BOSS YÖNETİŞİM HİZMETLERİ A.Ş. KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

23 Ocak 2017

1. GİRİŞ 5

1.1. GİRİŞ 5
1.2. POLİTİKANIN AMACI VE TANIMLAR 6
1.3. KAPSAM 7
1.4. POLİTİKANIN VE İLGİLİ MEVZUATIN UYGULANMASI 7
1.5. POLİTİKANIN YÜRÜRLÜĞÜ 8

2. KİŞİSEL VERİLERİN SAKLANMASINA İLİŞKİN HUSUSLAR 8

2.1. KİŞİSEL VERİLERİN GÜVENLİĞİNİN SAĞLANMASI 8
2.1.1. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan Teknik ve İdari Tedbirler 8
a) Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan Teknik Tedbirler 8
b) Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan İdari Tedbirler 9
2.1.2. Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik ve İdari Tedbirler 10
a) Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik Tedbirler 10
b) Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan İdari Tedbirler 11
2.1.3. Kişisel Verilerin Güvenli Ortamlarda Saklanması 12
a) Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan Teknik Tedbirler 13
b) Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan İdari Tedbirler 14
2.1.4 Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi 15
2.2. VERİ SAHİBİNİN HAKLARININ GÖZETİLMESİ; BU HAKLARI ŞİRKETİMİZE İLETECEĞİ KANALLARIN YARATILMASI VE VERİ SAHİPLERİNİN TALEPLERİNİN DEĞERLENDİRMESİ 15
2.3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI 16
2.4. İŞ BİRİMLERİNİN KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ KONUSUNDA FARKINDALIKLARININ ARTTIRILMASI VE DENETİMİ 17
2.5. İŞ ORTAKLARI VE TEDARİKÇİLERİN KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ KONUSUNDAKİ FARKINDALIKLARININ ARTTIRILMASI VE DENETİMİ 17

3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR 17

3.1. KİŞİSEL VERİLERİN MEVZUATTA ÖNGÖRÜLEN İLKELERE UYGUN OLARAK İŞLENMESİ 18
3.1.1. Hukuka ve Dürüstlük Kuralına Uygun İşleme 18
3.1.2. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama 18
3.2. KİŞİSEL VERİLERİN, KANUN'UN 5. MADDESİNDE BELİRTİLEN KİŞİSEL VERİ İŞLEME ŞARTLARINDAN BİR VEYA BİRKAÇINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLEME 19
3.3. KİŞİSEL VERİ SAHİBİNİN AYDINLATILMASI VE BİLGİLENDİRİLMESİ 19
3.4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ 19
3.5. KİŞİSEL VERİLERİN AKTARILMASI 20
3.5.1. Kişisel Verilerin Aktarılması 20
3.5.2. Özel Nitelikli Kişisel Verilerin Aktarılması 21

4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SÜRELERİ 21

4.1. KİŞİSEL VERİLERİN KATEGORİZASYONU 21
4.2. KİŞİSEL VERİNİN İŞLENME AMAÇLARI 24
4.3. KİŞİSEL VERİLERİN SAKLANMA SÜRELERİ 26

5. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN SAHİPLERİNE İLİŞKİN KATEGORİZASYON 26

