Uluslararası Sosyal Araştırmalar Dergisi / The Journal of International Social Research
Cilt: 12 Sayı: 65 Ağustos 2019 Volume: 12 Issue: 65 August 2019
www.sosyalarastirmalar.com Issn: 1307-9581
Doi Number: http://dx.doi.org/10.17719/jisr.2019.3552

İNSAN KAYNAKLARI VE BİLGİ İŞLEM DEPARTMANLARININ İŞLETMELERDE KİŞİSEL VERİLERİN KORUNMASINDAKİ ROLÜ: FARKLI SEKTÖRLERDEN ÖRNEK OLAY ÇALIŞMALARI•

THE ROLE OF HUMAN RESOURCES AND INFORMATION TECHNOLOGIES DEPARTMENTS IN PROTECTION OF PERSONAL DATA IN BUSINESS: CASE STUDIES FROM DIFFERENT SECTOR

E. Kübra İNCİROĞLU**
Ercan ÖGE***

Öz

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 bağlamda çalışmanın temel amacı, 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 konulmasıdır. Çalışmada, ülkemizin önde gelen köklü, alanında oldukça tecrübeli, ölçek olarak büyük işletme olarak ifade edilen birisi tekstil diğeri de lojistik işletmesi olmak üzere iki işletmesi incelenmiştir. Çalışmada yöntem olarak örnek olay(vaka) yöntemi kullanılmış, bu amaçla iki farklı işletme incelenmiştir. Literatür taraması ve görüşme yoluyla ile de elde edilen veriler sonucunda çalışma nitel bir değerlendirmeye tabi tutulmuştur.

Anahtar Kelimeler: Kişisel Verilerin Korunması Kanunu, İnsan Kaynaklarının Departmanının Rolü, Bilgi İşlem Departmanının Rolü.

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.

Regarding to this, the main goal of the study is the evaluation of the roles and responsibilities of the human resources and IT departments for the saving and protecting of personal data inline with legal boundaries and types of precautions accordingly. One big scale textile and one big scale logictics company which is prominent and experienced in their sectors have been analyzed in the scope of the study. Case methodology has been applied in this study by analyzing two companies. According to the literature research and interview-based data, the study has been subjected to a qualitative evaluation.

Keywords: Law on the Protection of Personal Data, Role of the Human Resources Department, Role of the IT Department

---

• Bu çalışma, İstanbul Aydın Üniversitesi Sosyal Bilimler Enstitüsü İnsan Kaynakları Yönetimi Anabilim dalında, 2019 yılında, Dr. Ercan ÖGE danışmanlığıyla kabul edilmiş olan "İşletmelerde Kişisel Verilerin Korunmasında İnsan Kaynakları ve Bilgi İşlem Departmanlarının Rolü: Özel Sektör İşletmeleri Örnek Olay Çalışmaları" adlı yüksek lisans tezindeki örnek olay çalışması yapılan işletmeler dışında, farklı iki özel işletmede örnek olay çalışması yapılarak türetilmiştir

** İstanbul Aydın Üniversitesi, Sosyal Bilimler Enstitüsü, emineinciroglu@stu.aydin.edu.tr
*** Dr. Öğr. Üyesi, İstanbul Aydın Üniversitesi, İnsan Kaynakları Yönetimi Programı, eoge@aydin.edu.tr

1. Giriş

Dijital değişim ve dönüşüm; sosyal, kültürel ve ticari ilişkilerin yanı sıra topludaki bireylerin yaşam tarzını da önemli ölçüde değiştirmiş ve değiştirmeye devam etmektedir. Bu durum beraberinde toplumdaki bireylerin aile mahremiyetinin korunması sorununu da beraberinde getirmektedir. Zira kişilerin temel hak ve özgürlüklerinin korunması kapsamında kişisel verilerin güvenliğinin sağlanması da gündemi meşgul eden önemli konulardan biri haline gelmiştir. Teknolojik gelişmeler ışığında ekonomik ve sosyal hayata ilişkin birçok konuda yapılan iş ve işlemler artık elektronik ortamda yapılmakta ve hemen her alanda hizmetlerin sunulması aşamasında hizmet alanların kişisel verilerine başvurulmakta ve elde edilen veriler başkalarıyla da paylaşılabilmektedir.

Günümüzde kişiler yaptıkları hemen her faaliyette kişisel verilerini kullanmak ya da bunların işlenmesine izin vermek zorunda kalmaktadırlar. Ancak kişisel verilerin bu kadar sık kullanılması ve özellikle kolay paylaşılır hale gelmesi çeşitli sorunları da beraberinde getirmektedir. Kişisel verilerin gerçek kişiler için alenileştirilmesi, bireyin sosyal yaşamını etkileyebileceği gibi dolandırılmasını ya da izlenebilmesini de mümkün hale getirmektedir.

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.

