izlediği bir süreç ortaya çıkmıştır. Tüm bu gelişmeler ise toplumun geneline dahil olabilme potansiyelini taşımaktadır

(Marx, 1988:217-219). Ayrıca teknolojinin hızla gelişmesi ile birlikte yeni imkanların ortaya çıkışı devam etmektedir. Yakın bir tarihte araç kullananların kalp atışlarının izlendiği, yorgunluk ya da uyku durumlarının tespit edilebileceği sensörler, GPS sistemleri, gelişmiş özelliklerle donatılmış mikro kameralar ve telefonların mutlak bir hakimiyet kuracağını ifade etmek mümkündür (Cadaoux, 1998:115).

Teknolojinin gelmiş olduğu noktada, sıradan telefon görüşmeleri üzerinden uyuşturucu alışverişlerinin tespit edilmesi, arananların kalabalık içerisinde rahatlıkla tespit edilmesi, uydu üzerinden şüpheli davranışlarının görüntülenmesi tam anlamı ile mümkün değildir. Ancak bu gelişmelerin çok yakın bir zaman içerisinde ortaya çıkacağını rahatlıkla ifade edebilmekteyiz (Schneier, 2014:31). Verilerin depolanması ve toplanmasında çok daha düşük alanlara gereksinim duyulması ve maliyetlerin düşmesi yönündeki eğilimler göz önünde bulundurulduğunda, gelecek yıllar içerisinde yaşamın her anının ses ve görüntüler üzerinden kayıt altına alınabileceğini öngörmek mümkündür.

Yukarıda verile ifadeler doğrultusunda, zaman içerisinde gelişimini sürdürmekte olan, hızlı bir yayılım gösteren ve maliyetleri süreç içerisinde düşen bilişim teknolojilerine dair unsurlar kısaca açıklanmaya çalışılmıştır. Buradan hareketle teknolojide yaşanan gelişmeler neticesinde verilerin saklanması, kayıtların elle yapıldığı süreçlere kıyasla çok daha kolaylaşmış ve benzer bir şekilde verilere erişim olanakları da gelişmiştir. Verilerin toplanması sonrası yeni işlemlere tabi tutmak ise geçmiş dönemlere kıyasla çok daha rahat ve düşük maliyetlerle gerçekleşmektedir (Samuelson, 2000:1126).

3.1.1.3 Internet

Teknolojide yaşanan gelişmelerin kişisel verilerin toplanması ve işlenmesi açısından değerlendirilmesi sürecinde ilk önemli basamak olarak bilgisayarların ve veri bankalarının oluşumunun üzerinde durulmuştur. Bu süreç içerisinde ortaya çıkan ikinci önemli aşama ise internet teknolojilerinin gelişimi ve internet kullanımının artmasıdır (Magee, 2002:277). Öyle ki, internet ve internet ile ilişki içerisinde olan teknolojilerin gelişimine ve kullanımının yaygınlaşmasına paralel olarak bilişim teknolojileri kapsamında yeni bir dönemin kapıları açılmıştır. 20.yüzyıl içerisinde hızla gelişim gösteren internet kavramı, 21. Yüzyıla gelindiğinde ise yaşamımızın ayrılmaz bir parçası olma özelliğine sahip olmuştur. İnternet ağı üzerinden bilgisayar sistemlerine birbirine bağlanması ile birlikte veri tabanlarının paylaşıma açılması,

kıyaslamaların ve birleştirilmelerin yapılması mümkün hale gelmiştir. Fakat internet kullanımının etkilerinin bu alanda sınırlandırılması söz konusu değildir.

Dünya genelinde internet kullanılmayan alan gün geçtikçe daralmakta ve bu alan dışında kalan yerlerde elektronik iletişim yöntemleri hayatımızın vazgeçilmez bir unsuru haline gelmektedir. Bu gelişmelerle birlikte metinlerin ve kelimelerin oluşturulmasında işlemciler kullanılmakta, bilgisayarlara ait hafızalarda saklanmakta, iletilme süreci ağlar, telefon hatları, uydular üzerinden yürütülmekte, görüntülenmesinde ise faks, yazıcı ve bilgisayar ekranlarından yararlanılmaktadır. Bu sistem içerisinde metinlerin, görüntüler ve seslerin kayıt altına alınmasında ise kameralardan, tarayıcılarda ve mikrofonlardan yararlanılmaktadır. Kayıt altına alınan unsurlar hafıza kartlarında, disklerde ya da teyplerde saklanmaktadır. Kayda alınan unsurlar havadan ya da fiber optik kablolar üzerinden yayına açılmakta, bilgisayarlar, cep telefonları ve televizyonlar tarafından da sunulmaktadır. Kısaca gün geçtikçe sanayileşmekte olan dünyamızda bilginin oldukça önemli bir kısmı elektronik özellikler içermektedir (Cate, 2001:159-195).

Kullanıcıların internet üzerindeki tüm hareketleri bir verinin ortaya çıkmasına neden olmaktadır. Bu durum kullanıcıların bilgisi dahi olmadan iletişim süreçlerinin takip edilmesine ve kendilerine ait verilerin toplanmasına yol açabilmektedir. Öyle ki, kullanıcılarda zaman içerisinde deneyimlerinden yola çıkarak bu alanda daha fazla bilgi sahibi olmaya başlamışlar ve bilgisayarların ve internet kullanımının dünyaya açılan bir pencere olduğunun farkına varmışlardır. Kullanıcıların internet üzerinden yaptıkları aramalar ve tercihleri sonrasında onlara dair birtakım bilgiler ilgili toplama merkezlerine veri olarak akmaktadır (Garrie ve Wong, 2006:129-152). Toplanan bu verilerle öncelikle ticari amaçlara hizmet verilmektedir. Söz konusu verilerin toplanması ise iki farklı şekilde ortaya çıkmaktadır.

İlk olarak internet siteleri tarafından kullanıcılara dair bilgiler açık bir şekilde talep edilmek suretiyle toplanmaktadır. Zira birçok sitede işlem yapabilmek için öncelikle kayıt olunması gerekmektedir. Bu kayıt formlarında ise çoğu zaman kullanıcı adı ve şifre haricinde çeşitli sorularda sorulabilmektedir (Solove, 2004:23). Böylece kullanıcılara ait veriler yine kullanıcıların kabulü ile sisteme kaydedilmektedir. Ancak bir sitedeki kayıt işlemi üzerinden öğrenilen bilgiler ve ilgi alanları bir başka sitemizde reklam içeriği olarak karşımıza çıkabilmektedir. Bu durum bize verilerin dolaşımda olduğunu göstermektedir.

Kişisel verilerin korunmasına yönelik olarak ortaya çıkan düzenlemelerin birçoğunun içeriğinde elde edilen verilerin paylaşımına dair sınırlamaların getirilmesi amaçlanmaktadır. Fakat bu amaçların uygulama aşamasında çok fazla etkinlik gösterdiğini ifade etmek mümkün olmamaktadır. Bir diğer veri toplama türünde ise, kullanıcılara ait veriler, kullanıcıların izni olmadan gizli metotlar üzerinden elde edilmektedir. Bu amaçla gelişen yöntemlerin ilki IP adreslerinin takip edilmesi iken, diğer yöntem ise "çerez"lerin kullanılmasıdır (DiMartino, 2005:20). Bir internet kavramı olarak çerezler, ticari amaçlarla kurulan sitelerde hedef kitle içerisinde yer alan tüketicilerin belirlenebilmesi amacı ile kullanılmaktadır. Buna ek olarak internet kullanıcılarının davranışlarını gözlemek amacı ile akademisyenler tarafından da bu yolun tercih edildiği bilinmektedir (Lipschultz, 2000:225). Kullanıcıların ziyaret ettiği sitelerle ilgili olarak bilgi almak adına kullanılan çerezler üzerinden, internet kullanıcılarının tüketim alışkanlıkları ve eğilimleri ile ilgili fikir sahibi olmak mümkün olmaktadır (Kang, 1998:1198-1199).

Fakat çerezlerden farklı olarak, internet kullanıcılarının takip edilmesi için geliştirilmiş olan farklı metotlarda bulunmaktadır. Bunlar içerisinde, tıklama akışlı veriler (clickstreamdata), "casus yazılımlar" (spyware) gibi yöntemler yer almaktadır (Solove, 2004:23-26). Bu yöntemler, alanında uzman kişiler tarafından sürekli olarak geliştirilmektedir. Gelişen farklı teknolojiler üzerinde ise kişisel verilerin korunması alanına yönelik olarak yeni sorunlar ortaya çıkmaktadır. Buna örnek olarak; yazılım, müzik, metin, film vb. fikir ve sanat ürünlerinin sahiplerini yasal zeminde koruma altına alabilmek adına geliştirilmiş olan "sayısal haklar yönetimi" (Digital Rights Management-DRM) sistemlerinin gösterilmesi mümkündür (Hoofnagle, 2005:7).

İnternet, içeriğinin genişliği bakımından değerlendirildiğinde dünyanın kapsamı en geniş kütüphanesi olarak ifade edilmektedir. Kullanıcılar tarafından internet tabanı üzerinden gerçekleştirilen çeşitli aramalar ise benzer sorunların ortaya çıkmasına neden olmaktadır. Bu derin kapsama sahip internet ortamında, kullanıcılar gereksinim duydukları bilgiye ulaşabilmek adına arama motorlarından yararlanmaktadır (Sever ve Tonta, 2006:95-99). Google, Yahoo, AltaVista gibi arama motorları üzerinden gerçekleştirilen aramalar bu siteler tarafından kayıt altına alınmaktadır. Kullanıcıların neleri araştırdığına dair gerçekleştirilen kayıtlar, kişisel verilerin korunması açısından birtakım sorunlara sebebiyet vermektedir. Bu alanda ortaya çıkan tartışmaların odak

noktasında ise çoğu zaman arama sonuçlarının kayıt altında tutulma süresi gelmektedir.

Son olarak eklenmesi gereken bir diğer konu ise, internet kullanımının ortaya çıkmış olduğu dönem içerisinde mevcut teknik yapısı, coğrafi dağılımının oldukça dağınık olması, içeriğinin sahip olduğu nitelikler doğrultusunda devletlerin denetiminden bağışık olduğuna yönelik bir düşünce öne çıkmaktaydı. Bu düşüncenin ortaya çıkmasında ki neden ise internet kontrolünü elinde bulundurmamak istemesi değildi. Bu küresel ağın denetlenmesi için devlet oldukça yavaş ve imkanları tahditli bir görüntü çizmekteydi. İlerleyen süreç içerisinde ise bu durumun çok geçerliliği olmadığına kanaat getirildi ve devletler gelişen teknolojiye uyum sağlayarak, ülke genelinde çeşitli amaçlarla internet üzerinde söz sahibi olabilmek adına girişimlerde bulunmuştur. Bu açıklamalar doğrultusunda internetin insan hakları üzerinde güçlü ve zayıf yönlerinin bulunduğunu ifade etmek mümkündür (Steeves, 2000:187).

Devlet tarafından internet iletişimine müdahale edebilmek adına geliştirilen araçlar ve bu alanda gerçekleştirmek istedikleri düzenlemelere yönelik uygulamalar beraberinde birtakım hak ihlallerini de getirebilmektedir (Deibert vd., 2008). Kişisel verilerin korunması hakkının da bu kapsamda değerlendirilmesi mümkündür.

Örgütlerin bünyesinde ise yukarıda ifade edilmekte olan yenilikçi teknolojiler ve araçlar üzerinden verilerin toplanması, korunması, işlenmesi ve gizliliği ile ilgili yenileme çalışmaları bilgi işlem departmanları tarafından yürütülmektedir. Bu anlamda veriler, çeşitli gözetim sistemleri, internet kullanımı ve aracı diğer kanallar üzerinden elde edilmekte, yasal bir zemin içerisinde değerlendirmeye tabi tutulmaktadır.

3.1.2 Bilgi işlem departmanlarının kişisel verilerin korunmasındaki rolü

Kurum ve kuruluşların bünyesinde faaliyet göstermekte olan bilgi ve işlem departmanları, elde edilen kişisel verilerin işlenmesi ve korunmasına yönelik yürütmüş olduğu faaliyetler çerçevesinde mevcut yöntemlerin imkanları doğrultusunda verilerin güncel kalması ve korunması adına gerekli tüm önlemleri alması gerekmektedir. Konu ile ilgili olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 8 inci maddesinde verilerin ulusal sınırlar içerisinde aktarımı ile ilgili olarak düzenlemeler yer almaktadır. Veri aktarımının gerçekleştirilmesine dair düzenlenen mevzuatta yer alan ifadelere uygun olarak sürecin yönetilmesi, aktarım esnasında mevcut hükümler ve

yürürlüğe sokulacak olan mevzuat hükümlerine göre düzenlemelerin yapılması Bilgi İşlem departmanlarının başlıca sorumlulukları arasında yer almaktadır. Bu süreç içerisinde gerekli takip ve koordinasyon işlemleri ise Kişisel Veri Sorumlusu Ekibi tarafından yönetilmektedir. Bilgi işlem departmanları tarafından, kişilerin hangi verileri ile ilgili olarak ülke sınırları içerisinde aktarılmasına rıza gösterdiğinin titizlikle belirlenmesi sureti ile verilerin tutulduğu envantere aktarımın sağlandığı kişilerin ve grupların işlenmesi ile veri aktarımı gerçekleşmektedir.

Kişilere ait niteliksel olarak özel verilerin işlenmesi ile ilgili gereken önlemlerin alınmasına dair belirlenen yükümlülükler, veri aktarımı süreçleri içinde benzer bir şekilde öngörülmüş, alınması gereken önlemlerin ve sürecin genel kontrol edilmesi Kişisel Veri Sorumlusu Ekibi tarafından üstlenilerek işletmelerin işleyişine entegre edilecektir. Bu süreç içerisinde kişisel veri aktarımlarının gerçekleştirileceği 3 üncü kişilerin de gereken tedbirleri alması gerekmektedir. Aktarımların gerçekleştiği süreç içerisinde alınacak önlemlerin belirlenmesi ve sürecin koordine edilmesi, bilgi işlem birimi ile kişisel veri sorumlusu ekibinin öncülüğünde gerçekleştirilmektedir.

Verilerin korunmasına dair hükümlerin yer aldığı 6698 sayılı Kanunun 9 uncu maddesi uyarınca kişisel verilerin ilgili kişilerin onayı alınmadan ülke sınırları dışına aktarılması söz konusu değildir. Veri aktarımlarının ülke sınırları dışında herhangi bir yere aktarılması gerektiğinde veri sahiplerinin açık rızalarının alınması sürecin temel esasları arasında kabul edilmektedir. Bu durumda işletmelerin, kişilerin hangi verilerini ülke sınırları dışındaki 3 üncü kişilere aktarabileceğinin özenle belirlenmesi ve Kişisel Veri Koruma Kurumu tarafından yayınlanacak olan güvenli ülke listelerinin göz önünde bulundurulması neticesinde aktarımların gerçekleştirilmesi gerekmektedir.

İşletmelerin bilgi işlem departmanları tarafından, verilerin hükümlere aykırı bir şekilde işlenmesinin önüne geçebilmek adına teknik tedbirlerin tamamını alması bir zorunluluk olarak ifade edilmektedir. Bu nedenle bilgi işlem departmanları tarafından yasalara aykırı veri işleme faaliyetlerinin engellenmesi amacı ile çeşitli sistemler oluşturulmakta, oluşturulan sistemlerin gözetim ve denetim etkinliklerini gerçekleştirmek üzere yetkili çalışanlar belirlenmekte ve sürecin geneline dair temel prensipler ortaya koyulmaktadır. Bunlara ek olarak bilgi işlem departmanları tarafından teknik sebeplere bağlı olarak ortaya çıkabilecek muhtemel güncellemeleri takip ederek sistemin işleyişine dair güncellemelerin yapılması gerekmektedir.

İşletmelerin çeşitli departmanları tarafından yürütülmekte olan veri işleme etkinlikleri sonrasında söz konusu verilere dair analiz sürecine geçilerek kişisel veri envanterleri hazırlanmaktadır. Bilgi işlem departmanları tarafından ise verilerin toplanması, işlenmesi, yedeklenmesi, güvenliğinin sağlanması, silinmesi, yok edilmesi, anonim hale getirilmesi gibi işlemlere dair donanım, yazılım altyapısı ve yönetim şeması oluşturulmaktadır. Bu yapıların işleyişinin izlenmesi, denetim süreçleri, gerekli güncellemelerin yapılması ise kişisel veri sorumlusu ekibi tarafından sağlanmaktadır.

Oluşturulan kişisel veri matrisleri ve envanterleri kapsamında kişisel verilerin erişimi, hangi amaçlarla işleneceği ve ilgili personeller tarafından bilgi işlem departmanları tarafından belirli sınırlar içerisinde yönetilmektedir. Süreç içerisinde işletmede çalışan herkesin verilere erişmesi mümkün olmamakla birlikte, farklı departmanların bünyesinde belirlenen erişim yetkilileri tarafından işlemlerin yapılması mümkün olmaktadır.

Teknik açıdan ortaya çıkan gelişmeler doğrultusunda gerekli önlemler bilgi işlem departmanları tarafından alınmakta, alınan önlemler teknik açıdan ortaya çıkan gelişmelerin hızına bağlı olarak belirli periyotlar halinde güncellenmekte, sair metotlar ve sızma testleri uygulanarak sistemin güvenliği kontrol edilmektedir. Veri Koruma Kurulu tarafından sızma testleri ya da diğer güvenlik tedbirleri ile ilgili olarak çeşitli düzenlemelerde bulunması ya da teknik açıdan belirlenen standartlara dair atıflarda bulunması durumunda oluşan yeni şartlara uyum gösterecek teknik çalışmaların yapılması, bilgi işlem departmanlarının sorumluluğundadır.

İşletmelerin bünyesinde oluşturulan bilgi işlem departmanları tarafından, işletmenin diğer birimleri üzerinden belirlenen yasal uygunluk prensiplerine uyumlu olarak yetkilendirme ve erişim ile ilgili teknik çözüm süreçleri hayata geçirilecek ve bu alanda Veri Koruma Kurulu tarafından yeni teknik standartların öne sürülmesi halinde standartlara uyum gösterecek yazılım ve donanımların geliştirilmesi ile çözüm süreçleri uygulamaya sokulacaktır. Bu alanda alınan tüm teknik tedbirler, belirli bir rutin halinde iç denetim mekanizmalarının işlemesi adına ilgili yetkililere ve kişisel veri sorumlusu olan ekibe bir rapor olarak sunulacaktır.

Yürütülmekte olan faaliyetler sırasında veri erişim yetkisi kapsamında yer alan tüm sistemlere, virüs koruma programlarının, sistem güvenlik duvarlarının, gereksinim

duyulan tüm yazılımların ve donanımların bilgi işlem departmanları tarafından kurulması gerekmektedir.

Sürecin en aktif birimleri içerisinde yer alan bilgi işlem departmanları kişisel verilerin erişimi ile ilgili olarak belirlenmekte olan prensipler çerçevesinde erişim yetkisine dair tanımlamaların yapılması, sistem içerisinde yer alan hesapların, yetkilerin ve cihazların belirli bir sınırlandırma ile kontrol altında tutulması gerekmektedir.

Departmanlara yönelik özelleştirilmiş prosedürlerin teknik önlemler çerçevesinde düzenlenmesi ve denetlenmesi ile ilgili süreçler, kişisel veri sorumlusu ekip, bilgi işlem birimi ve birim idarecileri tarafından yönetilmektedir.

Kişisel verilerin koruma altına alındığı sistemlere yönelik dışarıdan gelecek olası sızmaların önüne geçilmesi ve bu alanda ortaya çıkması muhtemel risklerin izlenebilmesi için gerek duyulan yazılımların ve donanımların kurulumunun gerçekleştirilmesi bilgi işlem departmanları tarafından yürütülmektedir. Bilgi işlem departmanları bu kapsamda sızma olup olmadığına dair testler yapmakta ya da yaptırmakta, olası veri kayıplarının önüne geçebilmek adına yapılacak yedekleme işlemleri sonrasında da benzer güvenlik önlemleri almakta, felaket durumuna dair yapılan planlamalar çerçevesinde çalışmaların yürütüldüğü üçüncü kişiler ile ilgili politikalar kapsamında ortaya çıkan tedbir unsurları uygulanmakta ve veri saklama faaliyetlerinin 6698 sayılı Kanununa uygun olması adına gerekli çalışmalar yapılmaktadır.

3.2 İnsan Kaynaklarının Kişisel Verilerin Korunmasındaki Rolü

İşletmelerde İnsan Kaynakları departmanları kişisel verilerin korunması ve ilişkili unsurlar ile ilgili çeşitli görevler ve ilkelere sahiptir. İnsan Kaynakları departmanı tüm personelinin KVKK ve kişisel verilerin hukuka uygun işlenmesi konusunda bilgilendirilmesi amacı ve sonrasında gerekli olacak dokümanları düzenleyerek her bir personeline ulaştırma ve gerekli eğitim faaliyetlerini düzenleme misyonuna sahiptir. Bununla birlikte insan kaynakları departmanının ilke ve misyonları bu başlık altında ortaya konulmuştur.

3.2.1 İnsan kaynakları departmanının kişisel verilerin korunması konusunda ilke ve görevleri

3.2.1.1 İlgilinin bilgilendirilmesi görevi

Elde edilen verilerin işleme sokulmasının öncesinde ve akabinde verilerin sahibinin mutlak suretle bilgilendirilmesi gerekmektedir. Bu bilgilendirmelerin yapılmaması durumunda, bireyler verileri üzerindeki kontrolü kaybetmiş olacaktır. Kişisel verilerin etkin bir şekilde korunması adına veri sahiplerinin kullanıma yönelik tam bilgiye sahip olması gerekmektedir (Yüksel, 2012:117). Verilerin işlenmesi sürecine yönelik olarak takip edilen dürüstlük ilkesinin de bir gereği olarak, verilerin işlendiğine dair sahiplerine bilgi verilmesi ve süreç içerisinde devamlı ve kapsamlı olarak bilgilendirilmesi gerekmektedir. Bu noktada iletişimde sürekliliğin sağlanması ile hem veri sahipleri bilgilendirilmiş olmakta hem de mevcut verilerin sağlıklı bir şekilde güncellenmesi sağlanmaktadır. Bir veri sahibinin verilerinin kullanması sürecinde bilgilendirilmesi gereken temel hususlar şu şekildedir (Karabulut, 2014:40-41):

- Verilerin işlenmesinde sorumlu olan kişinin ya da makamın kimliği;
- Veri kullanımının hangi amaçlar doğrultusunda gerçekleşeceği;
- Verilerin kim tarafından kabul edildiğine dair bilgiler;
- Bireylerin kendisine yöneltilen sorulara cevap verme zorunluluklarının olmadığının ve cevap vermesi ya da vermemesi halinde muhtemel olarak karşılaşacakları durumların aktarılması;
- Kendisine ait bilgiler hakkında devamlı bilgi alma özgürlüklerinin bulunduğu ve gerek duymaları halinde bu bilgileri değiştirebilecekleri.

Yukarıda da ifade edildiği üzere, bireylerin kendilerine ait bilgileri üzerinde işlem yapabilmesi, bu bilgilerin toplanabilmesi, depolanması, paylaşıma açılması vb. işlemlerin yürütülmesi sürecinde bilgilendirilmesinin temelinde yatan gereksinim, onayının alınması olarak ifade edilebilmektedir. Veri işleme süreçlerinde, bireylere kendisine ait hangi bilgilerin kullanılacağı, bu bilgilerin kullanım süreleri ve ne amaçla kullanılacağı ile ilgili olarak bilgilendirilmesi ve süreç içerisinde kullanabilecekleri temel hakların ve özgürlüklerin neler olduğunun bildirilmesi gerekmektedir. Burada ise dikkat edilmesi gereken bir husus vardır. Kişilerin kendisine dair verilerin neden, nasıl, ne zaman kullanılacağı ile bilgi verilmemesi halinde, kendi iradesi ile bu bilgilerin talep edilmesi gerekmektedir. Buna ek olarak bireylerin, verilerin

kullanmasına yönelik verdikleri onay aşamasında hür iradeleri ile hareket edebiliyor olmaları bir zorunluluk olarak ifade edilmektedir (Ayözger, 2016:120-121).

3.2.1.2 Veri güvenliğini sağlamak

Örgütlerin bünyesinde kurulan insan kaynakları departmanları tarafından, kişilere ait verilerin kullanım nedenlerinin, bu verilerin hangi koşullar altında saklanacağının mutlaka açıklanması gerekmektedir. Zira kişisel veriler, yaşanan doğal afetler, siber suçlar, bilgisayar ve depolama aygıtlarında meydana gelen hasarlar, ihmaller ve kötü niyetli kullanıcılar tarafından tehlike altında olabilmektedir. Yukarıda sayılan olumsuzlukların her birinin önüne geçebilmek adına önlemlerin alınması gerekmektedir. Bireyler ise istedikleri her an bu önlemlerin detayları ile ilgili bilgi alma hakkına sahip olmaktadır (Kılınç, 2012:1112).

Günümüz şartları içerisinde birçok işletme tarafından, veri güvenliği kavramı bir pazarlama unsuru olarak kullanılmaktadır. Birçok işletme tarafından veri güvenliği üzerinden yaşanacak sorunlara dair sorumluluklarının kabul edildiği beyan edilmiş ve mevcut yasal düzenlemeler haricinde, yaptırım kapsamında da müşterilerine belirli ödemelerin gerçekleştirileceği taahhüt edilmiştir. Birçok işletme bu alanda yürüttükleri politikalar üzerinden tüketicilerin güvenini kazanmaya çalışmaktadır. Ayrıca tüketici güveninin sağlanması işletmeler açısından bir rekabet avantajı olarak da değerlendirilmektedir. Bu durumda kişisel verilerin korunması aşamasında yaşanan aksaklıklar üzerinden işletmeler önemli zararlarla karşılaşmaktadır. Bu durumda işletmeler arasında verilerin işlenmesi durumunda dahi ortaya çıkabilecek zararların karşılanmasına yönelik sözleşmeler hazırlanmaktadır. Bu durumun temel nedeni ise, günümüzde verilerin dışarıya aktarılması halinde ortaya çıkabilecek sorunların net bir şekilde belirlenememesidir. ABD'de Ponemon Enstitüsü tarafından 2007 senesinde bir araştırma gerçekleştirilmiş ve bu araştırma neticesinde, işletme sahiplerinin verilerin sızdırılması sonrasında milyarlarca dolar zarar edebildikleri tespit edilmiştir. Bu bilgi Türkiye'de faaliyetlerini sürdürmekte olan alanında uzman Intellect işletmesi tarafından da kabul edilmektedir (Vural ve Sağıroğlu, 2010:72). Bu denli önem arz etmesine bağlı olarak, verilerin güvenliğinin sağlanması amacı ile hizmet veren işletmeler kurulmuştur.

3.2.1.3 Ölçülülük ilkesi

Kişisel verilerin elde edilmesi aşamasında sınırların belirlenmesi, ölçülülük ilkesi ile açıklanmaktadır. Bu ilke bazı kaynaklarda ise orantılılık ilkesi olarak ifade edilmektedir. İlkenin temelinde yatan ifade ise, hangi şartlar altında olursa olsun, verilerin yalnızca asgari seviyede toplanması gerekliliğidir. Bu ilke kapsamında verinin hangi seviyeye kadar gerekli olduğu belirlenmeye çalışılmaktadır. Öyle ki, dijital alemde bir uygulamanın dahi çalıştırılabilmesi için birçok iznin alınması gerekmektedir. Bu durum Mesut Serdar Çekin tarafından cep telefonlarındaki fener uygulaması üzerinden örneklendirilmektedir. Çekin tarafından, her uygulamada öncelikle erişim izinlerinin istendiğinin altı çizilmekte ve bu izinlerin arkasında yatan ilkenin ölçülülük olduğunu ifade etmektedir (Çekin, 2016:637).

Bu ilkenin etkinlik sağlaması neticesinde veriler ile kullanım amaçları arasında uygunluk sağlanmakta, amaçlara yönelik olarak verilerin toplanması aşamasında gereklilik bir şart olarak karşımıza çıkmaktadır. Aynı zamanda bu ilkenin varlığı ile, gereksiz bilgilerin toplanması ile ortaya çıkacak olan bilgi kirliliğinin de önüne geçmek mümkün olmaktadır. Bu ilke doğrultusunda elde edilen ve işlenecek olan her verinin gereksinim sınırları içerisinde olup olmadığına yönelik somut değerlendirmelerin yapılması gerekmektedir. Bu değerlendirme süreçleri içerisinde veri toplamanın başladığı anda ortaya çıkan amacın, devamında amaçta bir değişim olması durumunda ortaya çıkan yeni amacın ve bu amaçlar arasında herhangi bir bağlantının olup olmadığının değerlendirilmesi gerekmektedir. Bu değerlendirmeler neticesinde uygunluk durumunun varlığına kanaat getirilse dahi, ölçülülük durumunun süreklilik arz etmesi adına gerekli önlemlerin alınması gerekmektedir (Ayözger, 2016:126). Konu kapsamında söz konusu ilke ile ilgili olarak ise tartışmalar sürmeye devam etmektedir. Bu tartışmaların ortaya çıkmasının temel nedeni ise mevcut verinin gerekliliği ile ilgili değerlendirmelerin yoruma açık olabileceği endişedir. Mahkemeler tarafından dahi bu alanda farklı yorumların geliştirildiği önem verilmesi gereken bir durumdur (Kılınç, 2012:1130).