5.1. KİŞİSEL VERİ KATEGORİZASYONU 26

6. ŞİRKETİMİZ TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI 28

6.1. AKTARIM ARAÇLARI 28

7. KİŞİSEL VERİLERİN KANUNDAKİ İŞLEME ŞARTLARINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLENMESİ 28

7.1. KİŞİSEL VERİLERİN VE ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ 28

7.1.1. Kişisel Verilerin İşlenmesi 28

(i) Kişisel Veri Sahibinin Açık Rızasının Bulunması 28

(ii) Kanunlarda Açıkça Öngörülmesi 29

(iii) Fiili İmkânsızlık Sebebiyle İlgilinin Açık Rızasının Alınamaması 29

(iv) Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması 29

(v) Şirketin Hukuki Yükümlülüğünü Yerine Getirmesi 29

(vi) Kişisel Veri Sahibinin Kişisel Verisini Alenileştirmesi 29

(vii) Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması 29

(viii) Şirketimizin Meşru Menfaati için Veri İşlemenin Zorunlu Olması 29

7.1.2. Özel Nitelikli Kişisel Verilerin İşlenmesi 29

8. BİNA İÇERİSİNDE YAPILAN KİŞİSEL VERİ İŞLEME FAALİYETLERİ 30

8.1. iZLEME FAALİYETLERİ 30

8.1.1. Kamera ile İzleme Faaliyetinin Yasal Dayanağı 30

8.1.2. KVK Hukukuna Göre Güvenlik Kamerası ile İzleme Faaliyeti Yürütülmesi 30

8.1.3. Kamera ile İzleme Faaliyetinin Duyurulması 31

8.1.4. Kamera ile İzleme Faaliyetinin Yürütülme Amacı ve Amaçla Sınırlılık 31

8.1.5. Elde Edilen Verilerin Güvenliğinin Sağlanması 31

8.1.6. Kamera ile İzleme Faaliyeti ile Elde Edilen Kişisel Verilerin Muhafaza Süresi 31

8.1.7. İzleme Sonucunda Elde Edilen Bilgilere Kimlerin Erişebildiği ve Bu Bilgilerin Kimlere Aktarıldığı 31

8.2. BİNA İÇERİSİNDE YÜRÜTÜLEN MİSAFİR GİRİŞ ÇIKIŞLARININ TAKİBİ 31

8.3. BİNA ZİYARETÇİLERİMİZE SAĞLANAN İNTERNET ERİŞİMLERİNE İLİŞKİN KAYITLARIN SAKLANMASI 32

8.4. YANGIN 32

8.5. SICAKLIK 33

8.6. DEPREM VE PATLAMA 33

9. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI 34

9.1. KİŞİSEL VERİLERİ SİLME, YOK ETME VE ANONİMLEŞTİRME YÜKÜMLÜLÜĞÜ 34

9.2. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ TEKNİKLERİ 34

9.2.1. Kişisel Verilerin Silinmesi 35

(i) Fiziksel Olarak Silme 35

(ii) Yazılımdan Güvenli Olarak Silme (Secure Deletion Softare) 36

(iii) Uzman Tarafından Güvenli Olarak Silme (Sending to a Specialist for Secure Deletion) 36

9.2.2. Kişisel Verilerin Yok Edilmesi 36

9.2.3. Kişisel Verileri Anonim Hale Getirme Teknikleri 37

9.2.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri 38

9.2.3.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri 42

9.3. ANONİM HALE GETİRMEYİ KUVVETLENDİRİCİ İSTATİSTİK YÖNTEMLER 44

9.4. KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİNE VE GÖREV TANIMLARI 48

9.5. KİŞİSEL VERİLERİN PERİYODİK İMHA SÜRELERİ 49

9.6. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI; BU HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ METODOLOJİSİ 49

10. VERİ SAHİBİNİN HAKLARI VE BU HAKLARINI KULLANMASI 49

10.1. KİŞİSEL VERİ SAHİBİNİN HAKLARI 49
10.2. KİŞİSEL VERİ SAHİBİNİN HAKLARINI İLERİ SÜREMEYECEĞİ HALLER 49
10.3. KİŞİSEL VERİ SAHİBİNİN HAKLARINI KULLANMASI 50
10.4. KİŞİSEL VERİ SAHİBİNİN KVK KURULU'NA ŞİKÂYETTE BULUNMA HAKKI 50
10.5. ŞİRKET'İN BAŞVURULARA CEVAP VERMESİ 51
10.5.1. Şirketimizin Başvurulara Cevap Verme Usulü ve Süresi 51
10.5.2. Şirketimizin Başvuruda Bulunan Kişisel Veri Sahibinden Talep Edebileceği Bilgiler 51
10.5.3. Şirketimizin, Kişisel Veri Sahibinin Başvurusunu Reddetme Hakkı 51
10.6. ŞİRKET KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASININ DİĞER POLİTİKALARLA OLAN İLİŞKİSİ VE YASAL UYUMLULUK 52
EK - 1 54
EK - 2 56
EK - 3 57

1. GİRİŞ

1.1. GİRİŞ

Kişisel verilerin saklanması ve imha edilmesi, Şirketimizin en önemli öncelikleri arasındadır. Bu konunun en önemli ayağını ise işbu Politika ile yönetilen; müşterilerimizin, potansiyel müşterilerimizin, çalışanlarımızın, çalışan adaylarımızın, ziyaretçilerimizin, iş birliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkililerinin ve üçüncü kişilerin kişisel verilerinin korunması, saklanması ve imha edilmesi oluşturmaktadır. Çalışanlarımızın kişisel verilerinin saklanmasına ve imha edilmesine ilişkin Şirketimizin yürüttüğü faaliyetler ise bu Politika'daki esaslarla yönetilmektedir.

Türkiye Cumhuriyeti Anayasası'na göre, herkes, kendisiyle ilgili kişisel verilerin korunmasını ve imha edilmesini isteme hakkına sahiptir. Bir Anayasal hak olan kişisel verilerin korunması ve imha edilmesi konusunda, Şirket, işbu Politika ile yönetilen; kişisel verilerinin korunmasına ve imha edilmesine dair gerekli özeni göstermekte ve bunu bir Şirket politikası haline getirmektedir.