İşletmeler bakımından konu değerlendirildiğinde verilerin hangi biçimlerde güvenli bir şekilde saklanacağı ya da korunacağı konuları gizlilik kadar önem arz etmektedir. Kişisel verilerin korunması noktasında, bu makalede incelenecek temel konu işletmelerde kişisel verilerin korunması hususunda veri sorumlusu sıfatına haiz olan tüzel kişi işverenlerin ve onlar adına veri işleyen konumundaki İnsan Kaynakları ve Bilgi İşlem Departmanlarının uygulamaları ve bu konularda üstlendikleri rollerdir.

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 İnsan Kaynakları ve Bilgi İşlem Departmanları tarafından nasıl yönetileceği hususları ortaya konulacaktır.

2. Kişisel Verilerin Korunmasına Yönelik Bilgiler

2.1 Kişisel Veri Kavramı

6698 sayılı Kişisel Verilerin Korunması Kanunu m.3 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 gerekçesine bakıldığında ise kişisel veri kavramına örnek olarak; kişilerin adı ve soyadı, doğum yeri ve tarihi, kişilerin ailesine, fiziki durumuna, ekonomik ve sosyal durumuna ait bilgiler gösterilmiştir (6698/ m.3). Elde edilen bir veri neticesinde kişinin kim olduğunun anlaşılması mümkün hale geliyorsa kişisel veri olarak kabul edilmektedir. Kanunun madde gerekçesinde yer verilen belirlenebilir ifadesi ile ne anlatılmak istendiği aşağıda verilen örneklerle açıklanmıştır. Buna göre;

> "*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 Kanun Gerekçe m.3).

Bu tanımdan yola çıkarak, bir verinin kişisel veri olarak kabul edilmesi için iki husus ön plana çıkmaktadır. Bunlardan ilki; söz konusu verinin gerçek bir kişiye ait olması, ikincisi de bu veri doğrultusunda kişinin belirlenebilir olmasıdır. İlgili kanun gerekçesinde yer aldığı üzere, bireylerin kişisel, fiziksel, karakteristik, ailevi ve mesleki özelliklerini belirten bilgiler ışığında bireylerin diğer insanlardan ayrılmasına yol açan tüm veriler kişisel veri olarak kabul edilmektedir (6698/m.3). Söz konusu veriler kişilerin dini inançlarını, felsefi görüşlerini, etnik kökenini, sağlık durumunu, cinsel tercihlerini, iletişim bilgilerini, sosyal güvenlik bilgilerini, pasaport bilgilerini, üye olduğu dernek, vakıf ve sendikalar ile banka bilgilerini de içerebilmektedir (6698 sayılı Kanun Gerekçe m.6).

AB ülkeleri adına kişisel verilerin işlenmesine yönelik olarak düzenlenmiş olan Kişisel Veri Koruma Tüzüğü (GDPR) ile 6698 sayılı Kanunda yer alan tanımlar arasında paralellik söz konusudur. Türkiye'de kişisel verilerin korunması hukukunda temel düzenleme olarak kabul edilen 6698 sayılı Kanun'un amacı,

kapsamı ve hükümleri birlikte değerlendirildiğinde 1995/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi ile büyük ölçüde paralellik taşımaktadır. Bununla birlikte, 6698 sayılı Kanun'un Resmî 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 direktifte yer alan hükümlerin modernize edilmesi ve güncellenmesi amaçlanmıştır. Bu çerçevede, 6698 sayılı Kanun'un 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.

2.2 Kişisel Veri Türleri

2.2.1 Hassas (Özel Nitelikli) Kişisel Veriler

1995/46/EC sayılı Direktif 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, 2011, 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: 08.05.2019). 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.

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 6698 sayılı Kanun 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 sayılı Direktif 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, 1995/46/EC sayılı Direktif m.9'da da düzenlenmiş ve söz konusu madde 1995/EC VKD m. 8'i temel almıştır.

1995/46/EC sayılı Direktif m.8/1'de ise içeriğinde ırka, etnik kökene, düşünce özgürlüğüne ve genel sağlık durumuna ilişkin veriler, hassas kişisel veriler grubu içerisinde değerlendirilmektedir. Anılan direktifte 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, 2011, 787). Direktif 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, Çek Cumhuriyeti'nde 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 farklı 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).

6698 sayılı Kanun 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 engel durumları, Polonya'da bağımlılıkları, İzlanda'da bireylerin ilaç kullanımları bu grup içerisinde değerlendirilmektedir (Özdemir, 2009, 64).

Hassas kişisel verilere örnek olarak ise; işveren tarafından işgörenin 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.

6698 sayılı Kanun m.6'nın 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 (Özdemir, 2009, 58).

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 (Özdemir, 2009, 58).

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 (Özdemir, 2009, 58).

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."

2.2.2 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 6698 sayılı Kanun'da yer alan özel hükümler doğrultusunda değil, genel hukuka uygunluk nedenleri kapsamı içerisinde işlenebilmektedir. Aslına bakıldığında 6698 sayılı Kanun, hassas ve hassas olmayan verilerin işlenmesine ilişkin unsurlar arasındaki ayrımı asgari seviyelere indirmiş olsa da teorik olarak böyle bir ayrım yapılmaktadır.