3.2.1.4 Sorumluluk ilkesi

Kişiler, kendilerine ait hangi verilerin elde edildiğini öğrenme, elde edilen verilerin kullanım amaçlarını öğrenme, bu verilerin saklanma sürelerini öğrenme ve tüm bunların sonucunda verilerin kullanılması ve zarar görmeleri halinde tazmin

edilmesini talep etme haklarına sahiptirler. Bu aşamada ise bir sorumlunun varlığı ile karşılaşılmaktadır. Öyle ki, bireylerin zarar görmesi neticesinde tazminat haklarını kullanabilmeleri için mahkemeye başvurması gerekmektedir. Burada sürecek davalarda ise bir sorumlunun var olması gerekmektedir. Bu aşamada ise birbirinden farklı görüşler ortaya çıkmaktadır. Çekin, konu ile ilgili olarak; "ilk olarak tazminat durumu ele alındığında kanun kapsamında yer alan mekanizmanın bir ihlal ya da kusur sorumluluğu halini kabul etmesi oldukça zor görülmektedir. Öyle ki, kanun koyucu tarafından da herhangi bir kusur şartı aranmamaktadır. Öyle ise kanun hükmünde yer verilen tazminat sorumluluğunun bir neden sorumluluğu olarak değerlendirilmesi çok daha uygun görülmektedir. Öyle ki, veri sorumlusu olan kimse, 6698 sayılı Kanunun 12'nci maddesinde de belirtilen şartları yerine getirmiş ise, sorumluluğun aynı kişiye yüklenmesi anlamlı olmamaktadır. Bu nedenle, kural açısından değerlendirildiğinde zarar meydana gelmiş ise, 12'nci madde de yer alan yükümlülüklerin yerine getirilmediği kabul edilmeli, ancak bu şartların hepsinin yerine getirildiğine dair veri sorumlusunun kanıt getirmesi halinde, kendisini aklamasına imkan tanınması gerekmektedir" ifadelerini öne sürmüştür (Çekin, 2016:637).

3.2.1.5 Amaçlara uygun süreçlerin takip edilmesi

İşletmelerin insan kaynakları departmanları tarafından kişisel veri yönetimine dair geliştirilen politikaların vazgeçilemez unsurları içerisinde amaca bağlılık unsuru yer almaktadır. Kişisel verilerin toplanması, işlenmesi ve güvenli bir biçimde saklanması ile ilgili olarak ortaya çıkacak olan amaçların önceden belirlenmesi gerekmektedir. Belirlenen amaçların ise güvenilir ve yasal dayanağının olmasına dikkat edilmelidir. Verileri paylaşacak kişilerin zihinlerinde soru işaretlerinin varlığına neden olmayacak şekilde amaçlar belirlenmeli, tüm ifadeler somut bir biçimde açıklanmalıdır. Bu ifadelerin somut bir şekilde ortaya koyulmaması süreç içerisinde veri sahiplerinin kontrollerini kaybetmesi anlamına gelmektedir (Kuşkonmaz, 2018:89).

Verilerin elde edilmesi ve işleme tabi tutulması sürecinde amaçlarda değişikliklerin meydana gelmesi halinde, doğrudan veri sahiplerinin onayı da geçersiz hale gelmektedir. Örnek vermek gerekirse, suç tespitinin yapılmasına yönelik olarak alınan bir DNA örneğinin herhangi bir başka amaç doğrultusunda kullanılması söz konusu değildir. Ancak yeni amaç ile eski amaç arasında belirgin bir ilişkinin var olması

neticesinde yeniden onay alma zorunluluğu ortaya çıkmamaktadır (Ayözger, 2016:123).

Elde edilen bir verinin kişiye belirtilme amacı haricinde kullanıma tabi tutulması halinde birtakım sosyal temelli problemlerle birlikte, verilerin suiistimal edilmesi riski ile de karşı karşıya kalınmaktadır. İşlendikleri amaçla bağlantılı, tahditli ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerinden taviz verilmemelidir. Örneğin, beyaz eşya mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi yasal amaç kapsamındayken, kan gruplarını işlemesi yasal amaç kapsamında değerlendirilmemesi gerekir.

Bu doğrultuda veri güvenliğinin gerçek anlamda sağlanabilmesi için amaç dışı kullanım unsurunun üzerinde önemle durulması gerekmektedir.

Bu aşamada, belirlenen amaçların yasal bir çerçeveye de sahip olması gerekmektedir. Yasal sınırlar içerisinde net bir şekilde ifade edilemeyen tüm unsurların hukuk dışı olarak değerlendirilmektedir. Bir amacın yasal sayılması için takip edilmesi gereken düzenlemeler ise 1995/46/EC VKD md. 7'de açıklanmıştır (Ayözger, 2016:125).

Başta amaca bağlılık ilkesi yer almak üzere, tüm ilkelerin benimsenmesi ancak veri güvenliğinin gerçek anlamda sağlanabilmesi ile mümkün olmaktadır. Bu durumda veri elde etme ve verileri saklama hakkını elinde bulunduran tüm departmanların, güvenlik alanında ortaya çıkması muhtemel riskleri belirlemesi ve bu risklerin en düşük seviyelere çekilebilmesi için gerekli önlemleri alması gerekmektedir. İlgili çalışmanın devamında da yer verileceği üzere, kişisel verilerin korunması ile ilgili olarak ortaya çıkan ilkelerin tamamı ulusal ve uluslararası alanda oldukça önemli benzerlikler içermektedir.

3.2.1.6. Kişisel Verilerin Korunmasında İnsan Kaynakları Tedbirleri

Bir işletmede görev yapmakta olan çalışanların, yasal sınırlar dışında verilere erişimin engellenmesine dair alınacak önlemlere ilgili olarak bilgilendirilmesi ve eğitim süreçlerine tabi tutulmaları insan kaynakları departmanı tarafından sağlanmaktadır. İşletmeler tarafından, hazırlanan kişisel veri envanterlerine erişimi ve veri işleme faaliyetleri ilgili personeller belirlenmek sureti ile sınırlandırılmaktadır. İşletme içerisinde veri işleme amaçlarına yönelik değerlendirmelerin neticesinde yetkili personellerin belirlenmesi ve veri işleme sorumlularının tüm verilere erişmesinin bir sistem kapsamında engellenmesi gerekmektedir.

Personel ve işletme arasındaki ilişkileri yürüten, söz konusu birlikteliğe dair çeşitli belgelerin düzenlemelerini yapan insan kaynakları birimleri tarafından, çalışanların kişisel verilerin işlenmesi sürecinde yasalara uygun olarak hareket etmesi, veri işleme ve erişim süreçlerinde KVKK kapsamında var olan yükümlüklerin bilincinde olması ve bu alandaki yükümlülüklerinin iş sözleşmelerinin son bulması halinde de devam ettiğinin belirtilmesi adına gerekli kayıtların ve belgelerin hazırlanması gerekmektedir.

Kişisel verilere erişim sürecinde izlenecek prensiplerin ve bu anlamda hazırlanacak dokümanların işletmede yer alan tüm bireylere insan kaynakları departmanları tarafından aktarılması ve çalışanlara yönelik bu alanda gerekli eğitimlerin verilmesi gerekmektedir.

3.2.2 İş ilişkisinde kişisel verilerin korunmasında insan kaynaklarının rolü

3.2.2.1 İşe alım sürecinde kişisel verilerin korunması

İşverenler, işyerlerinde kendisi adına çalışacak kimselerin belirlenmesi sürecinde birçok bilgiyi edinmek istemektedir. Bu alanda edinmek istenilen bilgiler adına çalışanlara ya da adaylara kimlik bilgileri, adres bilgileri, iletişim bilgileri, eğitim bilgileri, ceza mahkumiyeti, yakınlık bilgileri, sağlık bilgileri ile iş deneyimleri ve referansları ve askerlik durumu ile ilgili olarak çeşitli sorular yöneltebilmektedir. İşverenler tarafından çalışanlara ya da adaylara yöneltilecek olan soruların içeriğinin meslekleri ya da meslek yaşamları ile ilgisi olmaktadır (Löwisch vd., 2014:72-73; Okur, 2011:289-290; Eyrenci, 1991:250; Ertürk, 2002:66). İşveren tarafından yöneltilen sorulara çalışanlar tarafından verilen bilgilerin doğru olması ve bu doğrultuda işverenlerin yanlış yönlendirilmemesi gerekmektedir. Fakat çalışanın mevcut iş imkanının önüne geçmesi endişeni doğuran ve işin nitelikleri ile bağlantısı olmayan bir konu ile ilgili yöneltilen bir soruya yanıt vermemesi olağan bir durum olarak değerlendirilmektedir. Bu doğrultuda çalışanların kişisel verilerinin korunması ve işverenlerin sözleşme özgürlüğü arasında makul bir dengenin oluşturulması gerekmektedir (Uncular, 2014:71). Çalışanların kişiliklerinin ve özel yaşamlarının muhafaza edilmesi, çalışanlar kadar, işletmeye katılım gösterme niyeti olan adaylar içinde önem arz etmektedir. Bu nedenle iş sözleşmeleri adına gerçekleştirilen görüşmeler kapsamında başvuruda bulunan adaylara karşı verilerin korunması yükümlülüğü ile karşı karşıyadır. Buna ek olarak iş sözleşmesi esnasında adaylar ya da mevcut çalışanlardan dosyalarına eklenmek üzere talep edilen belgelerin de işletme

tarafından koruma altına alınması bir zorunluluktur. İşletme tarafından saklanması ve korunması gerekenler arasında; tıbbi muayene raporları, personellere yöneltilen soru bilgileri, yetenek sınav sonuçları yer almaktadır (Okur, 2011:289-290). Aday tarafından iş görüşmesi esnasında verilen belgelerin, iş sözleşmesinin yapılmaması durumunda adaylara iade edilmesi bir zorunluluktur.

Bununla birlikte, Facebook, Twitter, Instagram, LinkedIn gibi sosyal medya hesapları üzerinden işe alım sürecinde işverenlerce referans araştırması yapılması uygulamada tartışılan konular arasındadır. Bir kısım uygulamacılar bunu hukuka ve etik ilkelere aykırı bulmakta ve sosyal ağ sitelerinde adaylar hakkında verilen mevcut bilgilerin, ayrımcılığa yol açabileceğini savunmaktadırlar. Bu tez sahipleri, sosyal medya üzerinden online inceleyen işverenlerin adayları seçerken; kılık kıyafet, cinsel yönelim, ırk, din, evlilik durumu, yaş ve politik görüşlerine göre bir tercihte bulunabileceklerini ileri sürerken bunun aksini düşünen diğer bir kesim ise, eğer ilgili kişi profil bilgilerini alenileştirmiş ise, burada bir mahremiyet sorunu olamayacağını eğer isteseydi ilgili kişinin bunu teknik olarak gelişmiş gizlilik ayarları vasıtasıyla kısıtlayabileceğini ileri sürüyorlar. Her iki görüşün haklılık yönü olmakla birlikte burada asıl olan objektif iyi niyet kuralarına uygun hareket edilmesidir.

Hemen ifade etmemiz gerekirse, iş başvurusunda bulunan adaylarla ilgili işverenlerin Facebook, Twitter, Instagram, LinkedIn gibi sosyal medya hesapları üzerinden profil bilgilerini inceleyerek işe alıma karar vermelerini yasaklayan herhangi bir kural da bulunmamaktadır.

- Özel Hayat ve Kişisel Duruma İlişkin Sorular

İş görüşmesi için gelen adayların daha önceki yapmış olduğu işten aldığı ücretin öğrenilmek istenmesi, yalnızca işin nitelikleri doğrultusunda söz konusu bilginin alınmasının bir gereksinim olması durumunda anlaşılır olabilmektedir. Doktrinde yer alan bir görüş doğrultusunda; adayın iş sözleşmesinde yeni iş yerinden alacağı ücretin en düşük sınırının bir önceki iş yerinde aldığı ücret olarak koşul şeklinde belirtmiş olması durumunda, adayın kötü bir niyetle bu soruya doğru olmayan bir bilgi vermesi durumunda söz konusu sözleşmenin fesih edilebileceği öne sürülmektedir (Odaman, 2002:41). Bu alanda ortaya çıkan bir diğer görüş doğrultusunda ise bu durumun bir fesih nedeni olmaması gerektiği, ücret konusunda yürütülen pazarlık süreci içerisinde daha yüksek bir ücret elde etmek isteyen adayın izlediği bir strateji olarak

değerlendirilmesi gerektiği öne sürülmektedir (Uncular, 2014:74). Ancak bu doğrultuda, sınırlamalardan bağımsız olarak daha yüksek bir ücret elde etmek amacı ile eski ücretin beyan edilmesinin işverene sözleşmeye dair fesih hakkını doğurduğu görüşü öne çıkmaktadır. Bu duruma dair bir yorumda bulunmak gerekirse; sözleşme kapsamında yürütülen ücret görüşmelerinde adayların daha yüksek bir ücret elde etmek adına gerçek dışı bilgi vermeleri olağan bir durumdur. Zira, ücret görüşmeleri karşılıklı beyanların aktarımı sonrasında uzlaşarak belirlenmektedir. Bu nedenle söz konusu durum bir fesih nedeni oluşturmamaktadır. Buna karşılık sözleşmede eski ücret bilgisinin doğru verilmesinin bir esas olduğu ifade edilmekte ise, olası bir yanıltıcı bilgi fesih hakkını ortaya çıkarmaktadır. Öyle ki konu ile ilgili olarak 4857 sayılı İş Kanunundaki düzenlemeye bakıldığında, *"İş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri için gerekli vasıflar veya şartlar kendisinde bulunmadığı halde bunların kendisinde bulunduğunu ileri sürerek yahut gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işçinin işvereni yanıltması*" fesih hakkı olarak ifade edilmiştir (m.25/II-(a)). Adayın başvuru yaptığı pozisyonun doğrudan para ile ilişki olması (muhasebecilik, veznedarlık vb.) halinde, adayın özel yaşamı ile ilgili olmasına karşılık malvarlığına dair soruların yöneltilmesi olağan bir durum olarak değerlendirilmektedir (Kaplan, 2004:379). Bunların haricinde para ile ilişkili olmayan bir pozisyon için başvuruda bulanan adaya malvarlığı ile ilgili soru sorulması durumunda yanıtlamaması mümkündür (Uncular, 2014:75).

Adaylara evliliğe dair düşüncelerinin öğrenilmesi amacı sorulan sorularda kural olarak uygun kabul edilmemektedir. Öyle ki, evlilikte bireylere verilmiş olan kişisel bir hak olarak değerlendirilmektedir. İşletmeler tarafından bu sorunun yöneltilmesi karşısında adayların doğru olmayan bilgiler aktarmasının hukuksal bir sonucu bulunmamaktadır (Aydınlı, 2004:30). İşverenler tarafından adaylara çalışma saatleri dışında tütün, alkol gibi yasal maddeleri kullanma durumunun sorulması da söz konusu değildir (Sevimli, 2008:155-156). Bu alanda yöneltilen sorular kişilik haklarına bir saldırı olarak görülmese de aday tarafından verilen doğru bilgiden kaynaklı bir şekilde işe alımın gerçekleşmemesi ayrımcılık yasağına aykırı bir durum olarak değerlendirilmektedir.

- Sağlık Durumuna İlişkin Sorular

Adaylara yöneltilecek sağlık alanında soruların ise içeriğinin yalnızca mevcut pozisyona uygun olup olmadığının değerlendirilmesi, iş sağlığı ve güvenliğine dair hükümlerin yerine getirilmesi ve adayların sosyal yardımlardan faydalanma

durumlarının tespit edilmesine dair olması gerekmektedir ve bu doğrultuda adaylardan belge istenmesi de mümkündür (Sevimli, 2008:127). Bu alanda doktrinde tartışılan bir diğer konu ise, kadın adaylara hamile olup olmadıklarının sorulmasına yöneliktir. Bu alanda ilk olarak başvurulan pozisyonun niteliklerine bağlı olmaksızın hamilelik durumu ile ilgili soru yöneltilebileceğine karar veren Alman Federal İş Mahkemesi; ilerleyen süreç içerisinde kadın ve erkek çalışanlar arasında ayrım yapılmasının önüne geçme amacı ile Alman Medeni Kanunu madde 611'in kabul edilmesi ile birlikte bu alanda yöneltilecek bir sorunun, cinsiyet ayrımına neden olan unsurlar olarak değerlendirilmeye başlanmıştır. Burada ortaya çıkan istisnai durum ise, başvuru yapanların tamamının kadın olmasıdır. Zira, başvuruyu yapan herkesin kadın olması durumunda herhangi bir cinsiyet ayrımcılığından bahsetmek mümkün değildir. Türkiye'de de doktrin kapsamında farklı yaklaşımlar bulunmaktadır. Bu alanda ortaya çıkan görüşlerden birinde, adayların başvuru yaptıkları pozisyonun niteliklerinden bağımsız olarak adayın hamilelik halinin işveren için bir külfet olması nedeni ile bu sorunun yöneltilebileceği öne sürülmüştür (Sözer, 1982:1051). Diğer bir görüş doğrultusunda ise, başvurulan işin nitelikleri ile doğrudan ilişkili olması halinde (sahne sanatçılığı, antrenörlük, mankenlik vb.) adaya bu yönde bir sorunun sorulması mümkündür ve adayların bu durumda yanıltıcı bilgi vermemesi gerekmektedir. Ancak, başvuruda bulunan pozisyonla bir ilgisinin olmaması halinde hamilelik durumunun sorulması kişilik haklarına bir saldırı olarak değerlendirilmektedir (Sevimli, 2008:154). Bu görüşe paralel bir diğer yaklaşım doğrultusunda ise iş yerinin özellikleri ve işin nitelikleri bir gereklilik ortaya çıkarmadığı sürece kadın çalışanlara bu yönde sorulan sorular, cinsiyet ayrımcılığını ortaya çıkarması nedeni ile geçersiz kabul edilmektedir (Eyrenci, 1991:254-255). Konuyla ilgili öne sürülen uluslararası düzenlemelere bakıldığında da iş yerinin özellikleri ve işin nitelikleri gerektirmediği sürece çalışanlara hamilelik hakkında soruların yöneltilmesi eşitlik ilkesine aykırı olarak değerlendirilmektedir. Bu alanda öne çıkan çalışmalar arasında yer alan, BM Kadınlara Karşı Her Türlü Ayrımcılığın Ortadan Kaldırılması Sözleşmesi de hamilelik ile ilgili soruların yöneltilmesi cinsiyet ayrımı olarak kabul edilmektedir (Uncular, 2014:77).

Bu duruma yönelik bir değerlendirme yapmak gerekirse; işin nitelikleri ve iş yerinin özelliklerinden doğan gereksinimler doğrultusunda hamilelik durumuna yönelik bir sorunun yöneltilmesinde işverenlerin haklı menfaatleri ön plana çıkmaktadır. Öyle ki,

bu durumun yalnızca çalışan tarafından değerlendirilmemesi gerekmektedir. Sonuçta sözleşme ile bağlı olarak işverenlerin çalışanları gözetme borcu nedeni ile bu bilgi önem arz etmektedir. Zira hamilelik durumuna bağlı olarak iş sözleşmesinin düzenlenmesi sonrasında çalışma esnasında yaşanacak bir sorun karşısında işverenlerin sorumluluğu bulunmaktadır. Ancak, çalışanın hamile olduğunun bilinmesi durumunda ise, işveren tarafından çalışana çok daha hafif bir iş verilmesi ya da izne ayrılması konusunda yardımcı olması mümkün olabilmektedir. Bunlara ek olarak hamilelik durumuna dair bilginin olması durumunda, çalışana ya da adaya mevcut işin hamilelik ile ilgili risklerine dair bilgilendirmenin yapılması da mümkün olmaktadır. Bu nedenle bu alanda yöneltilecek soruların kişilik haklarına saldırı olarak değerlendirilmesi çok doğru değildir.

İşin gereksinimleri doğrultusunda çalışanlara ya da adaylara sağlık durumları ile ilgili soruların da yöneltilmesi mümkündür. Öyle ki, işin niteliğine uygunluğun değerlendirilmesi amacı ile işveren tarafından sağlık sorunlarına dair sorular yöneltilmesi makul bir durumdur. Hatta işe uygunluğun kontrol edilmesi adına çalışanların belirli sağlık kontrollerine yönlendirilmesi de mümkündür (Kaplan, 2004:378-379). Bunlara ek olarak çalışanın ya da adayın doğrudan çalışmasını etkilemese dahi, işyerinde çalışmakta olan diğer çalışanların sağlık durumlarını tehlikeye sokabilecek bir bulaşıcı hastalığın var olup olmadığına dair çalışanların mutlak suretle işverenleri bilgilendirmesi gerekmektedir (Ertürk, 2002:68). Örnek vermek gerekirse özellikle sağlık kuruluşlarına iş başvurusunda bulunan kişilerin mevcut hastalık durumları hakkında mutlaka gerçek bilgileri aktarması gerekmektedir.

Bu durumda bir değerlendirme yapmak gerekirse; başvuruda bulunduğu bir işle doğrudan bağlantılı bir rahatsızlığı olan çalışan ya da adayın, işverenini mevcut durumla ilgili olarak gerçekçi bir şekilde bilgilendirmesi gerekmektedir. Öyle ki, adayın ya da aktif çalışanın tedavi edilmesi mümkün olmayan ya da bulaşıcı özellikleri olan bir hastalığa sahip olmaları ile işverenin bilgi sahibi olmasında haklı bir menfaat bulunmaktadır. İş sözleşmesi yapılmadan evvel, adaya sağlık durumu ile ilgili birtakım soruların yöneltilmiş olması halinde, adaydan herhangi bir sağlık belgesi istenmemiş ya da sağlık kontrolüne tabi tutulmasına karşılık, adayın doğrudan beyanları doğrusunda bir sözleşme yapılması ve sonrasında hastalık durumunun ortaya çıkması haklı bir fesih nedeni olarak değerlendirilmektedir. Çalışanların işleri ile ilgili hastalık risklerine dair bilgilendirilmesi, meslek hastalıklarına dair işverene yüklenen

sorumluluklar açısından da işverenlerin çıkarına uygun bir durumdur. İşverenler tarafından, mevcut iş faaliyetlerine bağlı olarak ortaya çıkan hastalık halinden kaynaklı tedavi masraflarının karşılanması, söz konusu meslek hastalıklarına bağlı olarak geçici ya da sürekli iş göremez durumuna gelinmesinden gelir kaybı ya da gider artışına bağlı olarak belirli bir gelirin garanti altına alınması, özet olarak bu sorunla karşılaşan çalışana gelir yardımı yapılması gerekmektedir. Bunlara ek olarak olası bir meslek hastalığı işverenlere iş gücünün kaybolması, iş sürecinin aksaması gibi olumsuzluklar olarak geri dönmesi ile birlikte yasal sorumluluklarından doğan nedenlerle çeşitli cezai yaptırımlarla karşılaşma riskini de ortaya çıkarmaktadır.

- Eski Hükümlülüğe Yönelik Sorular

İşletmelere çalışmak için başvuran bir adayın sabıka durumunun sorgulanabilmesi adına, geçmişte olsa var olan bir hükümlülük halinin bulunması ve bu halin doğrudan başvurulan pozisyonun nitelikleri ile ilişkili olması gerekmektedir. Ancak işin niteliği ile bağlantılı olmasına karşılık, adayın sabıkasının sicil kaydından silinmesi halinde, aday tarafından herhangi bir sabıkasının bulunmadığını beyan etmesi kabul edilebilir bir durumdur (Eyrenci, 1991:256; Uncular, 2014:78; Ertürk, 2002:71). Bu durumdan bağımsız olarak, örnek vermek gerekirse şoför olarak işe alınacak bir adaya trafik suçunun olup olmadığı ya da işletmenin mali departmanlarında görev yapacak bir adaya herhangi bir mali suçunun olup olmadığının sorması olağan bir durum olarak değerlendirilmektedir (Eyrenci, 1991:255). Bu alanda Yargıtay tarafından alınmış kararlar doğrultusunda; adayların, başvurulan pozisyonun niteliklerinden bağımsız olarak sabıka durumuna dair doğru bilgiyi vermemiş olması haklı bir fesih neden olarak değerlendirilmektedir. Nitekim 6698 sayılı Kişisel Verilerin Korunması Kanunu da sabıka kaydı (adli sicil) özel nitelikli (hassas) kişisel veri olarak kabul etmiştir (m.6). Bu verilerin, başkaları tarafından öğrenilmesi durumunda ilgili kişinin mağdur olabileceğine ya da ayrımcılığa maruz kalabileceğini kabul etmekte ve bu nedenle bu tür veriler özel nitelikli veri olarak nitelendirilmektedir.

- Sendika Üyeliğine Yönelik Sorular

İş görüşmelerinin yapıldığı esnada adaylara, sendika üyeliğinin olup olmadığının sorulması yasal sınırlar içerisinde yer almamaktadır. Öyle ki bireylerin sendikal özgürlükleri AY. m.51 ve 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun 25 inci maddesi doğrultusunda güvence altına alınmıştır. Bu nedenle mevcut

düzenlemeler çerçevesinde iş sözleşmelerinin hazırlanmasında adayların sendika üyeliklerine göre karar verilmesi söz konusu değildir. Nitekim 6698 sayılı Kişisel Verilerin Korunması Kanunu da dernek, sendika, vakıf ve gurup üyeliklerini özel nitelikli (hassas) kişisel veri olarak kabul etmiştir (m.6).

- Dini İnanç ve Siyasi Görüşe Yönelik Sorular

İş görüşmeleri ve sonrasında sözleşmelerin hazırlanması aşamasında adaylara dini inançları, politik yaklaşımları ile ilgili olarak soru yöneltilmesi mümkün değildir. Bu durum AY.m.15/2, 24, 25 çerçevesinde güvence altına alınmıştır. Bu madde de yer alan "kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz" ifadeleri oldukça açıklayıcıdır. 6698 sayılı Kişisel Verilerin Korunması Kanunu kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, özel nitelikli (hassas) kişisel veri olarak kabul etmiştir (m.6).

3.2.2.2 İş sözleşmesinin devamında kişisel verilerin korunması

- İş Sözleşmesi Devam Ederken Edinilen Bilgiler

Adaylara dair bilgiler işverenler tarafından ancak sözleşmenin devamında mutlak suretle gerekli olması durumunda kullanılabilmektedir. Sözleşme sonrasında çalışana dair düzenlenecek bir bilgide yalnızca işin gereklilikleri doğrultusunda bilgiler yer alabilmektedir. Bu tür belgelerin hiçbirinde çalışana dair kişisel bilgilerin yer alması mümkün değildir. Süreç içerisinde de işverenler tarafından çalışanların özel yaşamlarına kesinlikle müdahale edilmemesi, başvuru sürecinde alınan bilgilerin alınmaması ve çalışanların özel yaşamlarına dair bilgilerin bir üçüncü kişi ile paylaşılmaması gerekmektedir (Kaplan, 2004:45; Ertürk, 2002:127).

Ancak iş süreçlerinde birtakım edimlerin ifa edilebilmesi adına çalışanlara ait kişisel verilerin kullanılması gerekliliği ortaya çıkabilmektedir. Çok basit bir örnek ile çalışanların iş süreçleri sonrasında ödemelerinin yapılabilmesi adına sigorta sicil numaralarına, iban numaralarına gereksinim duyulabilmektedir (Sevimli, 2008:125).

Bazı hallerde ise, yasal düzenlemelerden kaynaklı olarak çalışanlara ait kimi verilerin de işyerinde saklanması ve gerek duyulması durumunda ilgili kurumlara aktarılması gerekmektedir. Örnek vermek gerekirse 4857 sayılı İş Kanunun 75. maddesi doğrultusunda işverenler tarafından çalışanlara dair özlük dosyalarının düzenlenmesi,

çalışanlara ait kimlik bilgileri ile birlikte kanundan doğan belgeleri ve kayıtları bulundurmak zorundadır. Resmî kurumlar tarafından talep edilmesi halinde işverenler tarafından gösterilmesi gerekmektedir (Sevimli, 2008:123). İşverenler tarafından, gerekli durumlarda kullanılmak üzere çalışanların kimlik bilgilerinin, becerilerini verimlilik düzeylerinin bilgisayar ortamlarında saklanması kural olarak mümkün görülmektedir. Bu doğrultuda söz konusu bilgilerin kullanılması için çalışanların rızasının alınması ve aktarımın sağlanacağı üçüncü kişilerin haklı çıkarlarının bulunması gerekmektedir (Aktay vd., 2013:150-151). Aktarımı sağlanacak bilgilerin yalnızca çalışanların iş süreçleri ile ilgili bilgileri ve tutumları ile ilgili olması gerekmektedir.