2.2.3 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.

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 çıkarılmıştır (Dülger, 2018, 72)

1982 Anayasası incelendiğinde aslında birçok temel hak ve özgürlüğün kişisel verilerle ilgili olduğu görülmektedir. Anayasada yer alan; özel hayatın gizliliği, haberleşme özgürlüğü, din ve vicdan özgürlüğü, düşünce ve kanaat özgürlüğü vb. birçok hakkın doğrudan kişisel verilerle bağlantılı olduğu anlaşılmaktadır. Anayasa m.22'de 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 Sözleşmesi m.8'de 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 verilerin korunması ile birlikte özel hayatın gizliliği, Anayasa m.20'de güvence altına alınmıştır. 12 Eylül 2010 tarihinde yapılan halkoylaması sonucu kabul edilen 5982 sayılı Kanun'la yapılan Anayasa değişikliği ile Anayasa m.20'ye 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.

Anayasa m.2/3'de kişisel verilerin korunması öngörülmektedir. Ayrıca kişisel verilerin hukuka aykırı olarak işlenmesi, Anayasa m.17 ile güvence altına alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı ile Anayasa m.20 ve 22'de düzenlenen özel hayatın gizliliği ve korunması hakkının ihlali anlamına da gelmektedir.

Anayasa m.20/3'de, 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 (İnciroğlu, 2018, 8).

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.

3. İş Sözleşmesinin Devamında Kişisel Verilerin Korunması

3.1 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, 2011, 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 İş Kanunu m.75 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 üçüncü kişilere aktarılmaması gerekmektedir (Sevimli, 2008, 146).

3.2 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).

3.3 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. (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 borcundan 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).

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).

3.4 Çalışanlara Ait Bilgilerin Yeni İşverenlerle Paylaşılması

Çalışanların iş sözleşmeleri devam ederken farklı bir işyerinde çalışmak üzere başvuruda bulunması durumunda, 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.

3.5 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 belirli bir süre de olsa saklanması işverenlerin de lehine olabilmektedir. Öyle ki, mesai ücretleri, fazla ücret vb. 5 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).

4. İnsan Kaynakları ve Bilgi İşlem Departmanlarının Kişisel Verilerin Korunmasındaki Rolü

4.1 İnsan Kaynakları Departmanlarının Kişisel Verilerin Korunmasındaki Rolü

İnsan kaynakları departmanları görevlileri o işletmede çalışan kişilerin bir nevi sırdaşı konumundadır. İşe alım sürecinden başlayarak işin devamı ve sonlanmasına kadar ki süreçte insan kaynakları personeli, kişisel verilerin işlenmesinde odak noktayı oluşturmaktadır.

Öncelikle insan kaynakları departmanlarında görevli işe alım uzmanlarının ya da bu konuda görevli insan kaynakları personelinin iş görüşmelerinde ve özgeçmişlerin değerlendirilmesi sürecinde önemli rol üstlenerek yoğun kişisel veri işledikleri bilinen bir gerçektir. İş başvuruları alınan çalışan adaylarının kişisel veri içeren başvuru evraklarının güvende tutulması, saklama sürelerinin belirlenmesi ve süresi dolan

belgelerin silinmesi, yok edilmesi ya da anonim hale getirilmesinde önemli roller üstlenmektedirler. İşyerinde oluşturulan CV havuzlarındaki bilgilerin güvenliğinin sağlanması için elektronik ortamda ise teknik tedbirlerinin, kâğıt ortamda saklanıyor ise, fiziki tedbirlerin alınması insan kaynaklarının görevleri arasındadır.

İşe alım sürecinde referans araştırmaları yapılırken, adayın yazdığı referansların aranmasında bir sakınca olmamakla birlikte, adayın kendisinin yazılı onayı olmayan referansların aranmasının KVKK'ya göre yasal olmayacağı, insan kaynaklarının bu yönünde hareket etmesi gerekmektedir. Bu konuda işe alım uzmanlarının da özel eğitim alması gerektiği açıktır.

İnsan kaynakları departmanlarının temel görevlerinden birisi de özlük dosyalarının oluşturulmasıdır. Görevleri nedeniyle çalışanların kimlik, iletişim, imza, görsel ve işitsel, adres, aile ve yakınlık, sağlık, eğitim, güvenlik ve biyometrik verilerini hem manuel olarak hem de elektronik ortamda işlemektedirler. Bununla birlikte insan kaynakları departmanı stajyerlerin de benzer nitelikteki kişisel verilerini işlemektedirler. Ayrıca tedarikçi ve alt işverenlerle kurulan iş ilişkisi nedeniyle veri işleme süreci burada da devam etmektedir.