Kimi zaman iş sözleşmelerinin devam ettiği esnada, herhangi bir bilgi edinme arayışı olmaksızın işverenler tarafından birtakım bilgilerin elde edilmesi mümkün olmaktadır. Örnek vermek gerekirse çalışanın işyerinde unuttuğu herhangi bir sağlık belgesinin incelenmesi neticesinde hastalık haline dair istemeden de olsa bir bilgi edinilebilmektedir. Öğrenilen hastalık bilgisinin, çalışanın performansı ve diğer çalışanların sağlık durumları ile ilgili bir risk unsurunu doğurmaması halinde söz konusu bilgilerin 3.kişilere aktarılmaması gerekmektedir (Sevimli, 2008:146). Fakat elde edilen bilgi neticesinde çalışanın performansının düşeceğinin ya da diğer çalışanların sağlık durumlarının riske atılacağının öğrenmesi halinde, bu durum sözleşmeye dair haklı bir fesih hakkını ortaya çıkarmaktadır. Böyle bir durumun ortaya çıkması durumunda çalışanlar ve işverenler arasında muhtemel bir çıkar çatışmasının doğacağı öngörülmektedir. İşveren ve işletmeler adına çıkarların muhafaza edilmesine yönelik olarak söz konusu bilgilerin kullanılması kanuna aykırı bir durum olarak değerlendirilmemektedir. Çalışanlara dair e-devlet şifrelerinin talep edilmesi de hukuksal açından uygun bir durum olarak değerlendirilmemektedir. Öyle ki, e-devlet şifresinin talep edilmesi çalışanların görevleri, işi ya da işin ifası ile alakalı bir durum değildir (Uncular, 2014:94; Alp, 2014:127).

- İş Sözleşmesi Süresince Çalışanların İşyerine Giriş ve Çıkış Denetimi

Çalışanların iş yerlerine giriş çıkışları işletmeler tarafından farklı yöntemler üzerinden kontrol altında tutulmaya çalışılmaktadır. Bunlar içerisinde; imza defterleri, akıllı kartla parmak izi, manyetik kimlik kartları ve retina taraması gibi uygulamalar yer almaktadır (Okur, 2011:111). Söz konusu uygulamaların işverenlerin yönetimsel yetkileri içerisinde değerlendirilmesine karşılık, uygulama esnasından kimi

durumlarda kişisel verilerin korunmasına aykırı durumlar ortaya çıkabilmektedir. Buradan hareketle, işverenlerin yetkileri ve çalışanların kişilik hakları arasında etkili bir denge mekanizmasının oluşturulması gerekmektedir. Bu uygulamaların, yalnızca işverenlerin meraklarından kaynaklanması doğru değildir. Güvenlik düzeyinin üst düzeyde olması gerektiği durumlarda ya da çalışanların mesai durumlarının başka bir şekilde takip edilmesi mümkün olmadığı durumlarda, çalışanlarında rızasının alınması şartı ile retina ya da parmak izi odaklı takip sistemlerinin uygulanması mümkündür (Uncular, 2014:95). Burada kişilik haklarına müdahaleyi haklı kılan temel unsurlar ise; işverenin üstün haklı menfaatleri, çalışma alanının güvenliğinin sağlanması, konut dokunulmazlığı, mülkiyet haklarının korunması ve çalışanların mesai sürelerinin belirlenmesi olarak sıralanabilmektedir (Okur, 2011:116).

Hukuki açıdan söz konusu takip programlarına dair doğrudan bir çalışma bulunmamaktadır. Ancak İstanbul Tabip Odası Hukuk Bürosu'nun parmak izi uygulamalarına dair yapmış oldukları çalışmalar neticesinde fiziksel belirleyici olması nedeni ile kişisel veri olarak kabul edilmesi gerektiğini ileri sürmüşlerdir (Uncular, 2014:95). Bu alanda Danıştay tarafından verilen karar doğrultusunda da parmak izi kişisel veri olarak değerlendirilmektedir. Bu nedenle çalışanların parmak izlerinin alınabilmesinin dayanağında hukuki bir unsurun bulunması gerekmektedir. Yargıtay tarafından verilen karar doğrultusunda ise; *"El izi alma işleminin işçi bakımından kişisel verilerin başkasının eline geçmesi kaygısına sebep olmasına ve bu durumun çalışma şartlarında esaslı değişiklik niteliğinde olduğunun kabulünün gerekmesi karşısında feshin haklı sebebe dayanmadığının anlaşılmasına, ancak işverenin işyeri güvenliğini sağlamak amacı ile bu değişikliğe gittiği ve geçerli olduğu, dolayısıyla davacının bu eylemi sebebiyle yapılan feshin haklı değil fakat geçerli sebebe dayanmasına göre, ...kararın onanmasına karar verildi."* İfadeleri konuya dair önemli bir karar olarak değerlendirilmektedir (akt. Manav, 2015:126-130).

- İş Sözleşmesi Süresince Çalışanların İzlenmesi ve Gözetlenmesi

Gelinen noktada çalışanlar teknolojide meydana gelen gelişmeler ve internet kullanımının getirdiği imkanlardan yalnızca iş süreçlerine yönelik olarak faydalanmamaktadır. Çalışanların mesai saatleri içerisinde illegal müzik, film indirmesi, pornografik ve ırkçı içerikleri olan siteleri ziyaret etmesi, sanal sohbet programlarında vakit geçirmesi ve genel olarak iş dışı etkinliklerle çalışma saatlerini geçirmeleri işverenlerin karşısına çıkan yeni bir risk unsuru olarak

değerlendirilmektedir (Savaş, 2009:97). Söz konusu durumların ortaya çıkması iş gören ve işveren arasındaki ilişkide güven sorunlarının ortaya çıkmasına neden olmaktadır. Bu durumda bir gereklilik olarak; çalışanların performanslarının denetlenmesi ve kontrol altında tutulması, yasal sorumluluklar ve güvenlik endişelerinden kaynaklı olmak üzere internet kullanımının, e-posta akışının hatta telefon görüşmelerinin dahi gözetlenmesi ve denetlenmesi durumunun ortaya çıkmasına neden olmaktadır. İş sözleşmesi sonrasında, çalışanların telefonlarının dinlenmesi, yapmış oldukları görüşmelerin kayıt altına alınması, internette ziyaret ettiği sitelerin izlenmesi, çalışma saatleri içerisindeki davranışlarının sesli ve görüntülü olarak kayıt altına alınması gibi durumlar kişisel verilere ulaşma olasılığını ortaya çıkardığından kişilik haklarına yapılan haksız bir saldırı olarak değerlendirilebilmektedir. Yapılan tüm kayıt, izleme, gözetleme ve denetleme etkinliklerinin özel hayata müdahale sınırları içerisinde kalması için mutlaka hukuksal bir dayanağın varlığına ihtiyaç duyulmaktadır. Bu nedenle söz konusu takip eylemlerinin hayata geçirilmesi adına mutlak suretle işverenler için ekonomik olarak haklı bir menfaatin bulunması ve çalışanların takip edilmelerine yönelik rızalarının alınmış olması gerekmektedir (Küzeci, 2010:283). Söz konusu haklı nedenlerin tamamının objektif ve gerçek nitelikli olması gerekmektedir. Örnek vermek gerekirse, işletmenin bilgisayar sistemlerinin virüs riskine karşı korunması açısından çalışanların bilgisayarlarının izlenmesini kabul etmesi, sadakat borucundan kaynaklanan bir gereksinim olarak değerlendirilmektedir. Benzer bir şekilde işletme içerisinde hırsızlık vakalarının artması sonrasında çalışanların kendisinin de izlenmeye rıza göstermesi de sadakat borcu kapsamında değerlendirilmektedir (Aktay vd., 2013:151). Bu konuda Anayasa Mahkemesinin 2016 yılında verdiği bir karar da "İşverenin, çalışanın kurumsal bilgisayar ve e-posta adresini kişisel amaçla ve işyeri düzenlemelerine aykırı olarak kullanıp kullanmadığını doğrulamak amacıyla kontrol edebilir" yönünde karar verdi (AYM/24.03.2016).

Bu doğrultuda bir işletme içerisinde çalışanların görüntülü kayıt cihazları ile bilgileri dahilinde izlenmesi ancak işyeri güvenliğinin sağlanması amacı ile gerçekleştirilebilmektedir. Gizli kayıt işlemlerinin yapılabilmesi için ise işveren tarafından sonradan ispatlanabilir bir şüphenin var olması gerekmektedir. Söz konusu koşulların var olmadığı durumlarda sözleşmelerin feshi amacı ile açılan davalarda, mevcut kayıtların delil olarak mahkemeye sunulması mümkün değildir (akt. Hekimler,

2011:433). İşyerlerinde çalışanların genel hareketlerinin izlenmesi amacı ile alınan görüntülü kayıtların ise hukuki bir dayanağı bulunmamaktadır. Öyle ki, işveren tarafından gerçekleştirilen ve dayanağı olmayan izlemeler, haklı menfaat unsurlarını içermemektedir (Aktay vd., 2013:150-151; Hekimler, 2011:584-585). Bir diğer ifade ile çalışanların mücbir nedenler olmadıkça gizli kameralar aracılığı ile izlenmesi ya da telefon görüşmelerinin dinlenmesi kişilik haklarına bir saldırı olarak değerlendirilmektedir (Kaplan, 2004:51). Zira çalışanların sürekli çeşitli cihazlarla izlenmesi ve denetlenmesi, üzerlerinden oldukça yoğun bir baskının doğmasına neden olarak birtakım psikolojik sorunlar yaşamalarına neden olabilmektedir. Bu konuda Yargıtay 12 nci Ceza Dairesinin 2013 yılında verdiği bir karar da "Yasal savunma ile ilgili olarak, kendisine karşı yapılan saldırıya ilişkin başka türlü delil elde etme imkanı bulunmadığı bir durumda ses ve görüntüsünün kayda alınması hukuka aykırı değildir" (Y12.CD.2013/14958).

Kimi işletmelerde çalışanların mesai saatlerinin denetimi amacı ile giriş ve çıkış saatlerinin kaydedildiği ya da performanslarının çeşitli biyometrik metotlarla veya kamera sistemleri ile izlendiği ve buradan elde edilen verilerin saklandığı görülmektedir. Bu durum, çalışanın her hareketinin izlenmesi nedeni ile kişilik haklarına bir saldırı olarak değerlendirilmektedir. Bu doğrultuda işyerlerinde çalışanların izlenmesi noktasında belirli bir dengenin sağlanması ve çalışanların izleme etkinlikleri ile ilgili mutlak suretle bilgilendirilmesi gerekmektedir (Küzeci, 2010:285). Bir işyerinde elektronik izlemenin yapılabilmesi için var olması gereken üç koşul bulunmaktadır. Bunlar; işverenin haklı menfaatleri, çalışanların onayı ve hukuksal dayanaktır (Okur, 2011:86). Bunlara ek olarak yapılan bu işlemlerde, işverenlerin bilgi edinme hakları ve çalışanların kişilik haklarının korunması arasında sağlıklı bir dengenin kurulması gerekmektedir. Bu durumda çalışanların izlenmesi sürecinde tercih edilen yöntemlerin belirli bir sınırın dışına çıkmaması gerekmektedir. Bu nedenle işletmelerin bu eylemlerine yönelik ölçülülük denetimlerinin yapılması ve işveren tarafından bilgi edinme hakkının dürüst bir şekilde kullanıldığının denetlenmesi gerekmektedir (Löwisch vd., 2014:73). Konuyla ilgili 2017 tarihinde Danıştay 11 inci Hukuk Dairesi tarafından verilen bir karar da "Olayda, personelden kişisel veri alınması kapsamında olan "yüz tanıma sistemi" ile mesai takibi uygulamasının, kamusal alanda da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu açık olup, dava konusu işlem tarihi itibarıyla uygulamanın sınırlarını usul

ve esaslarını gösteren bir yasal dayanağın bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında, yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmayan dava konusu işlemde ve davanın reddi yolundaki mahkeme kararında hukuka uygunluk bulunmamaktadır" (Danıştay,11HD, 13.06.*2017* tarih ve E.*2017*/816, K.*2017*/4906).

İşyerlerinde çalışanların iş dışı internet kullanımını ve haberleşmelerinin engellenmesi amacı ile bilgisayarların ve internet kullanımının işverenler tarafından denetlenmesi mümkündür. Örnek vermek gerekirse, çalışanların işletme bilgisayarı tarafından göndermiş olduğu e-postaların ve söz konusu e-postaların kime aktarıldığının, işletme güvenliğinin sağlanması amacı ile kontrol edilmesi olağan bir durumdur (Sevimli, 2008:201). Bu alanda Yargıtay tarafından verilen kararlara da bakıldığında, çalışanların işyerindeki bilgisayarları ve interneti özel işleri için kullanmaları haklı bir fesih nedenini ortaya çıkarabilecek bir durum olarak değerlendirilmiştir. Bu durumda söz konusu kullanımın, işverenin menfaatlerine aykırılık oluşturup oluşturmadığının anlaşılması adına çalışanların gözetim altında tutulabileceği ifade edilmektedir. Öyle ki, işverenlerin açıkça ya da örtülü bir şekilde rızası olmaksızın internet ve bilgisayarların kişisel amaçlarla kullanılması kural olarak yasaktır. Bu alanda bir iznin var olması halinde de sınırsız bir kullanım hakkı elde edilmemektedir. İşverenler tarafından açık bir ifade ile özel amaçlarla internetin kullanılması haklı bir fesih hakkı olarak değerlendirilmektedir. Benzer bir şekilde pornografik ya da illegal içeriklerin işletmenin veri taşıyıcılarına indirilmesi durumunda da herhangi bir ihtara gerek duyulmaksızın sözleşmelerin feshi mümkün olmaktadır. Bunlara ek olarak geçerli ve mücbir bir neden olmadıkça çalışanlar tarafından özel telefon görüşmelerinin yapılması da haklı bir fesih nedeni olarak kabul edilmektedir. Fakat bu noktada çalışanların söz konusu kurala dair mutlaka daha önceden bilgilendirilmesi gerekmektedir. Bu alanda haklı fesih nedeni olarak Yargıtay kararlarına konu olmuş ve tartışılmaya devam eden unsurlar ise; davalı konumda olan çalışanın e-posta üzerinden diğer çalışanları da işverene karşı durmaya teşvik etmesi, işletmenin yazılım programları ile ilgili olarak şahsi bilgisayarında birtakım bilgilerin yer alması, işverene ait donanımların kullanılması sureti ile işletmeye ait birtakım bilgilerin üçüncü kişilere aktarılması olarak sıralanabilmektedir (Manav, 2015:126-130). Nitekim Yargıtay verdiği bir kararında "Dosya kapsamına göre davacının görevi gereği işverenin işlerini

yürütmesi için kendisine verilen bilgisayar ve e-*mail* adreslerini kullanarak iş akdi daha önce feshedilen S. A. ile işle ilgili olmayan elektronik yazışmalar yaptığı, bu yazışmalar sırasında işverenin şahsına yönelik hakaret niteliğinde sözler sarf ettiği işyeri sırrı sayılabilecek konularda da yazışmalar yaptığı anlaşılmıştır. İşverenin kendisine ait bilgisayar ve e-*mail* adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisi bulunmakladır. Davalı işverene ait bilgisayarları ve e-*mail* adreslerini özel yazışmalarda kullanıp işverene hakaret niteliğinde sözler sarf etmenin, işveren açısından 4857 sayılı Yasanın 25 II-b. maddesi uyarınca sataşma niteliğinde haklı fesih nedeni oluşturacağı anlaşılmakla davacının ihbar ve kıdem tazminatı taleplerinin reddi yerine yazılı gerekçe ile kabulü hatalı olup bozmayı gerektirmiştir". Denilmek suretiyle işverene ait bilgisayarları ve e-*mail* adreslerini özel yazışmalarda kullanıp işverene hakaret niteliğinde sözler sarf etmenin haklı feshi gerektirdiğini hüküm altına almıştır (Y9HD.13.12.2010 T., E.2009/447, K.2010/37516 Legalbank).

Konu ile ilgili olarak Köln Eyalet İş Mahkemesi tarafından alınan bir karar doğrultusunda; çalışanların işletmeye ait bilgisayarları kullanmaması ile ilgili olarak açık bir bilgilendirmenin yapılmadığı hallerde, çok yoğun bir özel kullanım olmasına karşılık, çalışana bir ihtarda bulunmadan evvel sözleşmenin feshi söz konusu olmamaktadır. Bu mail kullanımının içeriğinde üste yönelik olumsuz ifadeler olsa dahi, üstün bilgi edinmesi amacı ile yazılmamış olması nedeni ile de aynı durum geçerli olmaktadır (Hekimler, 2004:225-226). Aynı mahkeme tarafından verilen bir başka karar doğrultusunda ise; işveren tarafından işletme telefonlarının ve internet bağlantısının özel amaçla kullanılamayacağı ile ilgili net bir yasaklamanın yapılmamış olması durumunda, telefon ve internet kullanımında herhangi bir sakınca görülmemektedir (Hekimler, 2004:225-226). Benzer bir durumda Nürnberg Eyalet İş Mahkemesi tarafından verilen bir karar doğrultusunda ise; özel amaçlı internet kullanımının işveren tarafından kesin bir şekilde yasaklanmasına karşılık, çalışanlar tarafından kullanılması bir fesih nedeni olarak değerlendirilmiştir (Hekimler, 2004:309-310).

Hukuksal açıdan değerlendirildiğinde çalışanların gizli bir şekilde izlenmesi ve çalışma saatlerinde davranışlarının gözetlenmesi kural olarak uygun görülmemektedir. Bu süreç içerisinde çalışanların mutlak suretle bilgilendirilmesi gerekmektedir. Doktrin içerisinde yer alan bir görüş doğrultusunda; çalışanlar hangi şart altında olursa olsun işverenler tarafından izlenmesi uygun olmayan bir durum olarak

değerlendirilmiştir. Kolluk birimlerinin dahi dinleme yapabilmek adına bir yargı kararına gereksinim duyduğu şartlar içerisinde işverenlere böyle bir hakkın tanınması kabul edilebilir değildir. Bu noktada, güvenlik gerekçesinden bağımsız olarak, çalışanların onayı alınsa dahi işveren tarafından çalışanların izlenmesinin kişilik haklarına bir saldırı olarak değerlendirilmesi gerekmektedir. Çalışanların bilgilendirilmesi amacı ile işyeri giriş ve çıkışlarına mesai saatlerinin kontrolü amacı ile kamera yerleştirilmesi mümkündür. Ancak, örnek vermek gerekirse çalışanların doğrudan çalışma masalarını gören bir alana kamera yerleştirmek sureti ile hareketlerinin gün içerisinde takip edilmesi hukuka uygun bir durum değildir (Sevimli, 2008:205). Zira günlük yaşamının önemli bir kısmını işyerlerinde geçirmekte olan çalışanlar açısından kendilerinin izlenmesi, hareketlerinin baskılanması noktasında özel yaşama müdahale olarak değerlendirilebilmektedir.

Çalışanların iş süreçlerinde performanslarının değerlendirilmesi, işyerlerinde iş sağlığı ve güvenliği ile ilgili belirlenen kurallara uygun davranılıp davranılmadığının denetlenmesi vb. nedenler doğrultusunda çalışma alanlarının görüntülü kayıt sistemleri ile izlenmesi mümkündür. Fakat söz konusu izlemenin süreklilik arz etmesi, çalışanların özel hareketlerinin de izlenmesine yol açacağından özel yaşama bir müdahale olarak değerlendirilebilmektedir. Bu doğrultuda izlemenin belirli periyotlar halinde yukarıda ifade edilen haklı nedenler doğrultusunda gerçekleştirilmesi gerekmektedir (Aydınlı, 2004:120).

- Çalışanlara Ait Bilgilerin Yeni İşverenlerle Paylaşılması

Çalışanların iş sözleşmeleri devam ederken farklı bir işyerinde çalışmak üzere başvuruda bulunması durumunda, çalışanın yeni işvereninin çalışanın onayı olmadan çalışanın eski işvereninden kendisi ile ilgili bilgi almaması gerekmektedir. Şayet, çalışan eski işverenini referans listesinde göstermiş ise bu durumda bilgi alınması için onay verdiği anlaşılmaktadır (Ertürk, 2002:75). Adayın izni olmaksızın yeni işverenin eski işverenden kendisi ile ilgili bilgi alması ve bu bilgiler doğrultusunda iş görüşmelerinin olumsuz sonuçlanması durumunda çalışan, culpa in contrahendo (sözleşmenin kurulmasından önce, henüz görüşmeler safhasında tarafların, kusurlu davranışlarıyla birbirlerine verdikleri zararlardan sorumluluğu) doğrultusunda yeni işverenden tazminat talep edebilmektedir.

3.2.2.3 İş sözleşmesinin bitiminden sonra

Sözleşmenin bitmesi ile birlikte, işverenlerin iş sözleşmesi kapsamında çalışanlara ait verilerin saklanmasına ve üçüncü kişilere verilerin aktarılamamasına dair sorumluluğu devam etmektedir. Bu süreç içerisinde eski çalışanların özlük dosyalarının da belir bir süre de olsa saklanması işverenlerin de lehine olabilmektedir. Öyle ki, mesai ücretleri, fazla ücret vb. beş yıllık zamanaşımı olan davalarla karşılaşılması halinde söz konusu dosyalar, işverenlere ispat kolaylığı sağlayabilmektedir. Fakat söz konusu dosyada yer alan bilgilerin çalışanın rızası alınmaksızın kullanılmaması gerekmektedir. Sonuç olarak iş sözleşmesi sona erse dahi işverenlerin eski çalışanlarına dair belgeleri ve bilgileri saklaması ve üçüncü kişilerle paylaşmaması gerekmektedir. Buna ek olarak yeni işverenlerin de çalışanın onayı olmaksızın eski işverenden kendisine dair bilgileri talep etmemesi gerekmektedir. Çalışanın eski işyeri ile iş sözleşmesinin sona ermesi sonrasında yeni iş başvurusu yapması ile birlikte eski işverenden kendisine dair bilgilerin istenmesi ya da çalışma belgesinin düzenlenmesi halinde aktarılan bilgilerin yanıltıcı olmaması gerekmektedir. Söz konusu belgelerde ya da bilgi aktarımlarda gerçek dışı verilere yer verilmesinin bir sonucu olarak çalışanın yeni iş yerine alınmaması durumunda, eski işverene yönelik tazminat davası açma hakkı doğmaktadır (Manav, 2015:129). Öyle ki, eski işveren tarafından düzenlenen çalışma belgelerinin içeriğinde yalnızca yapılan işin niteliklerinin, çalışanın yeterliliklerinin ve çalışma süresinin yer alması gerekmektedir. Nitekim Yargıtay 9.Hukuk Dairesi konuyla ilgili verdiği bir karar da "Yargılama sırasında dinlenen tanıklar ve sunulan deliller değerlendirildiğinde, içerisinde özel yazışmaların, davacının bir kısım senede bağlı tutarları eski işyerine ödeyeceğine dair taahhüdünü içeren işten ayrılma dilekçesi ve ödeme dekontlarının olduğu işyeri "*özlük dosyasının"* yeni çalıştığı işverenine gönderilmesi eyleminin davacıyı rahatsız etme, onu doğruları söylemeyen bir kişi olarak gösterme amacı taşıdığı, bu olay sonrası davacının iş sözleşmesinin feshinin gündeme geldiği ancak buna engel olunduğu, yaşanan olay nedeniyle davacının manevi yönden etkileneceği açık olup bu nedenle manevi tazminata hak kazandığının kabulü gerekir" denilmek suretiyle eski işverenin hukuka aykırı olarak kişisel veri içeren özlük dosyasını yeni işverenle paylaşmasından dolayı manevi tazminata hükmetmiştir (Y9HD.14.4.2016 T., E.2014/37215, K.2016/9418 Legalbank).

4. İŞLETMELERDE KİŞİSEL VERİLERİN KORUNMASINDA İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ ROLÜNE YÖNELİK ÖZEL SEKTÖR İŞLETMELERİ ÖRNEK OLAY ÇALIŞMALARI

4.1 Araştırmanın Amacı ve Önemi

Teknoloji ve özellikle de iletişime dair araçların ve unsurların gelişmesi ile birlikte, veri ve belgelerin korunması önemli bir konu haline gelmiştir. Bu bağlamda hem uluslararası hem de ulusal kurumlar veriler ve verilerin korunması üzerinde çeşitli yaptırımlar getirmişlerdir. Bilgi ve bilişim toplumunda kişisel verilerin hem toplum hem de kişilerin kendisi adına zarar verecek, kötü niyetli ya da rıza alınmadan kullanılması önemli sorunlar meydana getirmektedir. Bu durumun ortadan kalkması ve kişisel verilerin mevzuata uygun biçimde saklanması ve korunması noktasında işletmelerde İnsan Kaynakları ve Bilgi İşlem Departmanlarının nasıl önlemler alabileceği ve konunun neresinde olduklarının ortaya konulması gelecekteki veri güvenliği açısından da oldukça önemli bir konudur. İşletmelerde insan kaynağının yönetimi ve teknolojinin entegre olduğu süreçleri yöneten iki departmanın kişisel veriler konusunda ortaya koyduğu faaliyetlerin diğer birimlerden daha etkin sonuçlar ortaya çıkarttığı düşünülmektedir. Bu amaçla çalışmada; kişisel verilerin korunması hususundaki adımlarının anlaşılmasının ve geliştirilebilmesinin veri güvenliği açısından önemli sonuçlar doğurması nedeniyle insan kaynakları ve bilgi işlem departmanlarının bu süreçteki rolü, önemi ve sorumlulukları vurgulanmaya çalışılmıştır.

4.2 Araştırmanın Yöntemi

Bu çalışmada örnek olay yöntemi kullanılmıştır. Genel olarak örnek olay (vaka) yönteminin seçilmesinde etkili olan sebepler; araştırmada nasıl ve niçin sorularının cevaplarının aranması, araştırmacının araştırmaya konu olan olay ve bulgulara etkisinin az olması veya hiç olmaması ve araştırma konusunun tarihsel olmayıp güncel olması durumudur (Yin, 2009; Aktaran: Arslan, 2018:22). İşletmelerde kişisel verilerin korunmasında insan kaynakları ve bilgi işlem departmanlarının rolüne

yönelik özel sektör işletmeleri örnek olay çalışmaları nitel bir araştırma özelliği taşımaktadır. "Nitel araştırmalar gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırmalardır" (Yıldırım ve Şimşek, 2008:39).

Bu araştırmada kişisel verilerin mevzuata uygun biçimde saklanması ve korunması noktasında işletmelerde insan kaynakları ve bilgi işlem departmanlarının nasıl önlemler alabileceği ve konunun neresinde olduklarının ortaya konulması amacıyla örnek olay yöntemi olarak uygun bulunmuştur.

Bu araştırmada örnek olay incelemelerinin yapıldığı işletmelerde; kişisel verilerin mevzuata uygun biçimde saklanması ve korunması noktasında işletmelerde insan kaynakları ve bilgi işlem departmanlarının nasıl önlemler alabileceği ve konunun neresinde oldukları ayrıntılı bir şekilde incelenmiştir.

Bu çalışmada tek bir örnek olay(vaka) araştırması yerine çoklu örnek olay yöntemi tercih edilirken, bu amaçla da çoklu örnek olay yönteminin avantajlarından yararlanılmıştır. Bu durum şöyle ifade edilebilir: "Tek bir örnek olay üzerinden yapılan araştırma, hatalara daha açık olma, verilerin örnekleme özel, sübjektif olma ihtimali, genelleme yapmaya karşı zorluklar, çalışmanın kalitesine dair problem ihtimali gibi riskler taşmaktadır" (Eisenhardt ve Graebner, 2007; Aktaran: Arslan, 2018:24).

Örnek olay çalışmalarında birden fazla örnek olay ile ilgili araştırma yapılması; ayrı özellikteki işletmeler hakkında ayrıntılı bilgilere ulaşım sağlaması nedeniyle sadece birkaç benzer kalıpta birbirini tekrar eden veriler değil, tamamıyla bağımsız deneyimler ve veri setlerine ulaşmayı sağlamaktadır (Yin, 2009; Aktaran: Arslan, 2018:24). Bu sayede daha yüksek bir evreni temsil yeteneği ve daha fazla bir örneklemden veri elde edilmesi mümkün hale gelmiş olacaktır (Arslan, 2018:24).

Dolayısıyla çoklu örnek olay analizinde sayı kaç olmalıdır? Eisenhardt, (1989) bu sayının 4 ile 10 arasında olmasının isabetli olacağını yazmıştır. İlave edilen her bir örnek olay ile beraber öğrenme eğrisinin azalıp arttığına araştırmacı bakarak, yeni veri setlerine ulaşımın ihmal edilir derecede düşük olduğunu düşündüğü yere kadar araştırmacı yeni örnek olayları araştırmasına dâhil etmelidir. Bu sayı, araştırmanın doğası gereği duruma göre araştırmacı tarafından süreç içinde de belirlenebilecektir

(Aktaran: Arslan, 2018:25). Çalışmamızda iki işletme örnek olay çalışması çerçevesinde incelenmiştir.

Bu araştırmada hipotez sunulmaması nedeniyle hipotezlerin testi söz konusu olmadığı gibi, nitel ve tümevarım yöntemi ile yapılan değerlendirmeler bu çalışmanın doğası gereğidir (Arslan, 2018:25).

4.3 Örneklem

Örnek olay incelemesi ve çalışmasında işletme seçiminde, ülkemizin önde gelen köklü, alanında oldukça tecrübeli, ölçek olarak büyük işletme olarak ifade edilen birisi tekstil diğeri de gıda sektöründen olmak üzere iki işletmesi ele alınmıştır.

4.4 Veri Toplama Aracı

Özel sektör işletmeleri örnek olay çalışmasında, toplam iki farklı işletmede araştırma yapılmış olup, görüşme, gözlem, dokümanlar ve raporlar bilgi kaynağı olarak kullanılmıştır. Yapılan saha çalışmasında işletmelerin insan kaynakları ve bilgi işlem departmanlarının yöneticileri ile mülakat yapılmış ve projeleri, politikaları ve kurumları analiz edilmiştir. Özel sektör işletmeleri örnek olay çalışmasında en çok tercih edilen veri toplama yöntemleri doküman ve kayıtların incelenmesi ile mülakat ve gözlemlerden oluşmaktadır. Bu kapsamda çalışmamızda toplanan veriler, yüz yüze yapılan görüşmelerden, işletmelerin uygulamalarından, web sitelerinden ve dokümanlarından oluşmaktadır.

Görüşmelerin tamamı görüşülenlerin izni ile kayıt altına alınmıştır.

Saha çalışmamızda aşağıdaki sorulara cevap bulmaya çalışılmıştır:

- İşyerlerinin hangi amaçla ve hangi tür verileri işledikleri?
- Kişisel veri işleme şartları ve ilkeleri?
- Kişisel Veri Politika ve Prosedürlerinin uygulama biçimi?
- Kişisel Verilerin Korunması için hangi tür idari ve teknik tedbirleri aldıkları?

Saha çalışması modeli üç aşamadan oluşmaktadır.

- Mevcut durum analizi,
- Uygulanan strateji ve politikaların tespiti,

- Sonuç, değerlendirme ve öneriler.

4.5 Verinin Analizi

Örnek olay çalışmasına dahil edilen işletmeler bağımsız olarak ele alınmıştır. Araştırmanın amacına ulaşmak üzere her işletmeye ait veriler kendi içinde ayrı ayrı değerlendirmeye tabi tutulmuştur. Her bir işletmeye ait farklı örnek olay raporu oluşturulmuştur. Daha sonra işletmelere ait bağımsız örnek olaylar ve bunların verileri arasında karşılaştırmalar yapılması yoluyla değerlendirmeler yapılmış ve çeşitli sonuçlar ortaya konmuştur (Eisenhardt, 1989; Arslan, 2018:29).

4.6 Verinin Geçerliliği ve Güvenirliliği

Örnek olay yöntemi; gözleme ve deneyime dayalı bir yöntem olması nedeniyle araştırmanın kalitesinin en üst düzeye çıkarılması amacıyla genellikle dört tip test uygulanmaktadır. Bunlar sırasıyla; İç geçerlilik, dış geçerlilik, yapısal geçerlilik ve güvenirliktir. Kısaca bu dört tip testi açıklamakta fayda bulunmaktadır (Yin, 2009; Aktaran: Arslan, 2018:30).

Verinin iç geçerliliğinin sağlanması amacıyla verinin analizi sırasında alternatif veya karşı açıklamalar değerlendirilmiştir. Verinin dış geçerliliğinin sağlanması amacıyla analitik olarak veriler analiz edilmiş ve analitik genellemelere ulaşılmıştır. Üstelik iki işletmede örnek olay yapılmış olması karşılaştırmalar yapılmasına imkân vermiş olup tekrar eden sonuçlara ulaşılması sayesinde genellemelerin geçerliliği güçlendirilmiştir. Bununla beraber, burada genelleştirme nicel araştırmalarda olduğu gibi örneklemden evrene genelleme şeklinde değil ve fakat vakaya özel yapılmış analitik genelleme ile var olan teoriler arasında yapılmıştır (Yin, 2009; Aktaran: Arslan:2018:30).

Yapısal geçerliliğin sağlanması amacıyla birden çok veri kaynaklarından faydalanılmış, verinin doğruluğu kanıtlanmış ve her bir vaka ile alakalı görüşülmüş anahtar kişilere kendi işletmeleri ile ilgili rapor inceletilmiş ve doğrulanmıştır Güvenirlilik, bir araştırmayı başka bir araştırmacı da yapsa aynı sonuçlara ulaşabilmesi demektir (Yin, 2009; Aktaran:2018:31). Güvenirliliğin sağlanması amacıyla, her bir vaka ile alakalı veriler toplanmış, saklanmış ve veri bankasına kaydedilmiştir. Ayrıca görüşme notları, araştırma notları muhafaza edilmiş, görüşmeler ilgili kişinin izni ile kayıt altına alınmıştır.

4.7 Örnek Olay (Vak'a Çalışmaları)

4.7.1 İşletme-1 İmalat San. ve Tic. A.Ş.

4.7.1.1 İşletme-1 hakkında genel bilgiler

64 yıldır tekstil sektöründe faaliyet gösteren ve entegre bir tesis olan İşletme-1 İmalat San. ve Tic. A.Ş kuruluşu, Çerkezköy/Tekirdağ da halı ve iplik üretimi yapmaktadır. Türkiye'de CE sertifikasına sahip ilk tufting halı üreticisi olan işletme ülkemizin en büyük markaları arasında yer almakta ve tesislerinde duvardan duvara halı üretimi yapmaktadır. Ayrıca Türkiye'nin dört bir tarafına yayılmış olan bayi ağı ile hizmet vermektedir.

İşletme-1 İmalat San. ve Tic. A.Ş, kaliteli çalışma olgusu ile birlikte çevreyi koruyan, iş sağlığı ve iş güvenliğine önem veren yönetim anlayışını benimsemiştir. İşletme bu konuda uluslararası geçerliliği olan "Oeko-Tex Standard 100" belgesine sahiptir. Geniş ürün yelpazesi, yenilikçi yaklaşımı ve isabetli yatırımları ile dünya markası olma yolunda emin adımlarla ilerlemektedir.

İplik ve halı imalatı yapan ve yaklaşık 600 işçi istihdam eden, tekstil sektöründe tehlikeli sınıfta faaliyet gösteren İşletme-1 İmalat San. ve Tic. A.Ş, işletmesi entegre bir tesistir.

İşletme-1 İmalat San. ve Tic. A.Ş, 'nin misyon, vizyon ve değerleri aşağıdaki şekilde belirtilmiştir:

Vizyon;

- Büyümek
- Marka Olmak
- Kurumsal Yönetim Standartlarını Oturtmak
- Rekabetçi Olmak
- İnovatif
- Müşteri Odaklılık

Misyon;

Müşteri memnuniyetini ön planda tutarak, her kesimden tüketici beklentilerine cevap vermek.

Değerler;

- Kanunlara ve yasal düzenlemelere titizlikle uymak,
- İş ahlakı prensiplerine sahip çıkmak,
- İşte şeffaflık ilkelerine bağlı kalmak,
- Emeğe ve insana değer vermek,
- Çok çalışmak.
- İşletme-1 San. ve Tic. A.Ş.'nin Veri İşleme Amacı

İşletme-1 İmalat San. ve Tic. A.Ş. işyeri çalışanlarının, çalışan adaylarının, stajyerlerinin, tedarikçilerinin ve alt işverenleri ile alt işveren çalışanlarının, müşterilerinin ve ziyaretçilerinin kişisel verilerini amaca uygun, amaçla bağlantılı ve ölçülü bir şekilde işlemektedir. Nitekim işlenen kişisel veriler;

- Kurumsal sürdürülebilirlik faaliyetlerinin planlanması ve icrası,
- Etkinlik yönetiminin sağlanması,
- Tedarikçilerle olan ilişkilerin yönetiminin sağlanması,
- Alt İşverenlerle olan ilişiklerin sürdürülebilmesi,
- Personel ihtiyacının karşılanması sürecinin yürütülmesi,
- Risk yönetimi işlemleri ile Finansal raporlama ve takibi,
- Hukuk işlerinin takibi,
- Kurumsal iletişim faaliyetlerinin organizasyonu,
- Kurumsal yönetim faaliyetlerinin uygulanması,
- Şikâyet ve talep yönetiminin sağlanması,
- Yetkili kurum ve kuruluşlara ilgili mevzuat hakkında bilgi verilmesi,
- Ziyaretçi kayıtlarının oluşturularak takibinin sağlanması,
- Kanundan kaynaklanan yükümlülüklerin yerine getirilebilmesi,

amacıyla işlenmekte ve güvenli bir şekilde saklanmaktadır.

4.7.1.2 İşletme-1 İmalat San. ve Tic. A.Ş.'nin veri işleme ilkeleri

Kişisel Verilerin Korunması Kanunu m.4'de kişisel verilerin işlenmesine ilişkin usul ve esaslar 108 sayılı Sözleşmeye ve 95/46/EC sayılı Avrupa Birliği Direktifine eşgüdüm biçiminde düzenlenmiştir. Bu kapsamda; İşletme-1 İmalat San. ve Tic. A.Ş. işyeri 6698 sayılı Kanunda belirtilen kişisel verilerin işlenmesine esas ilkelere uygun olarak aşağıda gösterilen şekillerde veri işlemektedir.

- Dürüstlük kurallarına ve hukuka uygun olma:

İşletme-1 İmalat San. ve Tic. A.Ş.; kişisel verilerin işlenmesinde yasal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda İşletme-1 İmalat San. ve Tic. A.Ş. Kişisel verilerin işlenmesinde orantılılık gerekliliklerini nazarı dikkate alarak, kişisel verileri amacına uygun bir şekilde kullanmaktadır.

- Verilerin doğru ve gerektiğinde güncel olması:

İşletme-1 İmalat San. ve Tic. A.Ş.; veri sahiplerinin temel haklarını ve kendi yasal çıkarlarını nazarı dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını temin etmek amacıyla bu yönde gerekli tüm tedbirleri almaktadır. Örneğin, ilgili işletme tarafından; kişisel veri sahiplerinin kişisel verilerini düzeltme ve doğruluğunu teyit etmelerine yönelik olarak yeterli bilgilendirme yapılarak bu konuda gerekli prosedürleri hazırlamıştır.

- Belirli, açık ve legal amaçlar doğrultusunda işlenme:

İşletme-1 İmalat San. ve Tic. A.Ş. hukuka uygun olarak legal veri işleme amacını açık ve net olarak ortaya koymaktadır. İşletmede yürütülmekte olan ticari faaliyetlerle ilintili ve bunlar için gerekli olan kadar kişisel veri işlenmektedir. Veri sorumlusu olan işverence henüz kişisel veri işleme faaliyetine başlanmadan önce kişisel verilerin hangi amaçla işleneceği belirlenmektedir.

- Verinin işlendiği amaçla ilintili, ölçülü ve tahditli olması:

İşletme, verileri, amacıyla bağdaşmayan ve belirlenen amaçların gerçekleştirilebilmesine uygun bir şekilde işlemekte veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden imtina etmektedir. Örneğin, sonradan ortaya çıkması ihtimal dahilindeki ihtiyaçların karşılanması amacıyla veri işleme faaliyetinde bulunmamaktadır.

- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme:

İşletme-1 İmalat San. ve Tic. A.Ş. kişisel verileri sadece mer'i mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Bu kapsamda, ilgili işletme öncelikle mer'i mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini belirlemekte, bir süre belirlenmişse bu süreye uygun hareket etmekte, bir süre belirlenmemişse işyerinin ihtiyaçlarını nazarı dikkate alarak, verilerin işleme amacına uygun süre kadar saklamaktadır. İşletme tarafından belirlenen saklama sürenin sona ermesi ya da işlenmesini gerektiren nedenlerin ortadan kalkması durumunda veriler işletme tarafından yok edilmekte, silinmekte ya da anonim hale getirilmektedir. Gelecekte kullanma olasılığı olabilir düşüncesi ile işletme tarafından kişisel veriler saklanmamaktadır.

4.7.1.3 İşletme-1 İmalat San. ve Tic. A.Ş.'nin veri işleme şartları

6698 sayılı Kanunun m.5'de kişisel verilerin işlenme şartları sayılmış olup, buna istinaden aşağıdaki hallerden en az birinin varlığı halinde, kişisel verilerin işlenmesi mümkün olabilecektir.

- Veri sahibi açık onayının varlığı:

İşletme işyerinde iş başvurusu aşamasından başlamak üzere ilgili kişiler Kişisel Verilerin Korunması Kanunu kapsamında öncelikle aydınlatılmakta ve işlenen kişisel verileri konusunda açık rızaları usulüne uygun bir şekilde alınmaktadır. Örneğin iş başvurusu yapan çalışan adaylarının iş başvuru formlarında bu konuda aydınlatma ve onay metni bulunmaktadır. Çalışanlardan ise, bilgilendirme ve onay formu ile açık rıza yazılı olarak alınmaktadır. İşyerine gelen ziyaretçiler güvenlik girişine asılan aydınlatma metinleri ve yaka kartlarına yazılan metinler ile aydınlatılmaktadır. Nitekim güvenlik girişine asılan yazı içeriğinde, "Bu işyerine girişte ilettiğiniz kimlik bilgileriniz Kişisel Verilerin Korunması Kanununa uygun olarak güvenli bir şekilde saklanmakta yasal yükümlülükler dışında veri sahibinin izni olmadan bir başkasıyla paylaşılmamaktadır" ibaresi bulunmaktadır.

- Kanunlarda açıkça öngörülmesi:

İşletme, Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza hükümleri ile ilgili verilerini (sabıka kaydı) işyeri güvenliği için işe alım sürecinde talep etmektedir.

İSG Kanunu'na istinaden işe giriş periyodik sağlık raporu talep edilmektedir. İş Kanunu'na göre yazılı olarak imzalanması gereken iş sözleşmesi imzalanmaktadır.

- Rızasına hukuki geçerlilik tanınmayan kişinin ya da kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunmasının zorunlu olması ya da fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda olması:

İşletmede vuku bulacak bir iş kazasında kazazede işçinin kimlik bilgileri işletmenin konuyla ilgili yetkilisi tarafından götürüldüğü hastanede sağlık görevlileriyle paylaşılmaktadır.

- Bir sözleşmenin oluşturulması veya ifasıyla direkt ilgili olması şartıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin lüzumlu olması:

İşveren işe aldığı işçilerle yazılı olarak iş sözleşmesi yapmakta ve bunu İş Kanunu m. 8'e dayandırmaktadır. Ayrıca işveren, tedarikçileri, alt işverenleri ve müşterileri ile de yasal menfaatleri doğrultusunda sözleşme imzalamaktadır. Nitekim alt işverenlerle yazılı olarak imzalanan "Alt işverenlik Sözleşmesi" 4857 sayılı Kanunun 2 nci ve Alt İşverenlik Yönetmeliği'nin 9 uncu maddesine dayanmaktadır.

- Veri sorumlusu olan işletmenin yasal yükümlülüğünü yerine getirebilmesi için zorunlu olması:

İşveren tarafından işçilere aylık ücret ödenebilmesine esas olan, banka hesap numarası, işçinin medeni durumu, bakmakla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı ile ilgili bilgiler içeren Aile Durum Bildirimi istenmekte ayrıca daha önce başka bir işyerinde çalışması varsa mevcut SGK sicil numarası gibi kişisel verileri talep edilerek işlenmektedir. Bununla birlikte 1774 sayılı Kimlik Bildirme Kanunu gereğince işe giren veya çıkan işçilerin kimlik bilgilerini 3 gün içinde işyerinin bağlı bulunduğu kolluk birimlerine bildirerek kişisel verilerini hukuki yükümlülüğünü yerine getirmesi amacıyla paylaşmaktadır.

- İlgili kişinin kendisi tarafından alenileştirilmiş olması halinde:

İşletmeye iş başvurusu yapan çalışan adaylarının iletişim, kimlik ve eğitim bilgileri, iş başvurusu yapılmasına imkân veren internet sitelerinde (kariyer.net, secretcv. gibi) yayımlanması halinde, işe alım sürecinin yönetilmesi amacıyla işlenmektedir.

- Bir hakkın korunması veya kullanılması için veri işlemenin zaruri olması halinde:

İşletme, ispat niteliği taşıyan işçiye ait güvenlik bilgi ve belgelerini (sabıka kaydı, güvenlik soruşturma belgeleri gibi) polis, jandarma ve istihbarat birimlerinin talep etmesi halinde paylaşmaktadır.

- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun legal çıkarları için veri işlenmesinin mecburi olması halinde:

İşletme, işyerine ait bina ve tesislerde, işçilerin sağlık ve güvenliği ile işyeri güvenliğinin sağlanması amacıyla, güvenlik amaçlı kamera kaydı yapmaktadır. Bu konuda kamera izleme politikası oluşturulmuş olup, izlemeyle ilgili çalışanlar, stajyerler, ziyaretçiler, müşteriler, tedarikçiler ve alt işveren çalışanları bilgilendirilmektedir. Bilgilendirme her kameranın altına "Bu işyeri 7/24 saat kamera ile izlenmektedir" biçiminde bilgilendirme levhaları asılmaktadır. Ayrıca işçilerin iş sözleşmesine bu konuda hükümler konulmaktadır.

4.7.1.4 İşletme-1 İmalat San. ve Tic. A.Ş.'de işlenen kişisel veri sınıfları

İşletme-1 İmalat San. ve Tic. A.Ş.'de; işletmenin hukuka uygun ve yasal kişisel veri işleme amaçları nazarı dikkate alınarak, 6698 sayılı Kanunu'nun m.5'de öngörülen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve tahditli olarak, başta kişisel verilerin işlenmesine dair m.4'de açıklanan düsturlar başta olmak üzere Kanunda belirtilen genel ilkelere ve düzenlenen bütün yükümlülüklere uyularak ve "Kişisel Verilerin Korunması Politikası" kapsamındaki çalışanlar, çalışan adayları, stajyerler, alt işveren çalışanları, ziyaretçiler, müşteriler, tedarikçiler ve üçüncü kişiler tahditli olarak aşağıda belirtilen sınıflandırmadaki kişisel verileri, Kanun m.10 gereğince veri sahiplerinin bilgilendirilmesi kaydıyla işlenmektedir.

Çizelge 4.1: Kişisel Veri Sınıflaması

Kişisel Veri Sınıfları	Açıklama
Kimlik Bilgileri	A-İmalat San. Tic. A.Ş. tarafından işlenen kimlik bilgileri (adı-soyadı, TCKN, anne ve baba adı, doğum yeri ve tarihi, cinsiyet gibi bilgileri içeren ehliyet, pasaport no, SGK No, imza bilgisi, araç plakası v.b. bilgiler
İletişim Bilgileri	A-İmalat San. Tic. A.Ş. işvereni çalışanların başta olmak üzere ticari ilişki içerisinde olduğu kişilerin adres, telefon, e-mail, IP adresi ve faks numarası ve gibi iletişim bilgilerini

Çizelge 4.1 (devam): Kişisel Veri Sınıflaması

Kişisel Veri Sınıfları	Açıklama
Lokasyon ve Seyahat Bilgileri	A-İmalat San. Tic. A.Ş.'de tüm departmanlarca yürütülen iş organizasyonu kapsamında, firmanın ürün ve hizmetlerinin kullanımı sırasında veya iş birliği içerisinde olduğu kişi ve kuruluşların işletme araçlarını kullanırken bulunduğu mevkiinin konumunu tespit eden bilgiler; küresel konumlama sistemi ile seyahat bilgileri v.b.
Aile Bireyleri ve Yakın Bilgileri	A-İmalat San. Tic. A.Ş.'de tüm departmanlarda çalışanların, stajyerlerin, iş başvurusu yapanların, alt işveren çalışanlarının yasal çıkarlarını korumak amacıyla anne, baba, eş ve çocuktan oluşan aile bireylerine acil durumlarda ulaşılabilecek diğer kişiler hakkındaki bilgiler.
Fiziksel Mekân ve Güvenlik Bilgileri	İşyerine girişte, kamera ve güvenlik noktasında alınan kayıtları içeren ve işyerinde kalış süresi boyunca alınan kayıtlara ilişkin kişisel bilgiler.
Finans Bilgileri	İşletme çalışanları, stajyerleri, alt işveren çalışanları ve müşterileri ile kurmuş olduğu hukuki bağlantının şekli baz alınarak oluşturulan, her türlü finansal sonucu gösteren bilgiler (Örneğin, Banka Hes.No, IBAN No, Kredi Kartı bilgisi).
İşitsel ve Görsel Bilgileri	A-İmalat San. Tic. A.Ş.'nin iş ilişkileri ve yürüttüğü faaliyetler kapsamında elde ettiği gerçek kişiye ait olduğu açık olan; kamera ve ses kayıtları, fotoğraf ile kişisel veri içeren belgelerin kopyası niteliğindeki belgelerde yer alan veriler
Özlük Bilgileri	A-İmalat San. Tic. A.Ş. ile çalışma münasebeti içerisinde olan gerçek kişilerin özlük dosyalarının oluşturulması sırasında işverenin ve çalışanların yasal menfaatleri ve işverenin yasal yükümlülüklerini yerine getirmesine esas olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veriler
Hassas Nitelikli Kişisel Verileri	A-İmalat San. Tic. A.Ş. ile çalışma münasebeti içerisinde olan çalışanların, stajyerleri ve alt işveren çalışanlarının 6698 sayılı Kanunu'nun 6'ncı maddesinde belirtilen ve işverenin yasal yükümlüğünü yerine getirmek amacıyla (örn. kan grubu, sağlık raporu, sabıka kaydı,) işlenen veriler.
Şikâyet /Talep Yönetimi Bilgileri	İşletmeye yöneltilmiş olan her türlü istek veya şikayetlerin alınması ve değerlendirilmesine dair kişisel veriler.

4.7.1.5 İşletme-1 İmalat San. ve Tic. A.Ş.'de bilgi işlem departmanı tarafından kişisel verilerin korunmasına dair alınan teknik tedbirler

İşletme-1 İmalat San. ve Tic. A.Ş. işyerinde gösterdiği faaliyetler kapsamında işlediği kişisel verilerin hukuka uygun olarak işlenmesi, kaydedilmesi, değiştirilmesi, yeniden düzenlenmesi, güvenli bir şekilde saklanması, saklama sürelerinin belirlenmesi ve saklama süreleri sonunda yok edilmesi, silinmesi veya anonim hale getirilmesi için bir takım teknik tedbirler almaktadır. Bu kapsamda kişisel verilerin hukuka uygun işlenmesi, hukuka aykırı erişimin önlenmesi, verilerin güvenli bir şekilde saklanması, alınan tedbirlerin zaman içinde denetiminin sağlanması, kişisel verilerin yetkisiz kişiler tarafından ifşa edilmesi halinde alınacak teknik tedbirler konusunda mevzuat çerçevesinde hareket etmektedir.

İşyerine iş başı yapmak üzere gelen kişinin kimlik ve özlük bilgileri "Personel Devam Kontrol Sistemi" ne girilmektedir. İş başı yapan personelin sağlık kontrol tarama verileri "İş Sağlığı Ve Güvenliği Sağlık Bilgi Yönetim Sistemi" ne girişi elektronik ortamda yapılmakta ve iş sağlığı ve güvenliliği açısından işçinin oryantasyon eğitimi ve farkındalık eğitimi yaptırılarak yine iş sağlığı ve güvenliği sağlık bilgi yönetim sistemine işlenmektedir. İşyerinde çalışanların sağlık bilgileri ile güvenlik (sabıkaya) bilgileri dışında özel nitelik kişisel verileri işlenmemektedir.

- Hukuka uygun olarak kişisel verilerin işlenmesi bakımından alınan teknik tedbirler;
- İşletme içinde gerçekleştirilen kişisel veri işleme faaliyetleri kapsamında kurulan sistem İnsan Kaynakları Departmanı tarafından denetlenmektedir.
- İşlenen kişisel veriler ile ilgili ilgili kişiler eğitilmekte ve farkındalıkları artırılmaktadır.
- Alınan teknik önlemler periyodik olarak işletme üst yönetimine raporlanmaktadır.
- Bilgi işlem biriminde konusunda uzman personel çalıştırılmaktadır.
- Hukuka aykırı erişimi engelleyecek teknik tedbirler;
- Teknolojik gereklilikler kapsamında önlemler alınmakta ve alınan önlemler zaman zaman güncellenmektedir.

- Departmanlar itibariyle hukuka uygun ve işyeri üst yönetimince belirlenen erişim ve yetkilendirme teknik çözümleri uygulanmaktadır.

- Erişime yetkili olanların yetkileri sınırlandırılmakta ve yetkileri düzenli aralıklarla gözden geçirilmektedir. Bu kapsamda kişisel verilerin tutulduğu ve barındığı noktalara yetki matrisleri oluşturulmuştur. Yetkisi olmayan kişilerin ilgili noktalara erişimleri engellenmiştir.

- Teknik tedbirler zaman içinde iç denetim sistemi gereği ilgilisine raporlanmakta, eğer bir risk varsa yeniden değerlendirilmekte ve gerekli teknolojik çözümler üretilmektedir.

- Dışarıdan sızmaları önleyecek güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmakta, virüs koruma sistemleri kullanılmaktadır.

- Bilişim konusunda uzman teknik personel istihdam edilmektedir.

- Verilerin toplandığı uygulamadaki güvenlik açıklarını tespit amacıyla düzenli olarak güvenlik taramaları yapılmakta ve açıklar kapatılmaktadır.

- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.

- Verilerin güvenli bir şekilde saklanmasını sağlamak amacıyla alınan teknik tedbirler;

- Teknolojik gelişmelere uygun sistemler kullanılmak suretiyle kişisel verilerin güvenli ortamlarda saklanması sağlanmaktadır.

- Bilişim konusunda yetişmiş, tecrübeli personel istihdam edilmektedir.

- Saklama alanlarının güvenli hale getirilmesi bakımından güvenlik sistemleri kurulmakta, alınan teknik tedbirler periyodik olarak iç denetim mekanizması gereği ilgilisine raporlanmakta, şayet riskli bir durum ortaya çıkarsa, yeniden durum değerlendirilmesi yapılarak gerekli teknolojik çözümler üretilmektedir.

- Verilerin güvenli bir şekilde saklanması bakımından yeterli yedekleme programları kullanılmaktadır.

- İşyerinde kişisel verisi işlenen çalışanların kimlik, iletişim, adres, sağlık, özlük, görsel, sabıka kaydı bilgileri hem doküman üzerinde hem de elektronik ortamda kayıt altına alınarak yedeklenmekte ve güvenli bir şekilde saklanmaktadır. Bu kapsamda

PDKS, ISG, LOGO, DC (Domain Controller), programlarının sunucu cihaz ve ekipmanların günlük olarak yedeklenerek sağlıklı ve güvenlik bir şekilde çalışmasını sağlamak amacıyla teknik tedbirler alınmaktadır.

- Alınan teknik tedbirler kapsamında sunucuların donanım arızası yaşanması durumunda örneğin HDD ve RAM'ların yedekleri ile değiştirilmesi durumunda sistemi kesintiye uğratmadan devamlılığı sağlanmaktadır.

- Sunucu ve ekipmanların sağlıklı bir şekilde çalışması adına sistem odaları; ortam denetleme cihazlarıyla hava, ısı ve nem olmak üzere sensörlerde izlenip takip edilmekte, belirlenen seviyelerin altına ve üzerine seyretmesi halinde mail, sms ve sesli arama ile alarm vermektedir.

- Sunucuların bulundukları ortam kesintisiz olarak kamera kontrol sistemi ile kayıt altına alınarak alınan kayıtlar 90 gün süre ile saklanmaktadır.

- Dışarıdan gelebilecek her türlü saldırı ve tehditlere karşı internet hizmeti servis sağlayıcı tarafından DDOS atak önleme hizmeti, ISP, gelişmiş tehdit önleme hizmeti ve atanmış tehdit engelleme hizmeti ve güvenlik duvarı hizmetleri alınmaktadır.