Kişisel verilerin korunması kapsamında işe başlatılacak adaylardan lüzumundan fazla belge istenilmemesi ayrıca önem arz eden hususlardan birisidir. Nitekim özlük dosyalarında arşivlenecek belgelerin genel ve özel nitelikli kişisel veri içeriyor olması veri güvenliğinin sağlanması açısından risk oluşturacağından, riskin değerlendirilmesi ve gereksiz ve fazlaya dair belgelerin arşivlenmemesi konusunda gerekli hassasiyetini gösterilmesi de insan kaynaklarının görevlerindendir. Bu kapsamda işletmelerde insan kaynakları departmanları kişisel verilerin korunması hususunda idari, fiziki ve hukuki tedbirler almakla yükümlüdürler.

Bu kapsamda veri sorumlusu olan işveren adına veri işleyen konumunda olan insan kaynakları personeli, verisi işlenen tüm kişileri, insan kaynakları departmanında hukuka uygun veri işlendiği konusunda bilgilendirmeli, veri işleme amacını ve verilerin ne kadar süreyle saklanacağını, veri sahiplerinin haklarını ve hakların korunması için başvuru yollarını içeren yeterli bilgilendirmeler yaparak, farkındalık düzeylerini artırıcı gerekli eğitimleri düzenleme misyonuna sahiptir.

İnsan kaynakları departmanı, işletme çalışanlarının kendisine ait bilgiler hakkında devamlı bilgi alma özgürlüklerinin bulunduğu ve gerek duymaları halinde bu bilgileri değiştirebilecekleri hususunda, departmana nasıl başvuruda bulabilecekleri ve hangi süre içinde cevap alabilecekleri konularında da yeterli bilgilendirmeleri yapmakla yükümüdürler.

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 (Ayözger, 2016, 120-121). İşte insan kaynakları departmanı bu sürecin sağlıklı bir şekilde yürütülmesinde etkin rol oynamakta ve sorumluluk üstlenmektedir.

İşletmelerin 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. Kişiler ise istedikleri her an bu önlemlerin detayları ile ilgili bilgi alma hakkına sahip olmaktadır (Kılınç, 2012, 1112).

İşletmelerin insan kaynakları departmanları tarafından kişisel veri yönetimine dair geliştirilen politikaların vazgeçilemez unsurları içerisinde amaca bağlılık unsuru da 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, 2013, 89). Bu bağlamda insan kaynakları departmanı amaca uygun veri işleme konusunda önemli rol üstlenmektedir.

İnsan kaynakları departmanları veri sahiplerinden özellikle özel nitelikli (sabıka kaydı, biyometrik veriler, sağlık verileri) verileriyle ilgili açık rıza almalı ve açık rızanın çalışan tarafından özgür iradesi ile ve bilgilendirilmiş bir biçimde verilmesi gerekmektedir. Ayrıca açık rızanın amaca uygun, amaçla sınırlı ve ölçülü olması da gerekmektedir. Nitekim personel devam kontrol sistemine giriş çıkışlarda parmak izi, avuç izi, yüz okuma, retina gibi sistemlerle takip yapılması durumunda içinin onayı alınmak zorundadır. Bu sürecin yönetilmesinden de insan kaynakları departmanı sorumludur.

4.2 Bilgi İşlem Departmanlarının Kişisel Verilerin Korunmasındaki Rolü

İşletmelerde bilgiler artık çoğunlukla elektronik ortamlarda tutulmakta ve saklanmaktadır. Özellikle işletmelerde bu konuda yeterli güvenlik tedbirlerinin alınması konusunda bilgi işlem departmanlarına önemli görevler düşmektedir. Bu kapsamda işletmelerin 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 işlem 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 üçüncü 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 sunulmalıdır.

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.

5. İşletmelerde Kişisel Verilerin Korunmasında İnsan Kaynakları ve Bilgi İşlem Departmanlarının Rolüne Yönelik Özel Sektör İşletmeleri Örnek Olay Çalışmaları

5.1 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 insan kaynakları ve bilgi işlem 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 bu iki departmanın kişisel veriler konusunda ortaya koyduğu faaliyetlerin diğer birimlerden daha etkin sonuçlar ortaya çıkardığı düşünülmektedir. Bu amaçla makalede; 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.

5.2 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 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 yöntemi 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 sağlanması 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 ifade etmiştir. 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, 24).

5.3 Örneklem

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

5.4 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 (internet) sitelerinden ve dokümanlarından oluşmaktadır.

Görüşmelerin tamamı görüşülenlerin izni ile kayıt altına alınmıştır.

Örnek olay 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?

5.5 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).

5.6 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, 30-31);

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 çalışması yapılmış olması karşılaştırmalar yapılmasına imkân vermiş olup tekrar eden sonuçlara ulaşılması sayesinde genellemelerin geçerliliğini güçlendirmiştir. Bununla beraber, burada genelleştirme nicel araştırmalarda olduğu gibi örneklemden evrene genelleme şeklinde değil ve fakat örnek olaya 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:Arslan, 2018, 31). Güvenirliliğin sağlanması amacıyla, her bir örnek olay ile alakalı veriler toplanmış, saklanmış ve veri bankasına kaydedilmiştir. Ayrıca görüşme notları, araştırma notları muhafaza edilmiş, görüşmeler ilgili kişinin izni ile kayıt altına alınmıştır.