- Dışarıdan gelen isteklere lokasyon içerinde bulunan aktif olarak cluster mimarisinde çalışan güvenlik duvarı korumayı sağlamaktadır.

- Kişisel verilerin güvenliğinin sağlanması için log yönetim sistemi uygulanmaktadır.

- İşletme içerisinde bulunan tüm cihazlarda güncel Anti-Virüs yazılımı ile koruma sağlanmaktadır.

- Bilgi güvenliği ve gizliliğin sağlanması için kırılganlık zafiyet analizi ve sızdırmazlık testi yapılmaktadır.

- Tüm bilgisayarlarda antivirüs üzerinden trafik izleme ve denetleme yapılmakta, cihazların tamamında USB ve benzeri storage görevi gören tüm ekipmanların veri giriş çıkışını engellemek adına kullanımları kısıtlanmaktadır.

- İlgililere, erişim denemeleri veya uygunsuz erişimler, kişisel verilerin yer aldığı veri depolama alanlarına erişimler, loglanarak anlık olarak iletilmektedir.

- Verilerin bulunduğu veri tabanları yetki matrisi, güvenlik duvarı ve anti-virüs ile koruma altına alınmaktadır.

- İşyerinin bulutta depolanan kişisel verisi bulunmamaktadır.
- Kişisel bilgilerin korunması hususunda alınan önlemlerin denetimi;

İşletme-1 İmalat San. ve Tic. A.Ş., 6698 sayılı Kanunu m.12' ye elverişli olarak, kendi içerisinde lüzumlu denetimleri yapmaktadır. Bu denetim sonuçları konu ile ilgili bölüme raporlanan ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler işletmenin iç işleyişi kapsamında yürütülmektedir.

- Yetkisiz bir şekilde yayılan kişisel veriler için alınacak önlemler;

İşletme-1 İmalat San. ve Tic. A.Ş., KVKK'nın 12'nci maddesine uygun olarak işlenen kişisel verilerin başkaları tarafından legal olmayan yollarla elde edilmesi durumunda bu durumu kısa süre içerisinde ilgili kişisel veri sahibine ve Kişisel Verileri Koruma Kurumu'na iletilmesini sağlayan sistemi yürütmektedir.

Bu durum, Kurumun internet sitesinde veya başka bir usul ile Kişisel Verileri Koruma Kurumu tarafından gerek görülmesi durumunda, ilan edilebilecektir.

- İşyeri güvenlik girişinde alınan teknik tedbirler;

İşletme-1 İmalat San. Tic. A.Ş. Bilgi İşlem Departmanı, işyerine girişteki güvenlik noktasında çalışanlar başta olmak üzere işyerine giriş yapan tüm kişilerin kimlik sorgulamalarını yapmaktadır. Güvenlik noktasında güvenlik görevlilerince elektronik ortamda ve manuel olarak ziyaretçi ve personel kayıt defterine kimlik bilgileri işlenmektedir. Örneğin ziyaretçinin işyerine giriş yapması esnasında; TC. Kimlik Kartı talep edilmekte ve Ad-Soyad, TC. Kimlik Numarası, araç ile giriş yapılacaksa araç plaka numarası, ziyaretçinin nereden geldiği ve işletme adı, kiminle görüşeceği ile ilgili verileri hem elektronik ortamda hem de kayıt defterine manuel olarak işlenmektedir. Kendisine yaka kartı verilmekte ve TC. Kimlik Kartı işyerinden çıkışta teslim edilerek yaka kartı geri alınmaktadır. Ziyaretçiden alınan TC. Kimlik Kartı güvenlik odasında duvara monte edilmiş bir raflı dolapta güvenli bir şekilde muhafaza edilmektedir.

İşyerine giren ziyaretçilerin, müşterilerin, tedarikçilerin, alt işverenlerin elektronik ortamda tutulan kayıtları belirli sayıda yönetici tarafından görülecek şekilde sınırlandırılmıştır. Nitekim İnsan Kaynakları, İdari İşler, Bilgi İşlem ve Üst Yönetim dışında giriş yapan kişilerin kimlik bilgileri diğer kişiler tarafından görülememektedir.

4.7.1.6 İnsan kaynakları departmanı tarafından alınan idari tedbirler

- 6698 sayılı kanun uyarınca kişisel verilerin hukuka elverişli işlenmesini sağlamak için alınan idari önlemler;

İşletme-1 İmalat San. ve Tic. A.Ş. tarafından alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- İnsan Kaynakları Departmanına girişler özel kartlı sistemle yapılmamakla birlikte, özlük dosyalarının bulunduğu dolaplar kilit altına alınmakta görevlisi dışında erişim engellenmektedir.

- İş başvuru formlarının güvenliği için işyeri güvenlik girişine kilitli sandık yaptırılmıştır. Her akşam insan kaynakları görevlisi tarafından kilitli sandık açılmakta ve başvuru formları güvenli bir şekilde insan kaynakları departmanında değerlendirmeye alınmaktadır.

- İşyerinde Kişisel Veri Envanteri hazırlanmıştır.

- Veri İşleme Politika Belgesi bulunmaktadır.

- Veri Saklama ve İmha Politikası Belgesi bulunmaktadır.

- Kamera İzleme Politika Belgesi bulunmaktadır.

- Veri siciline (VERBİS) kayıt yapılmıştır.

- Özlük dosyaları gözden geçirilerek gereksiz evraklar temizlenmiştir.

- İşyerinde kullanılan ve kişisel veri içeren tüm dokümanlar kişisel verilerin korunması hususunda revize edilmiştir.

- İşletme web sayfasına kısa politika belgesi, aydınlatma belgesi ve başvuru belgesi konulmuştur.

- Kurumsal mail adreslerinin altına kişisel verilerin kullanılması ve gizliliği ile ilgili bilgilendirme metni konulmuştur.

- Çalışanlar, kişisel verilerin hukuka uygun bir şekilde işlenmesi hususunda bilgilendirilmektedir.

- İşletme-1 İmalat San. ve Tic. A.Ş.'nin yürütmekte olduğu tüm faaliyetler kapsamında tüm birimlerin gerçekleştirmiş olduğu ticari faaliyetler analiz edilerek,

kişisel veriler tanımlanmış, veri işleyenler tespit edilmiş, görev tanımları yapılmış, her biri yazılı olarak bilgilendirilmiş ve işlenen veriler ile ilgili yazılı onayları alınmıştır.

- İşletme-1 İmalat San. ve Tic. A.Ş.'nin tüm departmanlarınca yürütülmekte olan kişisel veri işleme faaliyetleri; 6698 sayılı Kanunun aradığı kişisel veri işleme şartları ve ilkelerine uygun bir şekilde gerçekleştirilmektedir. İlgili birimlerdeki uygulama kurallarını belirlemek ve veri işleyenler özelinde farkındalık yaratmak amacıyla gerekli idari önlemler işletme içi politikalar ve eğitimler yoluyla meydana gelmektedir.

- İlgili işletme ile çalışanlar arasındaki hukuki münasebeti ortaya koyan iş sözleşmelerine, işyeri iç yönetmeliğine, disiplin yönetmeliğine, hukuka aykırı kişisel veri işlememe, veriyi açıklamama, paylaşmama ve kullanmama yükümlülüğü getiren hükümler konulmakta ve bu konuda çalışanların farkındalığı artırılmakta ve denetimleri gerçekleştirilmektedir.

- Hukuka aykırı erişimi engellemek amacıyla alınan idari tedbirler;

- Departman bazında kişisel veri işlenmesinin hukuka uyumu açısından işletme içinde kişisel verilere erişim ve yetki matrisleri hazırlanmıştır.

- 6698 sayılı Kanun hükümlerine göre, çalışanlar, öğrendikleri kişisel verileri başkalarına açıklamama ve amacı dışında kullanmamanın yanı sıra bu yükümlülüklerinin görevlerinden ayrıldıktan sonra da devam edeceği hususunda bilgilendirilmekte ve kendilerinden gerekli taahhütler (Taahhütname) alınmaktadır.

- İşletme iş ilişkisi içinde bulunduğu diğer işletmelere kendi çalışanlarının kişisel verilerinin güvenliği bakımından, imzalanan gizlilik sözleşmelerine, gerekli güvenlik önlemlerinin alacağına ve kendi işletmelerinde bu önlemlere uyulmasını sağlanacağına dair ek hükümler konulmaktadır.

- Güvenli ortamlarda kişisel veri saklanması için alınan idari tedbirler;

İşletme, kişisel verilerin güvenliğinin sağlanması, hukuka uygun olarak işlenmesini temin etmek amacıyla teknolojik imkânlar ve uygulama maliyetlerini de dikkate alarak verilerin kaybolmasını veya değiştirilmesini önlemek için gerekli idari tedbirleri almaktadır. Bu kapsamda;

- İşyeri çalışanları, kişisel verilerin güvenle nasıl saklanması gerektiği hususunda periyodik olarak eğitilmektedirler.

- Veri sahibinin taleplerinin değerlendirmesi ve haklarının gözetilmesi;

İşletme-1 İmalat San. ve Tic. A.Ş., 6698 sayılı Kanun'un 13'üncü maddesi uyarınca; kişisel veri sahiplerinin haklarıyla ilgili olarak veri sahiplerine gerekli bilgilendirmeyi yapmak amacıyla, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

Veri sahibi olan kişiler aşağıda sayılan haklarına dair taleplerini yazılı olarak web sitesindeki başvuru formunu indirmek suretiyle İşletme-1 İmalat San. ve Tic. A.Ş.'ye iletmeleri halinde, işletme talebin niteliğini dikkate alarak en geç otuz gün içinde ücretsiz olarak sonuçlandırmaktadır. Kişisel veri sahipleri;

- Veri sahibi işlenen verisi hakkında bilgi talep etme,
- Verisinin işlenip işlenmediğini öğrenme,
- Verilerin hangi amaçla işlendiğini ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içine veya yurt dışına aktarılan verilerin aktarıldığı üçüncü kişileri bilme,
- Verilerin yanlış ya da eksik işlenmesi durumunda, düzeltme talep etme ve yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- 6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması durumunda kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- Veri sahibi kişinin verisinin otomatik sistemler aracılığıyla analiz edilmesi suretiyle kişi aleyhine bir sonucun ortaya çıkması halinde itiraz etme,
- Verinin kanuna aykırı işlenmesi sebebiyle veri sahibinin zarara uğraması halinde, zararın giderilmesini talep etme, haklarına sahiptir.
- Hassas (özel) nitelikli verilerin korunması amacıyla alınan idari tedbirler;

6698 sayılı Kanun ile bazı kişisel verilerin hukuka aykırı olarak işlenmesi durumunda, kişilerin mağduriyetine yol açabileceği gibi aynı zamanda ayrımcılığa da sebep olma riski bulunduğundan özel önem arz etmektedir. Kanunun gerekçesinde sayılan bu veriler; kişinin 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 veriler ile biyometrik ve genetik verileridir.

İşletme-1 İmalat San. ve Tic. A.Ş. tarafından sadece sağlık verileri ile güvenlik (adli sicil) verileri işlenmek olup diğer özel nitelikli veriler işlenmemektedir. Bu kapsamda işlenen sağlık verileri sağlık birimince, adli sicil bilgileri ise insan kaynakları birimince güvenli bir şekilde işlenmekte ve saklanmaktadır. Örneğin sağlık birimine giriş çıkışlar özel kartlı sistemle yapılmakta görevliler dışında bu birime girişler kapı girişine konulan zil ile yapılabilmektedir. Ayrıca sağlık dosyalarının bulunduğu dolaplar kilit altına alınmakta görevlisi dışında erişim engellenmektedir. İşyeri Hekiminin kullandığı bilgisayar şifresi periyodik olarak değiştirilmekte ve ekran saklama uygulanmaktadır. Kan gurubu paylaşımları fiili imkânsızlıklar dışında ilgili kişinin rızası dışında gerçekleşmemektedir.

- İşyerinde işlenen kişisel verilerin korunması konusunda farkındalık arttırılması ve denetimi ile ilgili alınan idari tedbirler;

İşletme-1 İmalat San. ve Tic. A.Ş. hukuka aykırı olarak kişisel veri işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemeye ve verilerin güvenli bir şekilde saklanmasına yönelik farkındalığın artırılması amacıyla tüm çalışanlarını bu konuda eğitmektedir.

İşletme tüm departmanlarındaki hali hazırdaki çalışanlarının ve işe yeni işe girmiş çalışanların kişisel verilerin korunması hususunda farkındalık artırmak için veri kayıt sistemi kurulmuş olup, konuyla ilgili profesyonel işletmelerden hizmet alınmaktadır.

İşletmenin tüm birimleri itibariyle çalışanlarına yönelik kişisel veri güvenliği konusunda farkındalığın artırılmasına dair yürüttüğü eğitim sonuçları işletme üst yönetimine raporlanmaktadır. İşletme-1 İmalat San. ve Tic. A.Ş. bu yönde verdiği eğitimlere, bilgilendirme oturumlarına ve seminerlere yapılan katılımları analiz etmekte ve gerekli denetimleri yapmaktadır. Ayrıca, ilgili mevzuatın güncellenmesine paralel bir biçimde eğitimlerini güncellemekte ve yenilemektedir.

- Alt işveren çalışanları, tedarikçiler ve stajyerlerin kişisel veri güvenliği konusunda farkındalık arttırılması ve denetimi;

İşletme-1 İmalat San. ve Tic. A.Ş. kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye, hukuka aykırı olarak verilere erişilmesini önlemeye ve verilerin güvenli bir şekilde saklanmasını sağlamaya dönük farkındalık artırmak amacıyla, Alt işveren çalışanları, Tedarikçileri ile Stajyerlerine eğitimler ve seminerler düzenlenmesini temin etmekte ve yürütülen eğitimler periyodik olarak tekrarlanmaktadır.

- Veri sahibinin aydınlatılması ve bilgilendirilmesi;

İşletme-1 İmalat San. ve Tic. A.Ş. işletme olarak 6698 sayılı Kanunu m.10 kapsamında, kişisel verilerin elde edilmesi sırasında veri sahiplerini aydınlatmaktadır. Bu bağlamda İşletme-1 İmalat San. ve Tic. A.Ş. kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile varsa temsilcisinin kimliği ve nihayetinde kişisel veri sahibinin sahip olduğu hakları konusunda aydınlatma yapmaktadır.

TC. Anayasası'nın 20' nci maddesi uyarınca, herkes, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme hakkına sahiptir. Bu kapsamda, 6698 sayılı Kanun m.11'de kişisel veri sahibinin hakları arasında "bilgi talep etme" de sayılmıştır. İşletme, bu nedenle, Anayasa'nın 20' nci ve 6698 sayılı Kanun'un 11 inci maddelerine uygun olarak veri sahibinin bilgi talep etmesi halinde, en geç 30 gün içinde gerekli bilgilendirmenin yapılması gerekmektedir.

4.7.1.7 İşletme-1 İmalat San. ve Tic. A.Ş. kişisel veri sahipleri sınıflandırması

İşletme tarafından aşağıda sıralanan kişisel veri sahibi sınıflarının kişisel verileri işlenmekle birlikte, "Kişisel Verilerin Korunması Politikası"na uygun olarak başta çalışanlar olmak üzere, alt işveren çalışanları, çalışan adayları, stajyerler, müşteriler, tedarikçiler, ziyaretçiler ve üçüncü kişiler ile sınırlıdır.

Aşağıda "İşletme-1 İmalat San. ve Tic. A.Ş. 'nin Kişisel Verilerin Korunması Politikası" kapsamında yer alan çalışanlar, alt işveren çalışanları, stajyerler, çalışan adayları, ziyaretçiler, tedarikçiler, müşteriler ve üçüncü kişilere açıklık getirilmektedir.

Çizelge 4.2: Kişisel Veri Sahibi Sınıflaması

Kişisel Veri Sahibi	Açıklaması
Çalışanlar	İş Kanunu uyarıca, bir iş sözleşmesine dayanarak çalışan ve iş ilişkileri üzerinden kişisel verileri elde edilen gerçek kişiler.
Ziyaretçi	A-İmalat San. ve Tic. A.Ş.'nin sahip olduğu fiziki bana ve tesislere muhtelif amaçlarla girmiş olan ziyaretçi konumundaki gerçek kişiler.

Çizelge 4.2 (devam): Kişisel Veri Sahibi Sınıflaması

Kişisel Veri Sahibi	Açıklaması
Üçüncü Kişi	İşyeri Çalışanları Kişisel Verilerin Korunması ve İşlenmesi Politikası kapsamına girmeyen diğer gerçek kişiler (Örneğin: Eski çalışanlar, Aile bireyleri ve yakınlar)
Çalışan Adayları	A-İmalat San. ve Tic. A.Ş.'ye herhangi bir yolla iş başvurusunda bulunmuş veya CV ve ilgili bilgilerini firmanın değerlendirmesine açmış olan gerçek kişiler
Alt işveren İşçileri	A-İmalat San. ve Tic. A.Ş.'de İş Kanunu kapsamında asıl işin bir bölümünde ya da yardımcı işlerinde iş alan alt işverenlerin istihdam ettiği gerçek kişiler
Stajyerler	İşyerinde, 3308 sayılı Mesleki Eğitim Kanunu'na göre, staj yapan gerçek kişiler
Tedarikçiler	Firmanın iş ilişkisinde bulunduğu tedarikçilerin çalışanı konumundaki gerçek kişiler
Müşteriler	Firma ile ticari faaliyetler kapsamında iş ilişkisinde bulunan gerçek kişiler

Aşağıdaki tabloda yukarıda belirtilen kişisel veri sahibi sınıfları içindeki kişilerin işlenen kişisel verilerinin detayı açıklanmaktadır.

Çizelge 4.3: Verisi İşlenen Kişi Sınıflaması

Kişisel Veri Sınıflaması	Verisi İşlenen Kişiler
Kimlik Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişiler
İletişim Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişiler
Lokasyon Verisi	Çalışanlar, Alt İşveren Çalışanları

Çizelge 4.3 (devam): Verisi İşlenen Kişi Sınıflaması

Kişisel Veri Sınıflaması	Verisi İşlenen Kişiler
Aile Bireyleri ve Yakın Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Stajyerler, Üçüncü Kişi,
Fiziksel Mekân Güvenlik Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi
Finansal Bilgi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler,
Görsel/İşitsel Bilgi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi
Özlük Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler,
Özel Nitelikli Kişisel Veri	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler,
Talep/Şikâyet Yönetimi Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi

İşletme-1 İmalat San. ve Tic. A.Ş. işyeri, 6098 sayılı Kanun m.8 ve 9'a uygun olarak veri sahiplerinin kişisel verilerini aşağıdaki kişi sınıflarına aktarabilir:

- İşletmenin üst düzey yetkililerine,
- İşletmenin diğer yetkililerine,
- Hukuksal olarak yetkili kamu kurum ve kuruluşlarına
- Hukuksal olarak yetkili özel hukuk kişilerine

Aktarımda bulunulan yukarıda belirtilen kişilerin kapsamı ve veri aktarım amaçları aşağıda belirtilmektedir.

Çizelge 4.4: Veri Aktarımı Yapılacak Kişi Sınıflaması

Veri Aktarımı Yapılabilecek Kişiler	Tanımı	Veri Aktarım Amacı
İşletme Yetkilileri	İşletme yönetim kurulu üyeleri ve diğer yetkili gerçek kişiler	İşletmenin ticari faaliyetlerine dair stratejilerin tasarlanması, en üst düzeyde yönetiminin sağlanması
Hukuksal Olarak Yetkili Kamu Kurum ve Kuruluşları	İlgili mevzuat hükümleri uyarınca işletmeden bilgi ve belge istemeye yetkisi olan kamu kurum ve kuruluşları	İlgili kamu kurum ve kuruluşlarının hukuksal yetkisi dahilinde talep ettiği amaçla sınırlı olarak
Hukuksal Olarak Yetkili Özel Hukuk Kişileri	İlgili mevzuat hükümlerine göre işletmeden bilgi ve belge istemeye yetkili özel hukuk kişileri	İlgili özel hukuk kişilerinin hukuksal yetkisi dahilinde talep ettiği amaçla sınırlı olarak

4.7.1.8 İşyeri girişi ile işyeri içerisinde veri işleme faaliyetleri

İşletme-1 İmalat San. ve Tic. A.Ş. tarafından işyeri güvenliğinin sağlanması, iş sağlığı ve güvenliğinin temini amacıyla işletmeye ait bina ve tesislerinde güvenlik kamerasıyla izleme faaliyeti ile misafir giriş çıkışlarının takibi amacına yönelik kişisel veri işleme faaliyetinde bulunulmaktadır.

- İşyeri girişi ile işyeri içerisinde kamera ile izleme faaliyeti;

İşletme-1 İmalat San. ve Tic. A.Ş.'nin kamera izleme politikası kapsamında kamera ile izleme sisteminin nasıl kurgulandığı ve verilerin gizliliği ile kişilerin temel haklarının nasıl korunacağına dair bilgilendirme yapılmaktadır.

İşletmenin güvenlik kamerası ile izleme faaliyeti kapsamında; işletme çalışanlarının ve diğer kişilerin sağlık ve güvenliğini sağlamaya yönelik yasal çıkarlarını korumayı amaçlamaktadır.

- Kamera ile izleme faaliyetinin yasal dayanağı;

Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata uygun bir biçimde işletme tarafından elektronik gözetleme faaliyeti ile sürdürülmektedir.

- Kişisel verilerin korunması hukukuna uygun olarak kamera izleme faaliyetinin yürütülmesi;

İşletme-1 İmalat San. ve Tic. A.Ş. tarafından 6698 sayılı Kanun'da yer alan düzenlemelere uygun hareket edilerek, güvenlik amacıyla kamera izleme faaliyeti yürütülmektedir. İşyerinin bina ve tesislerinde güvenliğin sağlanması amacıyla, yürürlükte bulunan ilgili mevzuatta öngörülen amaçlarla ve 6698 sayılı Kanunla sınırlı olarak kamera izleme faaliyetinde bulunulmaktadır.

- Kamera izleme faaliyeti hakkında bilgilendirme;

İlgili işletme tarafından 6698 sayılı Kanun m.10'a uygun olarak, kişisel veri sahibi bilgilendirilmektedir. Bilgilendirme hem kameraların altına asılan bilgilendirme levhaları ile hem de iş sözleşmelerine konulan hükümlerle yapılmaktadır. Veri sorumlusu olan işveren kamera ile izleme faaliyetine ilişkin olarak birden fazla yöntemle bildirimde bulunmaktadır. Buradaki amaç, veri sahibinin temel hak ve özgürlüklerine zarar verilmesini engellenmek, şeffaflığın ve kişisel veri sahibinin aydınlatılmasını sağlamaktır.

- Kamera izleme faaliyetinin yürütülmesindeki amaç ile amaçla sınırlılık;

İşletmede, kişisel veriler 6698 sayılı Kanun m.4'e uygun olarak, amaçla bağlantılı, tahditli ve ölçülü bir şekilde işlemektedir. İşletme, tarafından video kamera ile izleme faaliyetinin sürdürülmesindeki amaç "İşyeri Kamera İzleme Politikası"ndaki sayılan amaçlarla sınırlıdır. Bu kapsamda, güvenlik kameralarının izleme alanları ile sayısı ve ne zaman izleme yapılacağı, güvenlik amacına ulaşmak için yeterli ve bu amaçla tahditli olarak uygulamaya alınmaktadır. Kişinin mahremiyetini güvenlik amaçlarını aşan şekilde müdahale sonucu doğurabilecek alanlarda (örneğin, soyunma odaları, duş ve tuvaletler) izlemeye tabi tutulmamaktadır.

- Elde edilen verilerin güvenliğinin sağlanması;

İşletme-1 İmalat San. ve Tic. A.Ş. tarafından 6698 sayılı Kanun m.12'ye göre, kamera ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler, Kamera İzleme Politikası"nda belirlenen usul ve esaslar ile mer'i mevzuat çerçevesinde alınmaktadır.

4.7.2 İşletme-2 Gıda San. ve Tic. A.Ş.

4.7.2.1 İşletme-2 Gıda San. ve Tic. A.Ş. işletmesi hakkında genel bilgiler

1991 yılında Kocaeli Gebze ilçesinde kurulan, modern tesisleriyle bugün Türkiye`nin ve Dünya`nın en önemli şekerleme ve çikolata üreticilerinden biri olan İşletme-2 Gıda San. ve Tic. A.Ş. uluslararası pazarda büyük bir başarı göstermektedir. Geniş ürün yelpazesinde farklı damak tatlarına hitap eden iki yüz elinin üzerinde ürün çeşidi bulunduran ve ihracat konusundaki deneyimini tavizsiz uygulayan yüksek kalite ve hijyen kontrol normlarına borçlu olan işletme, Gıda Güvenliği, Kalite ve Helal Gıda Yönetim sistemi sertifikalarından ISO 22000, FSSC 22000, BRC, IFS ve HELAL gıda sertifikalarına sahiptir. Farklı ülkelerin en sıkı gıda kodekslerine uygunluğunu sağlayabilen ve ayrıntılı gıda analizlerini yapabilen işletme, koşulsuz müşteri memnuniyetini ilke edinmekte ve uygulamadaki başarısını sürdürmektedir. 2000 yılında Cenevre-İsviçre`de kazanılan Altın Kalite Yıldızı ödülü işletmenin başarısını tescil etmiş ve mükemmele ulaşma çabasını perçinlemiştir. Kalitenin yanında sürekli gelişim de işletmenin temel özelliklerindendir. Pazarlama departmanının koordinasyonu ile AR-GE Merkezi yeni ürünler için kılavuzluk etmekte, mevcut ürünlerin de geliştirilmesinde anahtar rol oynamaktadır.

İşletme-2 Gıda San. ve Tic. A.Ş., bugün itibariyle 33.000 m² kapalı alanda bini aşkın personeli ile günlük yüz elli ton satışa hazır üretim kapasitesiyle üretiminin yüzde doksanını dünya genelinde 130 ülkeye ihraç etmektedir. Yurtiçinde ise zincir mağazalar dışında araçlı satış dağıtım sistemiyle geleneksel kanala hizmet vermeye başlamıştır. İşletme, kalitesini her geçen gün artan ürün çeşitliliği ile daha geniş kitlelere ulaştırmaya, doğru yatırımlarla sektörünü geliştirmeye ve daha tatlı bir dünya için çalışmaya devam ediyor. Daima en iyisini üretmiş olmanın gururuyla gelecekte de en iyisini üretmek işletmenin temel gayesidir.

İşletmenin misyon ve vizyonu aşağıdaki gibidir:

Vizyonumuz;

Müşterilerimizin değişen ihtiyaçlarını ve dünya genelinde alışverişçi eğilimlerini sürekli takip ederek işletme adını sektörün itibarlı markalarından biri olarak sürdürerek, başta şeker ve çikolata kategorileri olmak üzere kendi ürün markalarımızla yurt içi ve yurtdışında lezzetli ve yenilikçi ürünlerle pazar liderleri arasında yer almak.

Misyonumuz;

- Üretimde ve Yönetimde ‘‘önce kalite’’ düsturunu benimseyerek, ileri teknolojiyi kullanarak, sürekli müşteri memnuniyetini artırmak ve yenilikçi ürünlerle ülke ekonomisine katkıda bulunmak
- İnovasyonu destekleyen kurum kültürü yaratmak ve bunun sürdürülebilir olmasını sağlamak
- Ar-Ge ve inovasyon projeleri ile müşterilerin beklentilerinin ötesinde ürün ve hizmetler tasarlayarak ve gerçekleştirerek, sürekli müşteri memnuniyetini sağlamak
- Çalışanlarımızın olanaklarını iyileştirerek ve kişisel gelişimlerine destek vererek mutlu bir ekip yaratmak
- Stratejik marka yönetimi ile bulunduğumuz pazarlarda “en iyiler “içinde olmak
- En güzel şeker denince akla gelen ilk marka olmak

4.7.2.2 İşletme-2 Gıda San. ve Tic. A.Ş.’nin Veri İşleme Amacı

İşletme-2 Gıda San. ve Tic. A.Ş. işyeri çalışanlarının, çalışan adaylarının, stajyerlerinin, tedarikçilerinin ve alt işverenleri ile alt işveren çalışanlarının, müşterilerinin ve ziyaretçilerinin kişisel verilerini amaca uygun, amaçla bağlantılı ve ölçülü bir şekilde işlemektedir. Nitekim işlenen kişisel veriler;

- Kurumsal sürdürülebilirlik faaliyetlerinin planlanması ve icrası,
- Etkinlik yönetiminin sağlanması,
- Tedarikçilerle olan ilişkilerin yönetiminin sağlanması,
- Alt İşverenlerle olan ilişiklerin sürdürülebilmesi,
- Personel temin süreçlerinin yürütülmesi,
- Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi,
- Hukuk işlerinin icrası/takibi,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Kurumsal yönetim faaliyetlerinin icrası,
- Talep ve şikâyet yönetiminin temini,
- Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi,
- Ziyaretçi kayıtlarının oluşturulması ve takibi,
- Kanundan kaynaklanan yükümlülüklerin yerine getirilebilmesi,

amacıyla işlenmekte ve güvenli bir şekilde saklanmaktadır.

4.7.2.3 İşletme-2 Gıda San. ve Tic. A.Ş.'nin veri işleme ilkeleri

6698 sayılı Kişisel Verilerin Korunması Kanunu m.4'de kişisel verilerin işlenmesine ilişkin usul ve esaslar 108 sayılı Sözleşmeye ve 95/46/EC sayılı Avrupa Birliği Direktifine eşgüdüm biçiminde düzenlenmiştir. Bu kapsamda; İşletme-2 Gıda San. ve Tic. A.Ş. işyeri 6698 sayılı Kanunda belirtilen kişisel verilerin işlenmesine esas ilkelere uygun olarak aşağıda gösterilen şekillerde veri işlemektedir.

- Hukuka ve dürüstlük kurallarına uygun olma:

İşletme-2 Gıda San. ve Tic. A.Ş.; kişisel verilerin işlenmesinde yasal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda İşletme-2 Gıda San. ve Tic. A.Ş. Kişisel verilerin işlenmesinde orantılılık gerekliliklerini nazarı dikkate alarak, kişisel verileri amacına uygun bir şekilde kullanmaktadır.

- Doğru ve gerektiğinde güncel olma:

İşletme-2 Gıda San. ve Tic. A.Ş.; kişisel veri sahiplerinin temel haklarını ve kendi yasal çıkarlarını nazarı dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını temin etmek amacıyla bu yönde gerekli tüm tedbirleri almaktadır. Örneğin, İşletme-2 Gıda San. ve Tic. A.Ş. tarafından; kişisel veri sahiplerinin kişisel verilerini düzeltme ve doğruluğunu teyit etmelerine yönelik olarak yeterli bilgilendirme yapılarak bu konuda gerekli prosedürleri hazırlamıştır.

- Belirli, açık ve yasal amaçlar için işlenme:

İşletme-2 Gıda San. ve Tic. A.Ş. hukuka uygun olarak yasal kişisel veri işleme amacını açık ve net olarak ortaya koymaktadır. İşletme-2 Gıda San. ve Tic. A.Ş. 'de yürütülmekte olan ticari faaliyetlerle bağlantılı ve bunlar için gerekli olan kadar kişisel veri işlenmektedir. İşletme-2 Gıda San. ve Tic. A.Ş. işverenince kişisel verilerin hangi amaçla işleneceği henüz kişisel veri işleme faaliyetine başlanmadan önce belirlenmektedir.

- İşlendikleri amaçla bağlantılı, tahditli ve ölçülü olma:

İşletme-2 Gıda San. ve Tic. A.Ş., kişisel verileri belirlenen amaçların gerçekleştirilebilmesine uygun bir şekilde işlemekte ve amacıyla bağdaşmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden imtina etmektedir. Örneğin,

sonradan ortaya çıkması ihtimal dahilindeki ihtiyaçların karşılanması amacıyla kişisel veri işleme faaliyetinde bulunmamaktadır.

- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme:

İşletme-2 Gıda San. ve Tic. A.Ş. kişisel verileri sadece mer'i mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Bu kapsamda, İşletme-2 Gıda San. ve Tic. A.Ş. öncelikle mer'i mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini belirlemekte, bir süre belirlenmişse bu süreye uygun hareket etmekte, bir süre belirlenmemişse işyerinin ihtiyaçlarını dikkate alarak, verilerin işleme amacına uygun süre kadar saklamaktadır. Belirlenen saklama sürenin sona ermesi ya da işlenmesini gerektiren nedenlerin ortadan kalkması durumunda kişisel veriler İşletme-2 Gıda San. ve Tic. A.Ş. tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir. Gelecekte kullanma olasılığı olabilir düşüncesi ile İşletme-2 Gıda San. ve Tic. A.Ş. tarafından kişisel veriler saklanmamaktadır.

4.7.2.4 İşletme-2 Gıda San. ve Tic. A.Ş.'nin veri işleme şartları

Kişisel verilerin işlenme şartları 6698 sayılı Kanunun 5 inci maddesinde sayılmış olup, buna göre aşağıdaki hallerden en az birinin bulunması durumunda kişisel verilerin işlenmesi mümkün olabilecektir.

- İlgili kişinin açık rızasının varlığı:

İşyerinde iş başvurusu aşamasından başlamak üzere ilgili kişiler Kişisel Verilerin Korunması Kanunu kapsamında öncelikle aydınlatılmakta ve işlenen kişisel verileri konusunda açık rızaları usulüne uygun bir şekilde alınmaktadır. Örneğin iş başvurusu yapan çalışan adaylarının iş başvuru formlarında bu konuda aydınlatma ve onay metni bulunmaktadır. Çalışanlardan ise, bilgilendirme ve onay formu ile açık rıza yazılı olarak alınmaktadır. İşyerine gelen ziyaretçiler güvenlik girişine asılan aydınlatma metinleri ve yaka kartlarına yazılan metinler ile aydınlatılmaktadır. Nitekim güvenlik girişine asılan yazı içeriğinde, "Bu işyerine girişte ilettiğiniz kimlik bilgileriniz Kişisel Verilerin Korunması Kanununa uygun olarak güvenli bir şekilde saklanmakta yasal yükümlülükler dışında veri sahibinin izni olmadan bir başkasıyla paylaşılmamaktadır" ibaresi bulunmaktadır.

- Kanunlarda açıkça öngörülmesi:

İşletme, 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin verilerini (sabıka kaydı) işyeri güvenliği için işe alım sürecinde talep etmektedir. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu gereğince işe giriş periyodik sağlık raporu talep edilmektedir. 4857 sayılı İş Kanunu'na göre yazılı olarak imzalanması gereken iş sözleşmesi imzalanmaktadır.

- Rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunluluk olması veya fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunması:

İşyerinde vaki meydana gelecek bir iş kazasında kazaya uğrayan işçinin kimlik ve sağlık bilgileri işletmenin konuyla ilgili yetkilisi tarafından götürüldüğü hastanede sağlık görevlileriyle paylaşılmaktadır.

- Bir sözleşmenin kurulması ya da ifasıyla doğrudan doğruya ilintili olması şartıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması:

İşveren işe aldığı işçilerle yazılı olarak iş sözleşmesi yapmakta bunu 4857 sayılı İş Kanunun 8 inci maddesine dayandırmaktadır. Ayrıca işletmenin tedarikçileri, alt işverenleri ve müşterileri ile de yasal menfaatleri doğrultusunda sözleşme imzalamaktadır. Nitekim alt işverenlerle yazılı olarak imzalanan "Alt işverenlik Sözleşmesi" 4857 sayılı Kanunun 2 nci ve Alt İşverenlik Yönetmeliği'nin 9 uncu maddesine dayanmaktadır.

- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması:

İşveren tarafından işçilere aylık ücret ödenebilmesi için, banka iban numarası, işçinin medeni durumu, bakımla yükümlü olduğu kişiler, eşinin çalışıp çalışmadığı ile ilgili bilgiler içeren Aile Durum Bildirimi istenmekte ayrıca daha önce başka bir işyerinde çalışması varsa mevcut SGK sicil numarası gibi kişisel verileri talep edilerek işlenmektedir. Bununla birlikte 1774 sayılı Kimlik Bildirme Kanunu gereğince işe giren veya çıkan işçilerin kimlik bilgilerini 3 gün içinde işyerinin bağlı bulunduğu kolluk birimlerine bildirerek kişisel verilerini hukuki yükümlülüğünü yerine getirmesi amacıyla paylaşmaktadır.

- İlgili kişinin kendisi tarafından alenileştirilmiş olması halinde:

İşyerine iş başvurusu yapan çalışan adaylarının iletişim, kimlik ve eğitim bilgileri, iş başvurusu yapılmasına imkân veren internet sitelerinde (kariyer.net, secretcv. gibi) yayımlanması halinde, işe alım sürecinin yönetilmesi amacıyla işlenmektedir.

- Bir hakkın tesisi veya korunması için veri işlemenin zorunluluk arz etmesi:

İşletme, ispat niteliği taşıyan işçiye ait güvenlik bilgi ve belgelerini (sabıka kaydı, güvenlik soruşturma belgeleri gibi) polis, jandarma ve istihbarat birimlerinin talep etmesi halinde paylaşmaktadır.

- Veri sahibinin temel hak ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun legal çıkarları için veri işlenmesinin zorunlu olması durumunda:

İşletme, işçilerin sağlık ve güvenliği ile işyeri güvenliğinin temini amacıyla, işyerine ait bina ve tesislerde güvenlik amaçlı olarak kamera kaydı yapmaktadır. Bu konuda kamera izleme politikası oluşturulmuş olup, izlemeyle ilgili çalışanlar, stajyerler, ziyaretçiler, müşteriler, tedarikçiler ve alt işveren çalışanları bilgilendirilmektedir. Bilgilendirme her kameranın altına "Bu işyeri 7/24 saat kamera ile izlenmektedir" biçiminde bilgilendirme levhaları asılmaktadır. Ayrıca işçilerin iş sözleşmesine bu konuda hükümler konulmaktadır.

4.7.2.5 İşletme-2 Gıda San. ve Tic. A.Ş.'de işlenen kişisel veri sınıfı

İşletmenin hukukun gereklerine uygun ve yasal veri işleme amaçları nazarı dikkate alınarak, 6698 sayılı Kanunu'nun 5 inci maddesinde öngörülen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve tahditli olarak, başta kişisel verilerin işlenmesine ilişkin 4' üncü maddede belirtilen ilkeler olmak üzere 6698 sayılı Kanunda belirtilen genel ilkelere ve düzenlenen bütün yükümlülüklere uyularak ve "İşletme-2 Gıda San. ve Tic. A.Ş. Kişisel Verilerin Korunması Politikası" kapsamındaki çalışanlar, çalışan adayları, stajyerler, alt işveren çalışanları, ziyaretçiler, müşteriler, tedarikçiler ve üçüncü kişiler tahditli olarak aşağıda belirtilen sınıflardaki kişisel verileri, 6698 sayılı Kanun m.10 gereğince veri sahiplerinin bilgilendirilmesi kaydıyla işlenmektedir.

Çizelge 4.5: Kişisel Veri Kategorizasyonu Sınıflaması

Kişisel Veri Sınıflaması	Kişisel Veri Kategorizasyonu Açıklama
Kimlik Bilgisi	6698 sayılı Kanunda, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen, kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kimlik verileri olarak nitelendirilmektedir. Buna göre, işyerinde çalışanların, adı-soyadı, T.C. kimlik numarası, uyruk bilgisi, anne-baba adı, doğum yeri-tarihi, cinsiyet bilgileri, ehliyet, nüfus cüzdanı ve pasaport gibi belgeler ile SGK No, imza bilgisi, taşıt plakası v.b. bilgiler
İletişim Bilgisi	İşletme-2 Gıda San. ve Tic. A.Ş. işvereni çalışanları başta olmak üzere ticari ilişki içerisinde olduğu kimliği belirli veya belirlenebilir bir gerçek kişiye ait olan; telefon ve faks numarası, adres, e-mail ve IP adresi gibi iletişim bilgileri
Lokasyon/Seyahat Verisi	İşletme-2 Gıda San. ve Tic. A.Ş.'de tüm departmanlarca yürütülen iş organizasyonu kapsamında, işletmenin ürün ve hizmetlerinin kullanımı sırasında veya iş birliği içerisinde olduğu kurumların çalışanlarının İşletme-2 Gıda San. ve Tic. A.Ş. araçlarını kullanırken bulunduğu yerin konumunu tespit eden bilgiler; seyahat verileri ile küresel konumlama sistemi (GPS), v.b.
Aile Bireyleri ve Yakın Bilgisi	İşletmenin tüm departmanlarda çalışanların, stajyerlerin, iş başvurusu yapanların, alt işveren çalışanlarının legal çıkarlarını korumak amacıyla eş, anne, baba, çocuktan oluşan aile bireyleri, yakınları ve acil hallerde erişilebilecek diğer kişiler hakkındaki bilgiler
Fiziki Mekân Güvenlik Bilgisi	İşletme çalışanları başta olmak üzere; işyerine girişte, fiziksel mekânın içerisinde kalış süresi boyunca alınan kamera kayıtları ve güvenlik noktasında alınan kayıtlar v.b.

Çizelge 4.5 (devam): Kişisel Veri Kategorizasyonu Sınıflaması

Kişisel Veri Sınıflaması	Kişisel Veri Kategorizasyonu Açıklama
Finansal Bilgi	İşletme-2 Gıda San. ve Tic. A.Ş.'nin kişisel veri sahibi olan çalışanları, stajyerleri, alt işveren çalışanları ve müşterileri ile kurmuş olduğu hukuksal ilişkinin şekline göre her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara dair işlenen kişisel veriler ile banka hesap no, IBAN No, kartı bilgileri, malvarlığı verisi, gelir bilgisi gibi veriler
Görsel ve İşitsel Bilgi	İşletmenin iş ilişkileri ve yürüttüğü faaliyetler kapsamında elde ettiği gerçek kişiye ait olduğu açık olan; fiziksel mekân güvenlik bilgisi kapsamında giren kayıtlar hariç, fotoğraf ve kamera kayıtları
Özlük Bilgisi	İşletme-2 Gıda San. ve Tic. A.Ş. ile çalışma ilişkisi içerisinde olan gerçek kişilerin özlük dosyalarının oluşturulması sırasında işverenin ve çalışanların yasal menfaatleri ve işverenin yasal yükümlülüklerini yerine getirmesine esas olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veriler
Özel Nitelikli Kişisel Veri	İşyeri ile çalışma ilişkisi içerisinde olan çalışanların, stajyerleri ve alt işveren çalışanlarının 6698 sayılı Kanunu'nun 6 ncı maddesinde belirtilen ve işverenin yasal yükümlüğünü yerine getirmek amacıyla (örn. kan grubu, sağlık raporu, sabıka kaydı,) işlenen veriler
Şikâyet/Talep Yönetimi Bilgisi	İşletme-2 Gıda San. ve Tic. A.Ş.'ye yöneltilmiş olan her türlü şikâyet veya talebin alınması ve değerlendirilmesine dair kişisel veriler

4.7.2.6 İşletme-2 Gıda San. ve Tic. A.Ş.'de bilgi işlem depertmanı tarafından kişisel verilerin korunmasına dair alınan teknik tedbirler

İşyerinde gösterdiği faaliyetler kapsamında işlediği kişisel verilerin hukuka uygun olarak işlenmesi, kaydedilmesi, değiştirilmesi, yeniden düzenlenmesi, güvenli bir şekilde saklanması, saklama sürelerinin belirlenmesi ve saklama süreleri sonunda silinmesi, yok edilmesi ya da anonim hale getirilmesi için bir takım teknik tedbirler

almaktadır. Bu kapsamda kişisel verilerin hukuka uygun işlenmesi, hukuka aykırı erişimin önlenmesi, verilerin güvenli bir şekilde saklanması, alınan tedbirlerin zaman içinde denetiminin sağlanması, kişisel verilerin yetkisiz kişiler tarafından ifşa edilmesi halinde alınacak teknik tedbirler konusunda mevzuat çerçevesinde hareket etmektedir.

İşyerine iş başı yapak üzere gelen kişinin kimlik ve özlük bilgileri "Personel Devam Kontrol Sistemi" ne girilmektedir. İş başı yapan personelin sağlık kontrol tarama verileri "İş Sağlığı ve Güvenliği Sağlık Bilgi Yönetim Sistemi" ne girişi elektronik ortamda yapılmakta ve iş sağlığı ve güvenliliği açısından işçinin oryantasyon eğitimi ve farkındalık eğitimi yaptırılarak yine iş sağlığı ve güvenliği sağlık bilgi yönetim sistemine işlenmektedir. İşyerinde çalışanların sağlık bilgileri ile güvenlik (sabıkaya) bilgileri dışında özel nitelik kişisel verileri işlenmemektedir.

- Hukuka uygun veri işlenmesi amacıyla alınan teknik tedbirler;
- İşletme-2 Gıda San. ve Tic. A.Ş.'de gerçekleştirilen kişisel veri işleme faaliyetleri kapsamında kurulan sistem bilgi işlem departmanı tarafından denetlenmektedir.
- İşlenen kişisel veriler ile ilgili ilgili kişiler eğitilmekte ve farkındalıkları artırılmaktadır.
- Alınan teknik önlemler periyodik olarak işletme üst yönetimine raporlanmaktadır.
- Teknik konularda uzman personel istihdam edilmektedir.
- Hukuka uygun olmayan verilere erişimin engellenmesi için alınan teknik tedbirler;
- Teknolojik gelişmelere uygun teknik tedbirler alınmakta, alınan tedbirler periyodik olarak güncellenmekte ve yenilenmektedir.
- Birimler itibariyle belirlenen hukuki uyum gerekliliklerine uygun olarak erişim ve yetkilendirme teknik çözümleri devreye alınmaktadır.
- Erişim yetkileri tahdit edilmekte olup, yetkiler belirli aralıklarla gözden geçirilmektedir. Bu kapsamda kişisel verilerin tutulduğu noktalara yetki matrisleri oluşturulmuştur. Yetkisi olmayan kişilerin ilgili noktalara erişimleri engellenmiştir.

- Risk taşıyan hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmekte olup, alınan teknik tedbirler aralıklı olarak iç denetim mekanizması gereği ilgilisine raporlanmakta,

- Güvenlik duvarlarını içeren yazılımlar ve donanımlar ile virüs koruma sistemleri kurulmaktadır.

- Teknik konularda bilişim uzmanı personel istihdam edilmektedir.

- Toplanan kişisel verilerin uygulamadaki güvenlik zafiyetlerini tespit etmek amacıyla düzenli olarak güvenlik taramalarından geçirilmekte ve bulunan açıkların kapatılması sağlanmaktadır.

- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.

- Güvenli ortamlarda verilerin saklanması için alınan teknik tedbirler;

- Güvenli ortamlarda kişisel verilerin saklanması için teknolojik gelişmelere uygun sistemler kullanılmaktadır.

- Erişim Yönetim Prosedürüne göre; kişisel bilgisayarlara 10 dakika boyunca müdahale edilmezse uyku moduna geçilmektedir.

- Kullanıcıların şifrelerinin belirli periyodlarda değiştirilmesi kapsamında Bilgi Güvenlik Yönetim Sistemi Politikasına göre; 90 günde bir şifreler değiştirilmektedir.

- Uzaktan bağlantı yapan kullanıcıların kontrolü ile ilgili olarak işletmenin BGYS Politikasına göre; çalışanların işletme dışından kurumsal bilgi sistemlerine bağlanmasına izin verilmemektedir.

- Hizmet alınan tedarikçilerin hizmet vermek için uzaktan bağlanma durumları için, imzalanan sözleşmelere Bilgi Güvenliği ile ilgili maddeler eklenmiştir.

- İşletmenin Bilgi Güvenlik Yönetim Sistemi Politikası ve Denetim İzi Yönetimi Prosedürüne göre; kayıtların silinme/düzeltme ile ilgili kayıtlar asgari 3 yıl, sistemlere erişimler ile ilgili kayıtlar asgari 1 yıl saklanmaktadır.

- İşletme bilgisayarların dışarıya çıkartılmasının izin prosedürüne bağlanmasıyla ilgili olarak, dizüstü bilgisayarlar, fabrika müdürünün onayı ile fabrika dışına çıkartılmaktadır. Ancak bu konuda yazılı bir prosedür ve takip edilen bir form bulunmamaktadır.

- Dışarı çıkarılan bilgisayarın internet bağlantı güvenliğinin sağlanması için bütün bilgisayarlara yüklenmiş olan antivirüs programı internet üzerinden çalıştığı için fabrikada ya da dışarda olsun zararlı sitelere girişleri engellemektedir.

- Dışarıdan gelen bilgisayar veya donanımların bilgi işlem tarafından denetlenmesi amacıyla, bilgisayarların işyerini ağına bağlanmasına izin verilmemektedir.

- İnternet çıkışı almak isteyen müşterileri/ziyaretçilerine sadece firewall kurallarımıza uygun şekilde internet çıkışı verilmektedir.

- Bu konuda amaçlanan, ziyaretçilere internet hizmeti verirken kendi cep telefonlarından SMS onayı ile internete çıkmalarını sağlayarak internet güvenliği arttırmaktır.

- İşletme bilgisayarlarında harici USB kullanımı yasaklanmış olup, sadece kişilere zimmetlenmiş olan USB cihazı ile kendine zimmetli olan bilgisayarda çalışılabilmektedir.

- Dışarıdan gelen USB'lerin bilgi işlemin kontrolünde kullanımının sağlanması amacıyla fabrika müdürünün onayı olmadan kullanıma izin verilmemekte olup, fabrika müdürünün onayı ile Bilgi İşlemin kontrolünde izin verilmektedir.

- İşletme bilgisayarların kişilere zimmetlenmesiyle ilgili olarak insan kaynağının yönetilmesi prosedürüne göre, bilgisayar, usb bellek vb cihazları ilgili kişilere zimmetlenmiştir.

- Kişisel verilerin kimler tarafından görüleceğinin yetki sınırlarının çizilmiş ve yetki matrisi oluşturulmuştur.

- İşletme bilgisayarlarında iş dışında internet erişiminin sınırlandırılması için kullanılan antivirüs programı ve firewall üzerinden ayarlar sayesinde sosyal forumlar, alışveriş siteleri, zararlı siteler vb. engellemeler yapılmıştır.

- İşletme bilgisayarında özel mail kullanımı sınırlandırılmamıştır.

- Bilişim uzmanı personel teknik konularda istihdam edilmektedir.

- Güvenli bir biçimde kişisel verilerin saklanmasını sağlamak için hukuka uygun ve teknik yeterliliği olan bir yedekleme programları kullanılmaktadır.

- İşyerinde kişisel verisi işlenen çalışanların kimlik, iletişim, adres, sağlık, özlük, görsel, sabıka kaydı bilgileri hem doküman üzerinde hem de elektronik ortamda kayıt altına alınarak yedeklenmekte ve güvenli bir şekilde saklanmaktadır.
- İşletmede Personel Devam Kontrol Sistemi (PDKS) kullanılmaktadır.
- Güvenlik duvarı Log sunucusu tarafından lokasyon içerindeki tüm kullanıcıların yapmış olduğu internet giriş çıkışları loglanarak saklanmaktadır.
- Bilgi güvenliği ve gizliliğin sağlanması için kırılganlık zafiyet analizi yapılmaktadır.
- Sızdırmazlık testi yapılmaktadır.
- Veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri yetkililere anında iletilmektedir.
- İşyerinin bulutta depolanan kişisel verisi bulunmamaktadır.
- Kişisel verilerin korunması hususunda alınan tedbirlerin denetimi;

İşletme, 6698 sayılı Kanun'un 12' nci maddesine uyarınca, hem kendi bünyesinde gerekli denetimleri yapmakta hem de dışarıdan hizmet satın alarak üçüncü göz denetimi yaptırmaktadır. Denetim sonuçları üst yönetime raporlanmakta ve alınan önlemlerin iyileştirilmesi için gerekli faaliyetler sürdürülmektedir.

- Verilerin yetkisiz bir şekilde açığa vurulması halinde alınacak tedbirler;

İşyerinde, 6698 sayılı Kanun m.12'ye uygun olarak işlenen verilerin yasal olmayan yöntemlerle başkaları tarafından elde edilmesi durumunda, bunu en kısa sürede ilgili kişisel veri sahibine ve Kişisel Verileri Koruma Kurumu'na bildirilmesini sağlayan sistem yürütülmektedir.

Kişisel Verileri Koruma Kurumu tarafından lüzumu halinde, bu durum, kurumun internet sitesinde veya başka bir yöntemle ilan edilebilecektir.

- İşyeri güvenlik girişinde alınan teknik tedbirler;

İşletmenin İdari İşler Departmanı, işyerine girişinde çalışanlar başta olmak üzere işyerine giriş yapan tüm kişilerin kimlik sorgusunu yapmaktadır. Güvenlik noktasında güvenlik görevlilerince elektronik ortamda ve manuel olarak ziyaretçi ve personel kayıt defterine kimlik bilgileri işlenmektedir. Örneğin ziyaretçinin işyerine giriş yapması esnasında; TC. Kimlik Kartı talep edilmekte ve Ad-Soyad, TC. Kimlik

Numarası, araç ile giriş yapılacaksa araç plaka numarası, ziyaretçinin nereden geldiği ve işletme adı, kiminle görüşeceği ile ilgili verileri hem elektronik ortamda hem de kayıt defterine manuel olarak işlenmektedir. Kendisine yaka kartı verilmekte ve TC. Kimlik Kartı işyerinden çıkışta teslim edilerek yaka kartı geri alınmaktadır. Ziyaretçiden alınan TC. Kimlik Kartı güvenlik odasında duvara monte edilmiş bir raflı dolapta güvenli bir şekilde muhafaza edilmektedir.

İşyerine girişte güvenlik noktasına asılan bilgilendirme levhası ile kimlik bilgilerini paylaşan ziyaretçiler bilgilendirilmektedir.

İşyerine giren ziyaretçilerin, müşterilerin, tedarikçilerin, alt işverenlerin elektronik ortamda tutulan kayıtları belirli sayıda yönetici tarafından görülecek şekilde sınırlandırılmıştır. Nitekim insan kaynakları, idari işler, bilgi işlem ve üst yönetim dışında giriş yapan kişilerin kimlik bilgileri diğer kişiler tarafından görülememektedir.

4.7.2.7 İnsan kaynakları departmanı tarafından alınan idari tedbirler

- 6698 sayılı kanun uyarınca hukuka uygun kişisel veri işlenmesi için alınan idari tedbirler;

- 27001 Bilgi Güvenliği Yönetim Sistemi bulunmamaktadır. Ancak Kişisel Verilerin Korunması ile ilgili uyum çalışması yapılmıştır.

- İnsan kaynakları departmanına girişler özel kartlı sistemle yapılmakta, görevliler dışında bu birime girişler kapı girişine konulan zil ile sağlanmaktadır. Ayrıca özlük dosyalarının bulunduğu dolaplar kilit altına alınmakta, görevlisi dışında erişim engellenmektedir.

- İş başvuru formlarının güvenliği için işyeri güvenlik girişine kilitli sandık yaptırılmıştır. Her akşam insan kaynakları görevlisi tarafından kilitli sandık açılmakta ve başvuru formları güvenli bir şekilde insan kaynakları departmanında değerlendirmeye alınmaktadır.

- İşyerinde Kişisel Veri Envanteri hazırlanmıştır.
- Veri İşleme Politika Belgesi bulunmaktadır.
- Veri Saklama ve İmha Politikası Belgesi bulunmaktadır.
- İmha politikası kapsamında imha komisyonu oluşturulmuştur.
- Kamera İzleme Politika Belgesi bulunmaktadır.

- Veri siciline (VERBİS) kayıt yapılmıştır.
- İrtibat kişisi belirlenerek ataması yapılmıştır.
- Özlük dosyaları gözden geçirilerek gereksiz evraklar temizlenmiştir.
- İşyerinde kullanılan ve kişisel veri içeren tüm dokümanlar kişisel verilerin korunması hususunda revize edilmiştir.
- İşletme web sayfasına kısa politika belgesi, aydınlatma belgesi ve başvuru belgesi konulmuştur.
- Kurumsal mail adreslerinin altına kişisel verilerin kullanılması ve gizliliği ile ilgili bilgilendirme metni konulmuştur.
- Kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda çalışanlar, bilgilendirilmekte ve eğitilmektedir.
- İşyerine girişteki güvenlik noktasında kimlik bilgilerini paylaşan ziyaretçiler bilgilendirme levhasıyla aydınlatılmıştır.
- İşe alım ve eleme sürecinde yer alan çalışanların eğitimi sağlanmıştır.
- İş başvurularında çalışan adayların elde edilen kişisel veriler sadece işe alım süreçleri için kullanılmaktadır. Bir başka amaç için kullanılmamaktadır.
- İş başvurularında çalışan adayların elde edilen kişisel verilerin saklama süreleri belirlenmiştir. Saklama süresini dolduran başvuru formları komisyon marifetiyle imha edilmektedir.
- İş başvuru formları yeniden revize edilmiş, formlara aydınlatma ve açık rıza metni ilave edilmiştir.
- İşletme-2 Gıda San. ve Tic. A.Ş. 'nin yürütmekte olduğu tüm faaliyetler kapsamında tüm birimlerin gerçekleştirmiş olduğu ticari faaliyetler analiz edilerek, kişisel veriler tanımlanmış, veri işleyenler tespit edilmiş, görev tanımları yapılmış, her biri yazılı olarak bilgilendirilmiş ve işlenen veriler ile ilgili yazılı onayları alınmıştır.
- İşyerinin tüm departmanlarınca yürütülmekte olan kişisel veri işleme faaliyetleri; 6698 sayılı Kanunun aradığı kişisel veri işleme şartları ve ilkelerine uygun bir şekilde gerçekleştirilmektedir. Diğer taraftan departmanlar bazında belirlenen hukuki uyum gerekliliklerinin sağlanması için ilgili birimlerdeki veri işleyenler

özelinde farkındalık oluşturmak ve uygulama kurallarını belirlemek amacıyla gerekli idari tedbirler işletme içi politikalar ve eğitimler yoluyla gerçekleştirilmektedir.