Örnek olay çalışması birisi tekstil diğeri lojistik olmak üzere iki farklı sektörde yapılmıştır. Çalışmada, insan kaynakları ve bilgi işlem departmanları yöneticileri ile mülakatlar yapılarak kişisel verilerin korunması ile ilgili işyeri uygulamaları ve politikaları değerlendirilmiştir. İki farklı işletmede yapılan araştırmada yüz yüze görüşme, gözlem, dokümanlar, işletmelerin web (internet) sayfaları ve raporlar bilgi kaynağı olarak kullanılmıştır. Örnek olay çalışmamızda, işyerlerinin 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 konularıyla ilgili sorulara cevaplar aranmıştır. İşletmelerin uygulamaları ve politikaları aynı mevzuata dayandığı için büyük benzerlik göstermektedir. Bu nedenle izlenen politikalar ve alınan idari-teknik tedbirler birlikte değerlendirilmiştir.

5.6 ABC Lojistik Kargo Hizmetleri A.Ş ile XYZ İplik San. ve Tic. A.Ş. Hakkında Genel Bilgiler

77 yıldır lojistik sektöründe faaliyet gösteren ABC Lojistik ve Kargo Hizmetleri A.Ş, uluslararası ortaklıkları, istihdamı, yarattığı ekonomi ve sağladığı katma değeriyle lojistik sektörünün liderliğini yapan dev bir işletmedir. Lojistik sektöründe Türkiye'nin ilk milli kuruluşu olan ve bugün, 5 kıtada, 107 ülkede, 600 noktada entegre lojistik çözümler üretebilmektedir. Sektörün yerli sermayeli en köklü kuruluşlarından olan işletme, bilgi birikimi ve tecrübesiyle sektörün ihtiyaç duyduğu nitelikli insan kaynağını yetiştirerek, sektörel gelişime katkı sağlamaktadır. Lojistik sektöründe faaliyet gösteren işletmede yaklaşık 1000 kişi istihdam edilmektedir.

1998 yılından itibaren ülkemizde tekstil sektöründe faaliyet gösteren XYZ İplik San. ve Tic. A.Ş. işletmesi Sentetik Polyester, Viskon, Lycra (Elastan) ve boyasız iplik üretimi ile hammadde alım satımı, iç ve dış ticaret faaliyetlerinde bulunmaktadır. Yaklaşık 200 kişi istihdam edilen ve tekstil sektöründe faaliyet gösteren işletme entegre bir tesistir. XYZ İplik San. ve Tic. A.Ş., Avrupa ve Japonya'dan temin ettiği ekipmanlarla son teknoloji ring iplik eğirme tesisine sahiptir. Fabrikada polyester ve suni ipliklerden eğrilmiş iplik üretimi ile başlanmış ve ayrıca pamuk iplikleri üretmek için çeşitlendirilmiştir.

5.6.1 İşletmelerin Veri İşleme Amacı

İşletmelerin 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 yürütülmesi,
- Etkinlik yönetiminin sağlanması,
- Tedarikçiler ve alt işverenlerle olan ilişiklerin sürdürülebilmesi,
- Personel ihtiyacının karşılanması sürecinin yürütülmesi,
- Risk yönetimi işlemleri ile finansal raporlama ve takibi,
- İç denetim ve hukuk işlerinin takibi,
- Kurumsal yönetim ve iletişim faaliyetlerinin yürütülmesi,
- 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.

5.6.2 İşletmelerin Veri İşleme İlkeleri

6698 sayılı Kanun 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; ABC-Lojistik ve Kargo Hizmetleri A.Ş, ile XYZ İplik San. ve Tic. A.Ş. işletmeleri 6698 sayılı Kanunda belirtilen kişisel verilerin işlenmesine esas ilkelere uygun olarak aşağıda gösterilen şekillerde veri işlemektedir:

- Dürüstlük kurallarına ve hukuka uygun olma,
- Verilerin doğru ve gerektiğinde güncel olması,
- Belirli, açık ve legal amaçlar doğrultusunda işlenme,
- Verinin işlendiği amaçla ilintili, ölçülü ve sınırlı olması,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

5.6.3 İşletmelerin Veri İşleme 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 sahibinin açık onayının varlığı,
- Kanunlarda açıkça öngörülmesi,
- 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,
- Bir sözleşmenin oluşturulması veya ifasıyla direkt ilgili olması şartıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin lüzumlu olması,
- Veri sorumlusu olan işletmenin yasal yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması halinde,
- Bir hakkın korunması veya kullanılması için veri işlemenin zaruri olması halinde,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek şartıyla, veri sorumlusunun legal çıkarları için veri işlenmesinin mecburi olması halinde.