- Veri sorumlusu işveren ile çalışanlar arasındaki hukuki ilişkiyi ortaya koyan iş sözleşmelerine, işyeri iç yönetmeliğine, disiplin yönetmeliğine, hukuka aykırı kişisel veri işlememe, ifşa etmeme, paylaşmama ve kullanmama yükümlülüğü getiren kayıtlar konulmakta ve bu konuda çalışanların farkındalığı artırılmakta ve denetimleri gerçekleştirilmektedir.

- Hukuka aykırı veri erişimini engellemek için alınan idari tedbirler;

- İnsan kaynakları departmanına, bilgi işlem departmanına, revire ve arşive erişim kontrol altına alınmıştır. Giriş ve çıkışlar kartlı sistemle yapılmaktadır.

- Kişisel verilere hukuka aykırı ulaşımı engellemek için alınacak idari ve teknik önlemler hususunda, çalışanlar eğitilmektedir.

- Departman bazında kişisel veri işlenmesinin hukuka uyumu açısından işletme içinde kişisel verilere erişim ve yetki matrisleri hazırlanmıştır.

- Çalışanların 6698 sayılı Kanun hükümlerine aykırı olarak, öğrendikleri kişisel verileri başkalarına açıklamama ve işleme amacı dışında kullanamama ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceğini bilmeleri amacıyla bilgilendirilmekte ve buna istinaden ilgili kişilerden taahhütname alınmaktadır.

- İşletme-2 Gıda San. ve Tic. A.Ş. tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile imzalanan gizlilik sözleşmelerine, kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin ilave hükümler konulmaktadır.

- Güvenli ortamlarda kişisel veri saklanması için alınan idari tedbirler;

İşletme-2 Gıda San. ve Tic. A.Ş., teknolojik imkânlar ve uygulama maliyetlerini dikkate alarak, kişisel verilerin güvenli ortamlarda saklanması ve hukuka aykırı amaçlarla kaybolmasını, yok edilmesini veya değiştirilmesini önlemek için gerekli idari tedbirleri almaktadır.

İlgili işletme tarafından alınan başlıca idari önlemler aşağıda sıralanmaktadır:

- Çalışanlar, kişisel verilerin güvenli bir şekilde nasıl saklanması gerektiği konusunda periyodik olarak eğitilmektedirler.

- İşletme tarafından kişisel verilerin saklanması konusunda hukuki gereklilikler nedeniyle dışarıdan bir hizmet temin edilmesi durumunda, kişisel verilerin hukuka uygun olarak aktarıldığı ilgili işletmeler ile imzalanan gizlilik sözleşmelerine; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlanacağına ilişkin düzenlemelere yer verilmektedir.

- Veri sahibinin haklarının gözetilmesi ve taleplerinin değerlendirilmesi;

İşletme, 6698 sayılı Kanun'un 13'üncü maddesine uygun bir biçimde, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gereken bilgilendirmenin yapılması için gerekli kanalları, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

Kişisel veri sahipleri aşağıda sayılan haklarına dair taleplerini yazılı olarak işletmenin web sitesindeki başvuru formunu indirerek işletmeye iletmeleri halinde, işletme talebin niteliğini dikkate alarak en geç otuz gün içinde ücretsiz olarak sonuçlandırmaktadır. Kişisel veri sahipleri;

- Kişisel verilerin işlenme amacını öğrenme,

- Kişisel verilerinin işlenip işlenmediğini öğrenme,

- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

- Yurt içi veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

- Verilerin yanlış veya eksik işlenmiş olması durumunda, düzeltilmesini talep etme ve yapılan bu işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

- 6698 sayılı Kanun ve ilgili mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenme sebeplerinin ortadan kalkması halinde, kişisel verilerin silinmesini veya yok edilmesini talep etme,

- İşlenen kişisel verilerin otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

- Kanuna aykırı olarak kişisel verilerin işlenmesi nedeniyle zarara uğraması hâlinde, zararın karşılanmasını talep etme, haklarına sahiptir.

- Kişisel verilerin silinmesi ve imha edilmesi için alınan idari tedbirler;

Kişisel Verilerin Saklama ve İmha Politikası kapsamında departmanlar itibariyle veriler sınıflandırılmış ve kişisel veri içeren dokümanlar ve elektronik ortamdaki veriler tespit edilerek saklama süreleri belirlenmiştir. Saklama sürelerinin belirlenmesinde öncelikle mevzuatta açıkça yapılan düzenlemeler dikkate alınmış, şayet mevzuatta düzenleme yoksa işletmenin gereklilikleri nazarı dikkate alınarak en geniş süreler benimsenerek saklama süreleri belirlenerek hem veri envanterine hem de politika belgesinin sonundaki tabloya işlenmiştir.

- Hassas (özel) nitelikli kişisel verilerin korunması amacıyla alınan idari tedbirler;

Bazı kişisel verilerin hukuka aykırı biçimde işlenmesi, kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşımaktadır. Bu verileri şu şekilde sıralamak mümkündür; kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, din, mezhep 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 verilerdir.

Bu kapsamda, İşletme-2 Gıda San. ve Tic. A.Ş. işyerinde, sadece sağlık verileri ile güvenlik (adli sicil) verileri işlenmek olup diğer özel nitelikli veriler işlenmemektedir. Bu bağlamda işlenen sağlık verileri sağlık birimince, adli sicil bilgileri ise insan kaynakları birimince güvenli bir şekilde işlenmekte ve saklanmaktadır. Örneğin sağlık birimine giriş çıkışlar özel kartlı sistemle yapılmakta görevliler dışında bu birime girişler kapı girişine konulan zil ile yapılabilmektedir. Ayrıca sağlık dosyalarının bulunduğu dolaplar kilit altına alınmakta görevlisi dışında erişim engellenmektedir. İşyeri Hekiminin kullandığı bilgisayar şifresi periyodik olarak değiştirilmekte ve ekran saklama uygulanmaktadır. Kan gurubu paylaşımları fiili imkânsızlıklar dışında ilgili kişinin rızası dışında gerçekleşmemektedir.

- İşyerinde verilerin işlenmesi ve korunması konusunda farkındalık arttırılması ve denetimi ile ilgili alınan idari tedbirler;

İşletme-2 Gıda San. ve Tic. A.Ş., tüm çalışanlarını kişisel verilerin hukuka aykırı olarak işlenmesi, verilere hukuka aykırı olarak erişilmesinin önlenmesi ve verilerin güvenli bir şekilde saklanması konusunda farkındalık oluşturmak için eğitmektedir.

İşletme-2 Gıda San. ve Tic. A.Ş. 'nin departmanlarındaki hali hazır çalışanları ile işe yeni girmiş olan çalışanların kişisel verilerin korunması hususunda farkındalık oluşmak için veri kayıt sistemi kurmuş olup, konuyla ilgili profesyonel işletmelerden hizmet almaktadır.

İşletme-2 Gıda San. ve Tic. A.Ş. 'nin tüm departmanlarında kişisel verilerin korunması ve işlenmesi konusunda farkındalığın artırılmasına yönelik yürütülen eğitim sonuçları İşletme üst yönetimine raporlanmaktadır. İşletme, bu yönde ilgili eğitimlere, seminerlere ve bilgilendirme toplantılarına yapılan katılımları değerlendirip, gerekli denetimleri yapmaktadır. İşletme, ilgili mevzuatın güncellenmesine paralel olarak eğitimlerini güncellemekte ve yenilemektedir.

- Alt işveren çalışanı, tedarikçi ve stajyerler 'in verilerin korunması ve işlenmesi hususunda farkındalık düzeylerinin arttırılması;

İşletme-2 Gıda San. ve Tic. A.Ş. hukuka aykırı olarak kişisel verilerin işlenmesini önlemeye, hukuka aykırı olarak verilere erişilmesini önlemeye ve verilerin güvenli bir şekilde saklanmasını sağlamaya dönük farkındalığın artırılması için alt işveren çalışanları, tedarikçileri ile stajyerlerine eğitimler ve seminerler düzenlenmesini temin etmekte ve yürütülen eğitimler periyodik olarak tekrarlanmaktadır.

- Kişisel veri sahibinin aydınlatılması ve bilgilendirilmesi;

İşletme-2 Gıda San. ve Tic. A.Ş. işletme olarak 6698 sayılı Kanun m.10'a uygun olarak, kişisel verilerin elde edilmesi sırasında Kişisel Veri Sahiplerini aydınlatmaktadır. Bu kapsamda İşletme-2 Gıda San. ve Tic. A.Ş. kişisel verilerin hangi amaçla işleneceği, varsa temsilcisinin kimliği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile kişisel veri sahibinin sahip olduğu hakları konusunda aydınlatma yapmaktadır.

TC. Anayasası'nın 20 nci maddesi "herkes, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme hakkına sahiptir" hükmüne amirdir. Bu doğrultuda 6698 sayılı Kanun

m.11'de kişisel veri sahibinin hakları arasında "bilgi talep etmede" sayılmıştır. İşletme, bu kapsamda, T.C. Anayasası'nın 20 nci ve 6698 sayılı Kanun'un 11 inci maddelerine uygun olarak kişisel veri sahibinin bilgi talep etmesi durumunda gerekli bilgilendirmeyi en geç 30 gün içinde yerine getirmektedir.

İşletmenin web sayfasında oluşturulan kişisel verilerin korunması ile ilgili modül altında örnek başvuru formu konulmuş olup, bilgi talep etmek isteyen veri sahipleri ilgili formu doldurarak veri sorumlusuna iletebilmektedir.

4.7.2.8 İşletme-2 Gıda San. ve Tic. A.Ş.'de işlenen kişisel verilerin sahiplerine ilişkin sınıflandırma

İşletme-2 Gıda San. ve Tic. A.Ş., toplam 17 departmanda 77 çalışanı ile kişisel veri işlemektedir.

İşletme-2 Gıda San. ve Tic. A.Ş. tarafından aşağıda sıralanan kişisel veri sahibi kategorilerinin kişisel verileri işlenmekle birlikte, "Kişisel Verilerin Korunması Politikası"na uygun olarak başta çalışanlar olmak üzere, alt işveren çalışanları, çalışan adayları, stajyerler, müşteriler, tedarikçiler, ziyaretçiler ve üçüncü kişiler ile sınırlıdır.

Aşağıda "İşletme-2 Gıda San. ve Tic. A.Ş.'nin Kişisel Verilerin Korunması Politikası" kapsamında yer alan çalışanlar, alt işveren çalışanları, stajyerler, çalışan adayları, ziyaretçiler, tedarikçiler, müşteriler ve üçüncü kişiler kavramlarına açıklık getirilmektedir.

Çizelge 4.6: Kişisel Veri Sahibi Kişi Sınıflaması

Kişisel Veri Sahibi Kategorisi	Açıklaması
Çalışanlar	İş Kanunu uyarınca, İşletme-2 Gıda San. ve Tic. A.Ş. 'de bir iş sözleşmesine dayanarak çalışan ve iş ilişkileri üzerinden kişisel verileri elde edilen gerçek kişiler
Ziyaretçi ler	İşletmenin sahip olduğu fiziksel mekanlara muhtelif gayelerle girmiş olan ziyaretçi konumundaki gerçek kişiler
Üçüncü Kişiler	İşletme Çalışanlarının Kişisel Verilerin Korunması ve İşlenmesi Politikası kapsamına girmeyen diğer gerçek kişiler (Örneğin. Aile bireyleri ve yakınlar, eski çalışanlar)
İş Başvurusunda Bulunan Çalışan Adayları	İşletme-2 Gıda San. Ve Tic. A.Ş. 'ye herhangi bir yolla iş başvurusunda bulunmuş ya da CV ve ilgili bilgilerini işletmemizin incelemesine açmış olan gerçek kişiler

Çizelge 4.6 (devam): Kişisel Veri Sahibi Kişi Sınıflaması

Kişisel Veri Sahibi Kategorisi	Açıklaması
Alt işveren Çalışanları	İş Kanunu kapsamında asıl işin bir bölümünde ya da yardımcı işlerinde iş alan alt işverenlerin istihdam ettiği gerçek kişiler
Stajyerleri	’de 3308 sayılı Mesleki Eğitim Kanunu kapsamında İşletme-2 Gıda San. Ve Tic. A.Ş. işyerinde staj yapan gerçek kişiler
Tedarikçileri	İşletmenin iş ilişkisi içerisinde bulunduğu, mal ve hizmet satın aldığı tedarikçilerin çalışanı olan gerçek kişiler
Müşterileri	İşletme-2 Gıda San. Ve Tic. A.Ş. ile ticari faaliyetleri kapsamında iş ilişkisi içerisinde bulunan gerçek kişiler

Aşağıdaki tabloda yukarıda belirtilen kişisel veri sahibi sınıflarını ve bu sınıflar içerisindeki kişilerin hangi tip kişisel verilerinin işlendiği detaylı olarak açıklanmaktadır.

Çizelge 4.7: Kişisel Verinin İlişkili Olduğu Veri Sahibinin Kişi Sınıflaması

Kişisel Veri Sınıfları	Kişisel Verinin İlişkili Olduğu Veri Sahibi Sınıfı
Kimlik Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişiler
İletişim Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişiler
Lokasyon Verisi	Çalışanlar, Alt İşveren Çalışanları
Aile Bireyleri ve Yakın Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Stajyerler, Üçüncü Kişi,
Fiziksel Mekân Güvenlik Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi
Finansal Bilgi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler,
Görsel ve İşitsel Bilgi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi
Özlük Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler,
Hassas Nitelikli Kişisel Veri	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler,
Şikâyet ve Talep Yönetimi Bilgisi	Çalışanlar, Alt İşveren Çalışanları, Çalışan Adayları, Stajyerler, Ziyaretçiler, Tedarikçiler, Müşteriler ve Üçüncü Kişi

İşletme-2 Gıda San. Ve Tic. A.Ş. 6698 sayılı Kanunu'nun 8 ve 9 uncu maddelerine uygun olarak veri sahiplerinin kişisel verilerini aşağıda sıralanan kişi kategorilerine aktarılabilir:

- İşletmenin üst düzey yetkililerine,
- İşletmenin diğer yetkililerine,
- Hukuken yetkili kişi, kamu kurum ve kuruluşlarına
- Hukuken yetkili özel hukuk kişilerine

Aktarımda bulunulan yukarıda belirtilen kişilerin kapsamı ve veri aktarım amaçları aşağıda belirtilmektedir.

Çizelge 4.8: Veri Aktarımı Yapılacak Kişi Sınıflaması

Veri Aktarımı Yapılabilecek Kişiler	**Tanımı**	**Veri Aktarım Amacı**
İşletme Yetkilileri	İşletmenin Yönetim Kurulu üyeleri ve diğer yetkili gerçek kişiler	İşletmenin ticari faaliyetlerine ilişkin stratejilerin tasarlanması, en üst düzeyde yönetiminin sağlanması ve denetim amaçlarıyla tahditli olarak
Hukuken Yetkili Kişi, Kamu Kurum ve Kuruluşları	İlgili mevzuat hükümlerine göre işletmeden bilgi ve belge almaya yetkili kişi, kamu kurum ve kuruluşları	İlgili kamu kurum ve kuruluşlarının hukuki yetkisi dahilinde talep ettiği amaçla tahditli olarak
Hukuken Yetkili Özel Hukuk Kişileri	İlgili mevzuat hükümlerine göre işletmeden bilgi ve belge almaya yetkili özel hukuk kişileri	İlgili özel hukuk kişilerinin hukuki yetkisi dahilinde talep ettiği amaçla tahditli olarak

4.7.2.9 İşyeri girişi ile işyeri içinde kişisel veri işleme faaliyetleri

İşletme-2 Gıda San. ve Tic. A.Ş. tarafından işyeri güvenliğinin sağlanması, iş sağlığı ve güvenliğinin temini amacıyla İşyerinin binalarında ve tesislerinde güvenlik kamerasıyla izleme faaliyetinde bulunulmaktadır. Özellikle işyerine giriş çıkış noktasından başlamak üzere stratejik öneme sahip tüm bölgelerde elektronik gözetleme yapılmaktadır. Yapılan elektronik gözetleme işletmenin Kamera İzleme Politikasına uygun olarak yapılmakta ve işlenen kişisel veriler (görüntü-ses kaydı) 90 günde bir silinmektedir.

- İşletme-2 Gıda San. ve Tic. A.Ş.'nin işyeri girişinde ve içerisinde yürütülen kamera ile izleme faaliyeti;

İşletmenin kamera izleme politikası kapsamında kamera ile izleme sisteminin nasıl kurgulandığı ve kişinin temel haklarının nasıl korumaya alındığına ve kişisel verilerin gizliliğinin nasıl sağlandığına ilişkin bilgilendirme yapılmaktadır.

İşletmenin stratejik alanları güvenlik kamerası ile izleme faaliyeti kapsamında izlenmekte ve çalışanların ve diğer kişilerin sağlık ve güvenliğini sağlamaya yönelik yasal çıkarlarını koruması amaçlanmaktadır.

- Kamera ile izleme faaliyetinin yasal dayanağı;

Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata dayalı olarak kamera ile izleme faaliyeti sürdürülmektedir.

- Kişisel veri koruma hukukuna uygun elektronik gözetleme faaliyeti yürütülmesi;

6698 sayılı Kanun'da yer alan düzenlemelere uygun olarak işletme içinde elektronik gözetleme faaliyetinde bulunulmaktadır. İşletmede yapılan kamera ile izleme faaliyeti tamamen işyerinin bina ve tesislerinde güvenliğin sağlanması amacını taşımakta ve aynı zamanda çalışanların sağlığı ve güvenliğinin sağlanmasını amaçlamaktadır.

- Elektronik gözetleme faaliyetinin duyurulması;

İşletme-2 Gıda San. ve Tic. A.Ş., tarafından 6698 sayılı Kanunu m.10'daki hükümlere uygun olarak, kişisel veri sahibi aydınlatılmaktadır. Aydınlatma hem kameraların altına asılan bilgilendirme levhaları ile hem de iş sözleşmelerine konulan hükümlerle yapılmaktadır. İşyerinde kamera ile izleme faaliyetine ilişkin birden fazla yöntem ile aydınlatma yapılmakta ve bildirimde bulunulmaktadır. Böylece, kişisel veri sahibinin

temel hak ve özgürlüklerine zarar verilmesine engel olunmakta ve şeffaflığın ve kişisel veri sahibinin aydınlatılmasının sağlanması amaçlanmaktadır.

- Elektronik gözetleme faaliyetinin amacı ve amaçla sınırlılık;

Elektronik gözetleme faaliyeti, 6698 sayılı Kanun'un 4' üncü maddesine uygun olarak, kişisel verileri işlendikleri amaçla bağlantılı, tahditli ve ölçülü bir biçimde işlenmektedir. İşyerinde, video kamera ile izleme faaliyetinin sürdürülmesindeki amaç "Kamera İzleme Politikası"ndaki sayılan amaçlarla sınırlıdır. Güvenlik kameralarıyla ne zaman izleme yapılacağı, izleme alanları, sayısı ve güvenlik amacına ulaşmak için yeterli ve bu amaçla tahditli olarak politika belgesi rehberliğinde uygulama yapılmaktadır. Özel hayatın gizliliğinin sınırlarını ve amacını aşan bir şekilde müdahale sonucu doğurabilecek alanlarda (örneğin, soyunma odaları, duş ve tuvaletler) izlemeye tabi tutulmamaktadır.

- Elde edilen verilerin güvenliğinin sağlanması;

İşletme-2 Gıda San. ve Tic. A.Ş. tarafından 6698 sayılı Kanun'un 12 nci maddesine uygun olarak, kamera ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler, Kamera İzleme Politikası"nda belirlenen usul ve esaslar ile mer'i mevzuat çerçevesinde alınmaktadır.

4.8 Örnek Olaylar ile İlgili Ortak Sonuç ve Analiz

Kişisel Verileri Koruma Kurulu VERBİS (veri güvenlik bilgi sistemi) sistemine kayıt yaptırması gereken veri sorumlularında iki kriter aramaktadır. Bu kapsamda yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan işletmeler VERBİS üzerinden sicile kayıt yaptırmakla yükümlüdürler. Aksi durumda 20 bin TL ila 1 milyon TL arasında idari para cezası ile karşı karşıya kalabilirler. Sicile kayıt veri sorumluları ile yurtdışında yerleşik tüm veri sorumluları için 01.10.2018 itibaren 30.09.2019 tarihine kadar yapılması gerekmektedir.

Örnek olay çalışmamıza konu iki işletmede de çalışan sayısının 50'nin üzerinde olması dolayısıyla bahse konu işletmeler VERBİS üzerinden sicile kayıt yükümlülüklerini yerine getirmişlerdir. VERBİS, sicile kayıt esnasında işletmelerin veri envanterlerini baz alarak saklama sürelerini ve veri işleme gerekçelerini sorgulamakta ve aynı zamanda veri sorumlusu tarafından alınacak bazı idari ve teknik tedbirin alınıp alınmadığını sorgulamaktadır.

VERBİS bu bağlamda; işletmelerin bilgi işlem departmanlarınca alınması gereken teknik tedbirler kapsamında, ağ güvenliği ve uygulama güvenliğinin sağlanmasını, ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmasını, anahtar yöntemi kullanılmasını, bilgi teknoloji sistemleri tedarik, geliştirme ve bakımı kapsamında güvenlik önlemleri alınmasını, bulutta depolanan kişisel verilerin güvenliği sağlanmasını, çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri öngörülmesini, çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmasını, çalışanlar için yetki matrisi oluşturulmasını, erişim loglarının düzenli olarak tutulmasını, erişim, bilgi güvenliği kullanım, saklama ve imha konularında kurumsal politikalar hazırlanıp uygulamaya konulmasını, gerektiğinde veri maskeleme yöntemi kullanılmasını, veri işleyenler ile gizlilik taahhütnameleri yapılmasını, görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin kaldırılmasını, güncel anti-virüs sistemleri kullanılmasını, güvenlik duvarları kullanılmasını, çalışanlarla, tedarikçilerle, alt işverenler, müşterilerle, danışmanlarla, avukatlarla imzalanan sözleşmelerin veri güvenliği hükümleri içermesi için önlem alınmasını, kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmasını ve ilgili evrakların gizlilik dereceli belge formatında gönderilmesini, kişisel veri güvenliği politika ve prosedürlerinin belirlenmesini, kişisel veri güvenliği ile ilgili sorunların hızlı bir şekilde üst yönetime raporlanmasını, kişisel veri güvenliğinin takibinin yapılmasını, kişisel veri içeren fiziksel ortamlara giriş çıkışlara gerekli güvenlik önlemlerin alınmasını, kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel, vb.) karşı güvenliği hale getirilmesini, kişisel veri içeren ortamların güvenliğinin sağlanmasını, kişisel verilerin mümkün olduğunca azaltılmasını, kişisel verilerin yedeklenmesini ve yedeklenen kişisel verilerin güvenliğinin sağlanmasını, kullanıcı hesap yöntemi ve yetki kontrol sistemi uygulanmasını ve bunların takibinin yapılmasını, kurum içi periyodik ve/veya rastgele denetimler yapılmasını, log kayıtlarının kullanıcı müdahalesi olmayacak şekilde tutulmasını, mevcut risk ve tehditlerin belirlenmesini, özel nitelikli kişisel veri güvenliğine yönelik protokol prosedürlerin belirlenmesini ve uygulanmasını, özel nitelikli kişisel veriler için güvenli şifreleme/ kriptografik anahtarların kullanılmasını ve farklı birimlerce yönetilmesini, saldırı tespit ve önleme sistemlerinin kullanılmasını, sızma testi uygulanmasını, siber güvenlik önlemlerinin alınmasını ve uygulamasının sürekli takip edilmesini, şifrelemenin yapılmasını, taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel verilerin şifrelenerek aktarılmasını,

veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetiminin sağlanmasını, veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda farkındalıklarının sağlanmasını, veri kaybı önleme yazılımının kullanılmasını istemektedir.

Örnek olay çalışması yaptığımız işletmelerin veri siciline kayıt sırasında yukarıda öngörülen teknik tedbirlerin hangilerini aldıkları araştırılmış ve işletmelerin öngördükleri tedbirler karşılaştırılmıştır. Nitekim her iki işyerinin de VERBİS sistemine süresi içinde kayıt yaptırdıkları tespit edilmiştir. Bu işyerlerinin henüz 27001 Bilgi Güvenliği Yönetim Sistemini kurmadıkları anlaşılmıştır. İşletmeler farklı sektörlerde (tekstil ve gıda) faaliyet gösterse dahi kişisel verilerin korunması ile ilgili almaları gereken idari ve teknik tedbirlerin yasal dayanağının aynı olması nedeniyle benzerlik gösterdiği yadsınamaz bir gerçektir. Çünkü işletmeler kendi çalışanları başta olmak üzere çalışan adaylarının, stajyerlerinin, alt işveren çalışanlarının tedarikçilerinin, müşterilerinin ve ziyaretçilerinin kişisel verilerini işlemektedirler. Elbette ki işletmelerin fiziki ve yönetim yapılarının ve yaklaşımlarının farklılık arz ettiği dikkate alındığında birtakım farklılıkların bulunduğunu söylememiz de mümkündür. Örneğin İşletme-1 İmalat San. ve Tic. A.Ş.'de çalışan adaylarının iş başvuru formları işyerinin girişindeki güvenlik noktasında alınması sebebiyle bunların güvenliği için işyeri güvenlik girişine kilitli sandık yaptırılmıştır. İşletme-2 Gıda San. ve Tic. A.Ş'de ise iş başvuru formları işyeri içinde alındığından böyle bir tedbir öngörülmemiştir.

Farklı sektörlerde faaliyet gösteren her iki işletmenin de veri işleme amacı aynıdır. Çünkü hem mevzuattan kaynaklanan hem de işyeri gerekliliklerinden kaynaklanan ihtiyaçlar doğrultusunda veri işlenmektedir. Nitekim işlenen kişisel veriler;

- Kurumsal sürdürülebilirlik faaliyetlerinin planlanması ve icrası,
- Etkinlik yönetiminin sağlanması,
- Tedarikçilerle olan ilişkilerin yönetiminin sağlanması,
- Alt İşverenlerle olan ilişiklerin sürdürülebilmesi,
- Personel temin süreçlerinin yürütülmesi,
- Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi,
- Hukuk işlerinin icrası/takibi,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,

- Kurumsal yönetim faaliyetlerinin icrası,
- Talep ve şikâyet yönetiminin temini,
- Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi,
- Ziyaretçi kayıtlarının oluşturulması ve takibi,
- Kanundan kaynaklanan yükümlülüklerin yerine getirilebilmesi,

amacını taşımaktadır.

Veri işleme şartlarına bakıldığında da benzer özellikler gösterdiği görülmektedir. Nitekim ilgili kişinin (veri sahibi) açık rızasının varlığı aranırken her bir işletme aynı yöntemle hareket etmektedir. Örneğin iş başvurusu yapan çalışan adaylarının iş başvuru formlarına aydınlatma ve onay metni konulması, çalışanların açık rızalarının bilgilendirme ve onay formu ile alınması, işyerine gelen ziyaretçilerin güvenlik girişine asılan aydınlatma metinleri ve yaka kartlarına yazılan metinler ile aydınlatılması konularındaki uygulamaları aynıdır. Aynı şekilde iş başvuru formundaki fazlaya dair kişisel verilerin azaltılmasına yönelik olarak yapılan revizyonlar konusunda da benzerlik bulunduğu tespit edilmiştir. Örnek olay çalışması yapılan her iki işletmede de iş başvuru formlarında, sağlık verilerinin ayrıntısının sorulmadığı, eş bilgilerinde ayrıntı istenilmediği, dernek, vakıf ve sendika üyeliği ile ilgili bilgi istenilmediği tespit edilmiştir. Bununla birlikte işe alım uzmanlarının ya da iş görüşmesine katılan yönetici pozisyonundaki kişilerin iş görüşmelerinde kadın çalışan adaylarına ne zaman evlenecekleri? ya da evli iseler ne zaman çocuk yapacaklarına dair sorular sormadıkları yapılan tespitlerimiz arasındadır.

İşletmelerin özellikle çalışanlarının kimlik, iletişim, adres ve sağlık verilerini kanunlarda açıkça öngörülmesi halinde yetkili kişi ya da kuruluşlarla paylaştıkları tespit edilmiştir. Örneğin İş Sağlığı ve Güvenliği Kanunu gereğince işe giriş periyodik sağlık raporlarının işyeri denetimine gelen iş güvenliği müfettişleri ile ya da sigorta müfettişleri ile paylaştıkları aynı şekilde işyerinin yürütümü yönünden denetime gelen iş müfettişleri ile de 4857 sayılı İş Kanunu gereği (m.92) özlük dosyalarını paylaştıkları tespit edilmiştir.

Örnek olay çalışma yapılan işletmeler işyerinde 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 halinde, kimlik ve sağlık verilerini paylaştıkları görülmüştür. Örneğin

işyerinde vuku bulan bir iş kazasında kazazede işçinin kimlik ve sağlık bilgileri (kan gurubu gibi) hastanede sağlık görevlileriyle paylaşılmaktadır.

İşletmeler bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde de veri paylaşımında bulunmaktadırlar. Örneğin veri sorumlusu olan işverenler tedarikçileri, alt işverenleri ve müşterileri ile de yasal menfaatleri ve yasal yükümlülükler doğrultusunda sözleşmeler imzalamakta ve bu nedenle veri işlemekte ve yasal gereklilikler ve yasal menfaatler gereği ilgili kurum ve kuruluşlarla paylaşmaktadırlar.

Veri sorumlusu sıfatıyla işletmeler hukuki yükümlülüğünü yerine getirebilmek için zorunlu olması durumunda, çalışanlarının verilerini işlemektedir. Örneğin çalışanlarına aylık ücret ödenebilmesi için, banka hesap numarası, Aile Durum Bildirimi, daha önce başka bir işyerinde çalışması varsa mevcut SGK sicil numarası gibi kişisel verileri talep edilerek işlenmektedir. Bununla birlikte 1774 sayılı Kimlik Bildirme Kanunu gereğince işe giren veya çıkan işçilerin kimlik bilgilerini 3 gün içinde işyerinin bağlı bulunduğu kolluk birimlerine bildirerek kişisel verilerini hukuki yükümlülüğünü yerine getirmesi amacıyla paylaşmaktadırlar.

İşletmeler işe alım sürecinin sağlıklı bir şekilde yürütülmesi amacıyla hem bizzat iş başvurularını kabul etmekte hem de sosyal medyadan yararlanarak personel temin etmektedirler. Örneğin kariyer web sitelerinden ilgili kişilerin kendisi tarafından alenileştirilmiş verilerinden yararlanarak işe alım süreci yönetmektedirler.

İşletmeler, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumunda da ilgili kişilerin verilerini yetkili kişi ya da kuruluşlarla paylaşmaktadırlar. Örneğin, ispat niteliği taşıyan işçiye ait güvenlik bilgi ve belgelerini (sabıka kaydı, güvenlik soruşturma belgeleri gibi) polis, jandarma ve istihbarat birimlerinin talep etmesi halinde paylaşmaktadırlar.

İşletmeler, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun yasal menfaatleri için veri işlenmesinin zorunlu olması durumunda, işçilerin sağlık ve güvenliği ile işyeri güvenliğinin temini amacıyla, işyerine ait bina ve tesislerde güvenlik amaçlı olarak kamera kaydı uygulaması yapmaktadır. Bununla birlikte örnek olay çalışması yapılan her iki işletme ile işçileri arasında imzalanan iş sözleşmelerinde elektronik gözetleme ile ilgili aydınlatma ve onay hükümlerinin

bulunduğu aynı zamanda kamera konulan bölgelere de bilgilendirme levhası astıkları tespitlerimiz arasındadır.

Örnek olay çalışması yapılan işletmelerin işledikleri veriler sınıflandırıldığında yine benzerlik gösterdiği görülmektedir. Nihayetinde veri sorumlusu olan işletmelerin hepsi "İşletme Çalışanlarının Kişisel Verilerini Korunması Politikasını" oluşturdukları ve bu kapsamda çalışanlar, çalışan adayları, stajyerler, alt işveren çalışanları, ziyaretçiler, müşteriler, tedarikçiler ve üçüncü kişilerle tahditli olmak üzere, kimlik, iletişim, lokasyon, yakınlık, sağlık, fiziksel mekan güvenliği, finansal, görsel ve işitsel, özlük, özel nitelikli kişisel veriler (sabıka kaydı, sağlık bilgisi) ile talep ve şikayet verilerini işledikleri görülmektedir. İşletmelere giriş çıkışlar kartlı sistemle yapıldığından, özel nitelikli (hassas) kişisel veri niteliği taşıyan biyometrik veriler işlenmemektedir.

İşletmelerin işe giriş sistemlerinin kontrolünün sağlanması ve iş sağlığı ve güvenliği kayıtlarının elektronik ortamda tutulması ile ilgili yine ortak özellikler taşıyan sistemler kullanılmaktadır. Nitekim işyerine iş başı yapak üzere gelen kişinin kimlik bilgileri "Personel Devam Kontrol Sistemi"'ne (PDKS) girilmektedir. İş başı yapan personelin sağlık kontrol tarama verileri "İş Sağlığı Ve Güvenliği Sağlık Bilgi Yönetim Sistemi" ne (İBYS) girişi elektronik ortamda yapılmaktadır.

İşletmelerde kişisel veri işleme faaliyetleri kapsamında kurulan sistemler İnsan Kaynakları ve Bilgi İşlem Departmanları tarafından denetlenmektedir. Ancak bu konuda işletmeler arasında farklılıklar bulunmaktadır. Örneğin İşletme-1 İmalat San. ve Tic. A.Ş bünyesinde gerçekleştirilen kişisel veri işleme faaliyetleri İnsan Kaynakları Departmanı tarafından yürütülmekte iken İşletme-2 Gıda San. Ve Tic. A.Ş.'nin veri işleme faaliyetlerinin denetimi Bilgi İşlem Departmanları tarafından yürütülmektedir.

Örnek olay çalışması yapılan her iki işletmenin Bilgi İşlem Departmanlarında uzman ekipler görev yapmakta ve alınan teknik önlemler periyodik olarak işletme üst yönetimine raporlanmaktadır.

İşletmelerin teknik tedbirler kapsamında ortak yönlerinden birisi de bilgi güvenliği ve gizliliğin sağlanması için belirli periyodlarla kırılganlık zafiyet analizi ve sızdırmazlık testi yaptırmalarıdır.

Ortak olan yönlerden bir diğeri de kişisel verilerin bulunduğu veri tabanları yetki matrisi, güvenlik duvarı ve anti-virüs ile koruma altına alınmakta ve log yönetim sistemi uygulanmaktadır.

İşletmelerin bilgi işlem departmanlarına ait server odaları bulunmakta ve giriş çıkışlar elektronik kartla yapılmakta ve gerekli güvenlik tedbirleri alınmaktadır.

Örnek olay çalışması yapılan her iki işletmede insan kaynakları departmanları tarafından alınan idari önlemler açısından ortak olan yönler şöyle sıralanabilir;

- İşyerinde Kişisel Veri Envanteri hazırlanmıştır.
- Veri İşleme Politika Belgesi Oluşturulmuştur.
- Veri Saklama ve İmha Politikası Belgesi Oluşturulmuştur.
- Kamera İzleme Politika Belgesi Oluşturulmuştur.
- Veri siciline (VERBİS) kayıt yapılmıştır.
- Özlük dosyaları gözden geçirilerek gereksiz evraklar temizlenmiştir.
- İşyerinde kullanılan ve kişisel veri içeren tüm dokümanlar kişisel verilerin korunması hususunda revize edilmiştir.
- Kurumsal mail adreslerinin altına kişisel verilerin kullanılması ve gizliliği ile ilgili bilgilendirme metni konulmuştur.
- Kurumsal web sayfalarına kısa politika metni, aydınlatma metni ve başvuru formu konulmuştur.
- Veri işleyenlere farkındalık eğitimleri verilmiştir.
- Çalışanlar, kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmiş ancak eğitimleri henüz tamamlanmamıştır.

Örnek olay çalışma yapılan işletmelerin ortak özelliklerinden birisi de ağırlıklı olarak veri işlenen insan kaynakları, bilgi işleme, sağlık birimi (revir), idari işler ve arşiv birimlerinin giriş çıkış sistemlerinin benzerlik göstermesidir. Örneğin insan kaynaklarına girişlerde sadece İşletme-2'de kart sistemi uygulanırken İşletme-1'de giriş serbest olup elektronik kart uygulaması yapılmamaktadır. Ancak her iki işletmede de server odalarına ve revire girişler elektronik kart ile yapılmakta olup, idari işler ve arşivlere girişler için özel önlemler alınmamıştır.

5. SONUÇ VE ÖNERİLER

İşletmelerde Kişisel Verilerin Korunmasında İnsan Kaynakları ve Bilgi İşlem Departmanlarının Rolü: Özel Sektör İşletmeleri Örnek Olay Çalışmaları başlıklı tez çalışmasında, sahada yapılan örnek olay çalışmaları sonucunda Kişisel Verilerin Korunması Kanunun yürürlüğe girdiği 7 Nisan 2016 tarihinden itibaren yükümlülük altında bulunan işletmeler ciddi anlamda idari ve teknik tedbir almışlar ve özellikle veri işleyenlerin farkındalık düzeylerini artırarak eğitimlerini sağlamışlardır. 6698 sayılı Kanuna aykırı davranılmasının işletmeler açısından ağır idari, hukuki ve cezai yaptırımlar getirmesi caydırıcı bir unsur olarak görülmektedir. Nitekim Kanuna aykırılığın 1 milyon TL ye varan idari para cezalarının yanısıra kişisel verilerin hukuka aykırı olarak ele geçirilmesi, bir başkasına verilmesi, yayılması, sosyal medyada paylaşılması, süresi içinde silinmemesi ya da imha edilmemesi durumunda, Türk Ceza Kanunda 1 yıldan 4 yıla kadar hapis cezasını gerektiren cezalar öngördüğü (m.135-138) ve kişisel verisinin hukuka aykırı olarak işlenmesi ve veri sahibinin kendisine zarar verici nitelikte bir başkalarıyla paylaşılması durumunda ise Türk Borçlar Kanunu açısından veri sahibinin maddi ve manevi tazminat talebinde bulunabileceği düzenlenmiştir (m.49-56) .

6698 sayılı Kanun 50'den fazla işçi çalıştıran veya yıllık 25 milyon TL'den fazla cirosu olan işyerlerine VERBİS sistemine kayıt zorunluluğu getirmiştir. Bununla birlikte VERBİS'e kayıt yükümlülüğü olmasa bile diğer işyerlerinin 6698 sayılı Kanunun öngördüğü diğer yükümlülükleri yerine getirmek zorundadırlar. Bu kapsamda örnek olay çalışması yapılan biri tekstil diğeri gıda sektöründe faaliyet gösteren iki işletmenin 50'den fazla işçi çalıştırması nedeniyle VERBİS sistemine kayıt yaptırdıkları ve 6698 sayılı Kanunun öngördüğü idari ve teknik tedbirleri aldıkları tespit edilmiştir.

6698 sayılı Kanun esas alındığı için işletmelerin aldıkları idari ve teknik tedbirlerin büyük bir çoğunluğunun birbiriyle aynı oldukları gözlenmiştir. İnsan kaynakları ve bilgi işlem departmanlarının kişisel verilerin yoğun olarak işlendiği birimler olduğu düşünüldüğünde, idari tedbirlerin insan kaynakları departmanınca, teknik tedbirlerin

de bilgi işlem departmanınca alındığı görülmektedir. Konunun kişisel verilerin korunması olması nedeniyle işe alım sürecinden itibaren kişisel verileri işleyen insan kaynakları departmanının bu alanda önemli rol üstlendiği ve bilgi güvenliğinin sağlanmasında temel rol oynadığı bir gerçektir. Çünkü işe alım, işin devamı ve işin sonlanması süreçlerinin yönetimi ve özlük dosyalarının tutulması insan kaynaklarının görevleri arasındadır. Performans sisteminin kurulması ve yönetilmesi, iş uyuşmazlıklarının çözümü, işyerinde izin, disiplin, İSG gibi kurulların sağlıklı bir şekilde yürütülmesi konusunda etkin görevler alan insan kaynakları çalışanları kişisel verilerin hukuka uygun olarak işlenmesi, güvenli bir şekilde saklanması ve kişisel veri içeren belgelerin saklama sürelerinin belirlenmesi ve saklama süresi dolan verilerin silinmesi, yok edilmesi ya da anonim hale getirilmesi aşamalarında etkin rol oynamaktadır.

İnsan kaynakları bir nevi kişilerin o işletmedeki sırdaşı konumundadır. Çünkü özlük dosyalarının oluşturulması görevleri nedeniyle çalışanların kimlik, iletişim, imza, görsel ve işitsel, adres, aile ve yakınlık, sağlık, eğitim, güvenlik ve biyometrik verilerine sahip olmaktadırlar. Bununla birlikte iş başvurusu yapan çalışan adaylarının, stajyerlerin ve işyerine gelen ziyaretçilerin de benzer nitelikteki kişisel verilerini işlemektedirler. Ayrıca tedarikçi ve alt işverenlerle kurulan iş ilişkisi nedeniyle veri işleme süreci burada da devam etmektedir. Elbette ki insan kaynakları çalışanlarının işten ayrılmalarından sonra da edindikleri kişisel verilerin saklanması konusundaki sorumlulukları devam etmektedir. Bu sorumluluk işçinin sır saklama borcu kapsamında değerlendirilmektedir.

İşletmelerde bilgiler artık çoğunlukla elektronik ortamlarda tutulmakta ve saklanmaktadır. Çağımız dijital değişim ve dönüşüm çağıdır. Endüstri 4.0 ‘ın konuşulduğu dünyamızda artık akıllı fabrikalar, karanlık fabrikalar, robotlar, yapay zekâ, nesnelerin interneti gündemi oluşturmaktadır. Bilgi, hızla akmakta ve kontrolü zorlaşmaktadır. İşte bu aşamada kişisel verilerin korunması konusu büyük önem arz etmektedir. Özellikle işletmelerde bu konuda yeterli güvenlik tedbirlerinin alınması konusunda Bilgi İşlem Departmanlarına önemli görevler düşmektedir. Zira işyerine ilk giriş noktası olan güvenlik noktasında elektronik gözetleme başlamakta ve yine bu noktada kimlik paylaşımı yapılarak elektronik ortama aktarılmaktadır. Verinin kaydedilmesinden sonra kimlerin bu verileri görmesi gerektiğine dair üst yönetimin

kararı doğrultusunda önlem alma ve yetki matrisi oluşturma görev ve yetkisi bilgi işlem departmanına aittir.

Personel Devam Kontrol Sistemi PDKS, Özlük İşlemlerinin takip edildiği NETSİS ve SAP gibi programların sağlıklı bir şekilde işletilmesi ve bu programlara işlenen verilerin yedeklenmesi ve güvenliğinin sağlanması konusunda önemli rol oynamaktadırlar. Özellikle işyerinde saklanan verilerin iç ve dış ataklara karşı güvenliğinin sağlanması için güvenlik duvarı oluşturulması, bilgi güvenliği ve gizliliğini sağlamak amacıyla kırılganlık zafiyet analizi ve sızdırmazlık testi yapılmasını temin etme görevi de bilgi işlem departmanının görevleri arasındadır.

Örnek olay çalışması yapılan işletmelerden yola çıkılarak işletmelere yapılacak önerilerimizin başında 27001 Bilgi Güvenliği Yönetim Sisteminin işyerlerinde oluşturulması gelmektedir. Çünkü araştırma yapılan her iki işletmede de henüz bu sistem oluşturulmamıştır. Aynı zamanda fiziki mekân güvenliğinin sağlanması için de gerekli tedbir alınmalıdır. Örneğin en yoğun kişisel veri işlenen insan kaynakları, bilgi işlem, revir, idari işler ve arşiv gibi birimlere giriş çıkışların elektronik kart ile yapılması önerilmektedir. Farkındalığın artırılması için kişisel verilerin korunması konusunda verilen eğitimler sadece veri işleyenlere değil, işyerindeki tüm çalışanlara yönelik olmalıdır. Veriyi işleyen kadar verisi işlenen de bu konularda bilinçlendirilmelidir. İşe başlatılmak üzere davet edilen çalışanlardan özel nitelikli kişisel veri olarak nitelendirilen adli sicil belgesi istenilmeli görüldükten sonra özlük dosyasında arşivlenmeden geri verilmelidir. Adli sicil belgesi arşivlenecek meslekler tahditli olmalıdır. Örneğin güvenlik personeli, insan kaynakları, bilgi işlem ve yönetici konumundaki kişiler dışında adli sicil belgeleri sadece görülmeli, arşivlenmemelidir.

İşyerine girişte alınan kimliklerin bilgileri alındıktan sonra ziyaretçilere geri iade edilmeli, güvenlik noktasında alıkonulmamalıdır. Kişisel Verilerin Korunması Kanununa göre, veri sahiplerinden fazlaya dair bilgi ve belge istenmemelidir. Gereğinden fazla bilgi ve belgeler risk oluşturacağından, riskin değerlendirilip minimize edilmesi ve tehlikenin ortadan kaldırılması gerekir. Bu kapsamda işyerine giriş ve çıkışlarda işyeri güvenliği açısından ziyaretçilerden istenilen kimlik belgeleri, manuel ya da elektronik ortamda işlendikten sonra, güvenlik noktasında alıkonulması yerine kimlik sahibine verilerek, riskin minimize edilmesi gerekmektedir. Kurumsal mailler ve telefonların özel işlerde kullanılmasının önlenmesi için gerekli tedbirler alınmalıdır. Özellikle işçilerin işten ayrıldıktan sonra teslim ettikleri kurumsal

maillerin içerisinde bulunan kişisel veriler temizlendikten sonra bir başkasına tahsis edilmelidir.

Veri güvenliğinin oldukça önem kazandığı günümüzde işletmeler; edindikleri kişisel verilerin güvenliğini sağlamak için yeni güvenlik stratejileri geliştirmeli ve gerekli önlemleri almalıdırlar. Data Loss Prevention (DLP), işletmelerin hassas verilerinin, işletme içinde nasıl yer değiştirdiğini gözleyen ve kontrollü bir şekilde; "dışarı sızmalarını" engelleyen bir teknoloji olması nedeniyle mutlaka bu yazılımın edinilmesi önerilmektedir.

KAYNAKLAR

Adalı, E. (2016). *Bilgisayar ve Bilgi Güvenliği Yönetimi, Şifreleme Yöntemleri*, İstanbul: Özkaracan Matbacılık.

Aktay , A. N. ve diğerleri (2013). *İş Hukuku*, 1. Bası, Ankara.

Alp, M. (2014). *"Yeni Borçlar Kanunu'nun İş Hukukuna Etkileri", İzmir Barosu İş Hukuku Günleri-II, Sempozyum, 10-11 Mayıs 2013, İzmir 2014 (118-134.)*

Arslan, İ. (2018). Türk Tekstil ve Hazır Giyim Üreticilerinin Uluslararasılaşması Süreci: Çoklu Vaka Araştırması, İstanbul Sebahattin Zaim Üniversitesi Sosyal Bilimler Enstitüsü, *Yayınlanmamış Yüksek Lisans Tezi*. İstanbul.

Aydınlı, İ. (2004). *İşverenin Sosyal Temas ve İş İlişkisinden Doğan Edimden Bağımsız Koruma Yükümlülükleri ve Sonuçları*, Ankara, (Edimden Bağımsız Koruma).

Ayözger, A.Ç. (2016). Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, *Doktora Tezi,* İstanbul.

Bellia, P.L., Berman, Paul, S.C. ve David, C. (2003). *Problems of Policy and Jurisprundence in the Information Age,* Thomson-West.

Bennett, C.J. (1992). *Regulating Privacy, Data Protection and Public Policy in Europe and the United States*, Cornell University Press,

Cadaoux, L. (1998). *Privacy: Our Future Under Close Surveillance, Freedom of Expression,* IQ Collectif, Kanada.

Canavan, J.E. (2001). *Fundamentals of Network Security*, Basic Security Concepts, USA: Canavan.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, *Politeknik Dergisi*, 9(3).

Cate, F.H. (1997). *Privacy in the Information Age*, Brookings Institution Press, ABD.

Cate, F.H. (2001). *Privacy in perspective*. American Enterprise Institute.

Civelek, D.Y. (2011). Kişisel Verilerin Korunması ve Bir Kurumsal Yapı Önermesi, *Uzmanlık Tezi,* **T**.C. Başbakanlık Devlet Planlama Teşkilatı Müşteşarlığı. Ankara.

Cole, E., Krutz, R. ve Conley, J.W. (2005). *Network Security Bible, Information System Security Principles,* Indianapolis: Wiley.

Çekin, M.S. (2016). *Tehlike Sorumluluğu (6098 sayılı Türk Borçlar Kanunu Madde 71 Çerçevesinde).* İstanbul: On iki levha yayıncılık.

Çölkesen, R. (2006). *Rifat Çölkesen. Türkiye Bilişim Ansiklopedisi. İstanbul: Papatya, (879-883).*

Deibert, R., Palfrey, J., Rohozinski,R. Zittrain, J. (2008*).eds., Access Denied: The Practice and Policy of Global Internet Filtering,* (Cambridge: MIT Press)

DiMartino, A. (2005). *Datenschutz im europäischen Recht*, Nomos, 20

Dülger, M.V. (2018). *İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması.*

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, 14(4), 532-550.

Eisenhardt, K. M. ve Graebner, M. E. (2007). Theory Building From Cases: Opportunities and Challenges, *Academy of Management Journal*, 50(1), 25-32

Ersoy, E. (2007). Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması. *Akademik Bilişim Konferansı 2007.*

Ertürk, Ş. (2002). *İş İlişkisinde Temel Haklar*, Ankara.

Eyrenci, Ö. (1991). İşe Girişte Personel Seçimi ile İlgili Hukuki Sorunlar. *İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi,* 15.

Garrie, D.B. ve Wong, R. (2006). The future of consumer web data: a european/us perspective. *International Journal of Law and Information Technology*, 15(2).

Hekimler, A. (2004). *Çalışma ve Toplum Dergisi*, 3(3).

Hekimler, A. (2011). *Çalışma ve Toplum Dergisi*, 11(3).

Henderson, H. (2006). *Privacy in the Information Age*, Facts of File, ABD.

Hoofnagle, C.J. (2005). *Privacy Self-Regulation: A Decade of Disappointment*,

İş Hukuku ve Sosyal Güvenlik Hukuku (1991) *Türk Milli Komitesi 15. Yıl Armağanı,* İstanbul.

Jay, R. (2007). *Data Protection Law and Practice,* Fourth Edition, London, Sweet & Maxwell.

Kang, J. (1998). Information Privacy in Cyberspace Transactions, *Stanford Law Review,* 50.

Kaplan, Y. (2004). *İnternet Ortamında Fikri Hakların Korunmasında Uygulanacak Hukuk,* Ankara: Seçkin yayıncılık.

Karabulut, R. (2014). Kişisel Verilerin Korunması ve Kolluk Hizmetleri, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, *Yüksek Lisans Tezi,* Diyarbakır.

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61(3).

King, R. ve Stansfield, W.D. (1997). *Dictionary of Genetics*, Oxford University Press, 5. Baskı, Buyuk Britanya.

Koops, B.P. ve Leenes, R. (2009). *'Code' and the Slow Erosion of Privacy*, bepress.

Kuşkonmaz, E.M. (2018). *Kişisel verilerin Türk Ceza Kanunu kapsamında korunması.*

Küzeci, E. (2010). *Kişisel Verilerin Korunması*, Ankara: Turhan Kitabevi Yayınları.

KVKK (2016). *6698 Sayılı Kişisel Verilerin Korunması Kanunu*, metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, Erişim Tarihi: 18.02.2019.

KVKK, (2017). *Kişisel Verileri Koruma Kurumu* https://www.kvkk.gov.tr/Icerik/ 41 13/2017-61, Erişim Tarihi 15.02.2019

Lipschultz, H.S. (2000). Free Expression in the Age of the Internet, *Social and Legal Boundaries,* Westview Press, ABD.

Lloyd, I.J. (2017). *Information Technology Law*. Oxford University Press.

Löwisch, M., Caspers, G. and Klumpp, S. (2014). *Arbeitsrecht,* 10. Auflage, M

Lyon, D. (2006). 9/11, Synopticon, and scopophilia: Watching and being watched. *The new politics of surveillance and visibility*.

MacRonin, R. (2008). *Electronic Data Recorders in Vehicles*.

Magee, J. (2002). *Freedom of Expression,* Grenwood Press, ABD.

Manav, A.E. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 19(2).

Marx, G.T. (1988). *Undercover: police surveillance in America*. Univ of California Press.

Miller, A.R. (1971). *The Assault on Privacy, Computers, Data Banks, and Dossiers*, The Univercity of Michigan Press, ABD.

Odaman, S. (2002) İşçinin İşe Başvurusu Sırasında İşvereni Yanıltması ve Hukuki Sonuçları, *Tekstil İşveren Dergisi*, 274

Okur, Z., (2011). *İş Hukukunda Elektronik Gözetleme*, Legal Yayınları Ekim 2011.

Özdemir, H. (2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Ankara: Seçkin Yayınları.

Samuelson, P. (2000). Privacy As Intellectual Property, *tan. L. Rev.* 1125.

Savaş, B. (2009). İş Hukukunda Siber Gözetim, *Çalışma ve Toplum Dergisi*, 3.

Schneier, B. (2014). *Secrets and Lies, Digital Security in a etworked World, with new information about post-9/11 security*, Wiley, ABD.

Sever, H. ve Tonta, Y. (2006). Arama Motorları, *Türkiye Bilişim Ansiklopedisi*, İstanbul: Papatya yayıncılık.

Sevimli, A. (2008). İşçinin Özel Yaşam Hakkı Bağlamında İşçi–İşveren İlişkisi. *Sicil İş Hukuku Dergisi,* Yıl, 3.

Slay, J. ve Koronios, A. (2006). *Information Technology Security & Risk Management, Basic Cryptography and Public Key Infastructure*, Australia: Wiley

Solove, D.J. (2004). Reconstruncting Electronic Surveillance Law, *The George Washington Law Review.*

Sözer, A.N. (1982). Hamilelik ve İş Hukukunda Sonuçları, *Adalet D.*, C.73 S.6 (1049-1069).

Steeves, V. (2000). *Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace, Human Rights and the Internet*, Macmillan Press, Birleşik Krallık.

Şahin, O. (2011). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Saklanması ve Gizliliğin Korunması, *Bilişim Uzmanlığı Tezi*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Tansuğ, A. (2006). AB'nin Yeni Ekonomi Silahı: "Veri Saklama Hukuku", *Bilişim Hukuku,* Kadir Has Üniversitesi Yayınları, İstanbul.

TBD, (2008). *Kişisel Verilerin Korunması ya da Kişisel Verilerin İşlenmesi Karşısında Bireyin Korunması*, Ankara: Türkiye Bilişim Derneği.

TDK, (2019). *Türkçe Sözlük*: http://www.tdk.gov.tr

Uncular, S. (2014). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Ankara, Seçkin Yayıncılık.

Vural, Y. ve Sağıroğlu, Ş. (2010). Veri tabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri, *Politeknik Dergisi,* 13(2).

Yıldırım, A., & Şimşek, H. (2008). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (6. Baskı). Ankara: Seçkin Yayıncılık

Yılmaz, M. (2009). Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi, *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi,* 49(1).

Yin, R. K. (2009). *Case Study Research: Design and Methods*, SAGE publications.

Yüksel, S. (2012). *Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale*, İstanbul, Beta Yayınları.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı **:** E. Kübra İNCİROĞLU

Doğum Tarihi **:** 17.03.1989

Doğum Yeri **:** Alaca

İletişim Bilgileri

Adres **:** Atakent Mah. İstanbul Sarayları Hisar Kule-1 No: 26/52 Küçükçekmece/İSTANBUL

Cep **:** 0505 572 88 63

E-Posta **:** k.inciroglu@hotmail.com

İş Deneyimi

Ocak 2015 İnsan Kaynakları Sorumlusu
Trakya Polatlı Cam Sanayii A.Ş.- Şişecam

Kasım 2015- Uzman
Türk Hava Yolları A.O/ Endüstriyel İlişkiler ve Ücret Md.

Eğitim Bilgileri

Üniversite (Lisans)

08.2009-07.2013 Gazi Üniversitesi-İktisadi ve İdari Bilimler Fakültesi
Çalışma Ekonomisi ve Endüstri İlişkileri (Türkçe)

Lise

06.2007 1. Murat Lisesi (Edirne)
Türkçe – Matematik

Yabancı Dil

İngilizce	Okuma	Yazma	Konuşma
	Orta	Orta	Orta

Sertifika Bilgileri

İngilizce Kursu Bitirme Sertifikası

English Center / Malta- 08.2011

Malta'da 3 ay süreli İngilizce eğitim ve kültürel değişim programına katıldım.

Yetkinlikler

Bilgisayar Bilgileri: İnternet, Windows, MS Office, SAP