5.6.4 İşletmelerde İşlenen Kişisel Veri Sınıfları

İşletmelerde; kişisel veriler hukuka uygun ve yasal veri işleme amaçları nazarı dikkate alınarak, 6698 sayılı Kanun'un 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" gözetilerek;
çalışanlar, çalışan adayları, stajyerler, alt işveren ve alt işveren çalışanları, ziyaretçiler, müşteriler, tedarikçiler ve tedarikçi çalışanları ile üçüncü kişilerin verileri sınırlı olarak aşağıda belirtilen sınıflandırmaya göre ve veri sahiplerinin bilgilendirilmesi kaydıyla işlenmektedir. İşletmelerde işlenen veriler aşağıdaki şekilde sınıflandırılmıştır.

Kimlik Bilgileri: İşletmeler 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 vb. bilgiler.

İletişim Bilgileri: İşletmeler çalışanların başta olmak üzere ticari ilişki içerisinde olduğu kişilerin adres, telefon, e-mail, ıp adresi ve faks numarası vb. bilgiler.

Lokasyon ve Seyahat Bilgileri: İşletmelerin tüm departmanlarca yürütülen iş organizasyonu kapsamında, 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 gibi.

Aile Bireyleri ve Yakın Bilgileri: İşletmelerin 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: İşletmelere girişte, kamera ve güvenlik noktasında alınan kayıtları içeren ve işyerinde kalış süresi boyunca alınan kayıtlara ilişkin kişisel bilgiler.

Finans Bilgileri: İşletmede çalışanlar, stajyerleri, alt işveren çalışanları ve müşterileri ile kurmuş olduğu hukuki bağlantının şekli baz alınarak oluşturulan, her türlü finansal sonucu gösteren bilgiler (Örneğin, banka hesap no, iban no, kredi kartı bilgisi).

İşitsel ve Görsel Bilgileri: İşletmelerin 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: İşletmeler 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 (Örneğin, bordro, ücret bilgisi).

Hassas Nitelikli Kişisel Verileri: İşletmeler ile çalışma münasebeti içerisinde olan çalışanların, stajyerleri ve alt işveren çalışanlarının 6698 sayılı Kanun m.6''da belirtilen ve işverenin yasal yükümlüğünü yerine getirmek amacıyla (Örneğin, kan grubu, sağlık raporu, sabıka kaydı) işlenen veriler.

Şikâyet ve Talep Yönetimi Bilgileri: İşletmelere yöneltilmiş olan her türlü istek veya şikayetlerin alınması ve değerlendirilmesine dair kişisel veriler.

5.7 ABC ve XYZ İşletmelerinde Kişisel Verilerin Korunması Kapsamında Bilgi İşlem ve İnsan Kaynakları Departmanları Tarafından Alınan İdari ve Teknik Tedbirler

ABC ve XYZ işletmeleri, 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 almışlardır. Nitekim 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 idari ve teknik tedbirler konusunda mevzuat çerçevesinde hareket ettikleri görülmüştür. Bu kapsamda alınan teknik tedbirler;

- Her iki işletmede işletmelerin kişisel veri işleme faaliyetleri her ikisinde de insan kaynakları departmanları tarafından yürütülmektedir,
- ABC-Lojistik ve Kargo Hizmetleri A.Ş.'de 27001 Bilgi Güvenlik Yönetim Sistemi bulunmasına rağmen XYZ-İplik San. ve Tic. A.Ş.'de bu sistem bulunmamaktadır,
- İşlenen kişisel verilerle ilgili olarak veri işleyen kişilerin eğitildikleri ve farkındalıklarının artırıldığı ve sertifikalandırıldığı görülmüştür,
- Alınan teknik önlemler periyodik olarak işletme üst yönetimine raporlanmaktadır,
- Bilgi işlem departmanlarında konusunda uzman personel çalıştırılmaktadır,
- 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 yetkisi 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,
- 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,

- Teknolojik gelişmelere uygun sistemler kullanılmak suretiyle kişisel verilerin güvenli ortamlarda saklanması sağlanmaktadır,
- 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,
- 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 atak önleme hizmeti, 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.

İşletmeler, 6698 sayılı Kanun'un 12'nci maddesine uygun olarak işlenen kişisel verilerin başkaları tarafından legal (yasal) 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. İşletmelerin İdari İşler Departmanları, 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.

ABC ve XYZ işletmelerinin İnsan Kaynakları Departmanları tarafından alınan idari tedbirler:

- İnsan kaynakları departmanına girişler özel kartlı sistemle yapılmamakla birlikte özlük dosyalarının bulunduğu dolaplar kilit altına alınmaktadır,
- İş başvuru formları her iki işletmede de insan kaynakları departmanında 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,
- İşletmelerin 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,
- İşletmelerin 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,
- İşletmelerin 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 işletmeler 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,
- Departman bazında kişisel veri işlenmesinin hukuka uyumu açısından işletmelerin bünyesinde 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,
- İşletmeler, 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 koymaktadır,
- İşletmeler, 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; işyeri çalışanları, kişisel verilerin güvenle nasıl saklanması gerektiği hususunda periyodik olarak eğitilmektedirler,
- İşletmeler tarafından kişisel verilerin saklanması konusunda hukuki gereklilikler nedeniyle dışarıdan bir hizmet temin edilmesi halinde, kişisel verilerin hukuka uygun olarak aktarıldığı diğer işletmeler ile imzalanan gizlilik sözleşmelerine, kişisel verilerin aktarıldığı kişilerin, verilerinin korunması için gerekli tedbirleri alacağına ve kendi işletmelerinin de bu önlemlere uyulmasını sağlanacağına ilişkin düzenlemelere yer verilmektedir,
- İşletmeler, 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 işletmelerin web sitesindeki başvuru formunu indirmek suretiyle işletmelere iletmeleri halinde, işletmeler yöneltilen talebin niteliğine göre, en geç otuz gün içinde ücretsiz olarak sonuçlandırmaktadır,
- 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.

İşletmeler 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. Ancak sağlık birimine giriş çıkışlar özel kartlı sistemle yapılmamaktadır. Bununla birlikte 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.

İşletmeler 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.

İşletmelerin kamera izleme politikası kapsamında kamera ile izleme sisteminin nasıl kurgulandığı ve verilerin gizliliği ile kişilerin temel haklarının nasıl korunacağına dair bilgilendirme yapılmaktadır.

İşletmelerin güvenlik kamerası ile izleme faaliyeti kapsamında; işletme çalışanlarının ve diğer kişilerin sağlık ve güvenliğini sağlamaya yönelik yasal çıkarlarını korumayı amaçlamaktadır. Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata uygun bir biçimde işletme tarafından elektronik gözetleme faaliyeti sürdürülmektedir.

İşletmeler 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.

6. Örnek Olaylar İle İlgili Ortak Sonuç ve Analiz

Kişisel Verileri Koruma Kurulu VERBİS (Veri sorumlusu sicil bilgi sistemi) sistemine kayıt yaptırması gereken veri sorumlularında iki kriterden birini aramaktadır. Bunlardan ilki çalışan sayısının 50'nin üzerinde olması, ikincisi de yıllık mali bilanço toplamının 25 milyon TL'den fazla olmasıdır. Bu kapsamdaki işyerleri VERBİS üzerinden sicile kayıt yaptırmak zorundadırlar. Bu yükümlülüğe aykırı davranan işletmeler hakkında 20 bin TL ila 1 milyon TL arasında idari para cezası uygulanabilecektir. Veri Siciline kayıt yükümlüsü olan veri sorumlusu sıfatına haiz işletmeler ile yurtdışında yerleşik veri sorumlusu işletmeler 01.10.2018 tarihinden 30.09.2019 tarihine kadar sicile kayıt yaptırmak zorundadırlar.

Örnek olay çalışmamıza konu her iki işletmenin çalışan sayısının 50'nin üzerinde olması nedeniyle, işletmeler tarafından VERBİS üzerinden sicile kayıt yükümlülükleri yerine getirilmiştir. VERBİS'e kayıt esnasında işyerlerinin veri envanteri baz alınarak saklama süreleri, veri işleme amaçları, yasal dayanakları, verilerin nerelere aktarıldığı ve veri sorumlusu tarafından alınan idari ve teknik tedbirler 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 işletmenin de VERBİS sistemine süresi içinde kayıt yaptırdıkları tespit edilmiştir. Bu işletmelerden XYZ-İplik San. ve Tic. A.Ş.'de henüz 27001 Bilgi Güvenliği Yönetim Sistemini kurulmamıştır. işletmeler farklı sektörlerde (lojistik ve tekstil) faaliyet gösterse dahi kişisel verilerin korunması ile ilgili almaları gereken idari ve teknik tedbirlerin yasal dayanağının aynı olması nedeniyle benzerlik göstermektedir. Çünkü işletmeler kendi çalışanları başta olmak üzere çalışan adaylarının, stajyerlerinin, alt işveren çalışanlarının tedarikçilerinin, müşterilerinin ve ziyaretçilerinin kişisel verilerini işlemektedir. Elbette ki işletmelerin fiziki ve yönetim yapılarının ve yaklaşımlarının farklılık arz ettiği dikkate alındığında birtakım farklılıkların bulunduğunu da söylememiz mümkündür.

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,
- Tedarikçiler ve alt işverenlerle olan ilişkilerin yönetiminin sağlanması,
- Personel temin süreçlerinin yürütülmesi,
- Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi,
- İç denetim ve Hukuk işlerinin icrası,
- Kurumsal yönetim ve iletişim faaliyetlerinin planlanması ve yürütülmesi,
- 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. Benzer şekilde iş başvuru formlarındaki fazlaya dair kişisel verilerin azaltılmasına yönelik olarak yapılan revizyonlar konusunda da benzerlik bulunduğu tespit edilmiştir. Örnek olay çalışması yapılan her iki işyerinde 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 soruların sorulmadığı 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 çalışması 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 üç 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 sürecini 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 levhalarının asıldıkları tespitlerimiz arasındadır.

Örnek olay çalışması yapılan işletmelerin işledikleri veriler sınıflandırıldığında yine benzerlik gösterdiği görülmektedir. Nihayetinde veri sorumlusu olan işletmelerin her ikisinde de "Kişisel Verilerin Korunması ve İşlenmesi Politikasını" oluşturdukları ve bu kapsamda çalışanlar, çalışan adayları, stajyerler, alt işverenler ve alt işveren çalışanları, ziyaretçiler, müşteriler, tedarikçiler ve tedarikçi çalışanları ile üçüncü kişilerle tahditli olmak üzere, kimlik, iletişim, lokasyon, yakınlık, sağlık, biyometrik, 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 insan kaynakları ve bilgi işlem departmanları tarafından denetlenmektedir. Örnek olay çalışması yapılan her iki işletmenin bilgi işlem 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 periyotlarla 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 girişler serbest olup elektronik kart uygulaması yapılmamaktadır. Sadece server odalarına girişler elektronik kart ile yapılmakta olup, revir, idari işler ve arşivlere girişler için özel önlemler alınmamıştır.

7. Sonuç ve Öneriler

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. 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 yanı sıra 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 elliden 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 lojistik sektöründe faaliyet gösteren iki işletmenin elliden 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 departmanları 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 işlem 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 işletmeler dikkate alındığında işletmelere yapılacak önerilerimizin başında 27001 Bilgi Güvenliği Yönetim Sisteminin işyerlerinde oluşturulmasıdır. Aynı zamanda fiziki mekân güvenliğinin sağlanması içinde 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 işletmeler 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 sınırlı olmalıdır. Örneğin güvenlik personeli, insan kaynakları, bilgi işlem ve yönetici konumundaki kişiler dışında adli sicil belgeleri sadece görülmeli, arşivlenmemelidir.

İşletmelere, işyerine girişte alınan kimliklerin bilgileri alındıktan sonra ziyaretçilere geri iade edilmeli, güvenlik noktasında alıkonulmaması önerilmektedir. 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 geliştirmektedirler. 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.

KAYNAKÇA

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

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

Civelek, Dilek Y. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*. Yayınlanmamış Uzmanlık Tezi, Ankara: Devlet Planlama Teşkilatı.

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

Eisenhardt, Kathleen M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, 14(4), s.24-29.

Eisenhardt, Kathleen M. ve Graebner, Melissa E. (2007). Theory Building From Cases: Opportunities and Challenges. *Academy of Management Journal*, 50(1), s.24.

Ertürk, Şükran. (2002). İş İlişkisinde Temel Haklar. Ankara: Seçkin Yayınları.
İnciroğlu, Lütfi. (2018). İşçinin Kişisel Verilerinin Korunması Hakkı Kapsamında İşveren Yükümlülükleri. *Toprak İşveren Dergisi,* S.119.
Jay, Rosemary. (2007). *Data Protection Law and Practice*. Fourth Edition, London: Sweet & Maxwell.
Kaplan, Yavuz. (2004). *İnternet Ortamında Fikri Hakların Korunmasında Uygulanacak Hukuk*. Ankara: Seçkin Yayınları.
Kılınç, Doğan. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61(3), s.1112.
Kuşkonmaz, Elif.M. (2018). *Kişisel verilerin Türk Ceza Kanunu kapsamında korunması*. Yüksek Lisans Tezi, İstanbul.
Küzeci, Elif. (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: 25.06.2019.
KVKK (2017). *Kişisel Verileri Koruma Kurumu*. https://www.kvkk.gov.tr/Icerik/4113/2017-61, Erişim Tarihi 25.06.2019
Lloyd, Ian.J. (2011). Information technology law. Oxford University Press, s.169-187.
Manav, A. Eda. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 19(2).
Okur, Zeki. (2011). *İş Hukukunda Elektronik Gözetleme*. İstanbul: Legal Yayınları.
Özdemir, H. (2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara: Seçkin Yayınları, s.55-69.
Savaş, Burcu. (2009). İş Hukukunda Siber Gözetim. *Çalışma ve Toplum Dergisi,* 2009/3.
Sevimli, Ahmet. (2008). İşçinin Özel Yaşam Hakkı Bağlamında İşçi–İşveren İlişkisi. *Sicil İş Hukuku Dergisi,* Yıl, 2008/3. s.53-71.
Şahin, Osman. (2011). *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Saklanması ve Gizliliğin Korunması*. Bilişim Uzmanlığı Tezi, Ankara: Bilgi Teknolojileri ve İletişim Kurumu.
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, Selen. (2014). *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. Ankara: Seçkin Yayıncılık.
Yıldırım, Ali ve Şimşek, Hasan. (2008). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*. (6. Baskı), Ankara: Seçkin Yayıncılık.
Yin, K.Robert. (2009). *Case Study Research: Design and Methods*. SAGE Publications.