Bu kapsamda, ilgili mevzuat gereğince işlenen kişisel verilerin korunması için Şirket tarafından gereken idari ve teknik tedbirler alınmaktadır. Bu Politika'da kişisel verilerin işlenmesinde Şirketimizin benimsediği ve aşağıda sıralanan temel ilkelere ilişkin detaylı açıklamalarda bulunulacaktır:

- Kişisel verileri hukuka ve dürüstlük kurallarına uygun olma,
- Kişisel verileri doğru ve gerektiğinde güncel tutma,
- Kişisel verileri belirli, açık ve meşru amaçlar için işleme,
- Kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü işleme,
- Kişisel verileri ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme ve gerekli koşullar oluştuğunda imha etme,
- Kişisel veri sahiplerini aydınlatma ve bilgilendirme,

a Kişisel veri sahiplerinin haklarını kullanması için gerekli sistemi kurma,

b Kişisel verilerin muhafazasında gerekli tedbirleri alma,

c Kişisel verilerin işleme amacının gereklilikleri doğrultusunda üçüncü kişilere aktarılmasında, ilgili mevzuata ve KVK Kurulu düzenlemelerine uygun davranma,

d Özel nitelikli kişisel verilerin işlenmesine ve korunmasına gerekli hassasiyeti gösterme.

1.2. POLİTİKANIN AMACI VE TANIMLAR

Bu Politika'nın temel amacı, Şirket tarafından hukuka uygun bir biçimde yürütülen kişisel veri işleme faaliyeti ve kişisel verilerin korunmasına yönelik benimsenen sistemler konusunda açıklamalarda bulunmak, bu kapsamda kişisel verileri şirketimiz tarafından işlenen kişileri bilgilendirilerek şeffaflığı sağlamaktır.

Tanım	Açıklama
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	Kişisel verinin, kişisel veri niteliğini kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
Çalışan	Boss Yönetişim Hizmetleri ve CottGroup üye ağı şirketleri personeli.
Çalışan Adayı	Şirketimize herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini şirketimizin incelemesine açmış olan gerçek kişiler
İşbirliği İçerisinde Olduğumuz Kurumların Çalışanları, Hissedarları ve Yetkilileri	Şirketimizin her türlü iş ilişkisi içerisinde bulunduğu kurumlarda (iş ortağı, tedarikçi gibi, ancak bunlarla sınırlı olmaksınız) çalışan, bu kurumların hissedarları ve yetkilileri dahil olmak üzere, gerçek kişiler
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Kişisel Veri Sahibi	Kişisel verisi işlenen gerçek kişi. Örneğin; Müşteriler ve çalışanlar.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örneğin; ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası vb.
Müşteri	Şirketimizle herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirketimizin sunmuş olduğu hizmetleri kullanan veya kullanmış olan gerçek kişiler
Özel Nitelikli Kişisel Veri	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
Potansiyel Müşteri	Hizmetlerimizi kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişiler
Şirket Hissedarı	Şirketimizin hissedarı gerçek kişiler
Şirket Yetkilisi	Şirketimizin yönetim kurulu üyesi ve diğer yetkili gerçek kişiler

Üçüncü Kişi	Şirketimizin yukarıda bahsi geçen taraflarla arasındaki ticari işlem güvenliğini sağlamak veya bahsi geçen kişilerin haklarını korumak ve menfaat temin etmek üzere bu kişilerle ilişkili olan üçüncü taraf gerçek kişiler (Örn. Kefil, Refakatçi, Aile Bireyleri ve yakınlar)
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir. Örneğin, Şirketimizin verilerini tutan bulut bilişim firması, müşterilere formları imzalattığı anketörleri, scriptler çerçevesinde arama yapan call-center firması *vb.*
Veri Sorumlusu	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten kişi veri sorumlusudur.
Ziyaretçi	Şirketimizin sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler

1.3. KAPSAM

Bu Politika; otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verilere ilişkindir. Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.4. POLİTİKANIN VE İLGİLİ MEVZUATIN UYGULANMASI

Kişisel verilerin işlenmesi, saklanması ve imha edilmesi konularında yürürlükte bulunan ilgili yasal düzenlemeler öncelikle uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Şirketimiz yürürlükteki mevzuatın uygulama alanı bulacağını kabul etmektedir.

Şirketimiz Sosyal Güvenlik Kurumu, İşkur, Bölge Çalışma Kurumu, Göç İdaresi, Gelir İdaresi Başkanlığı ve ilgili diğer kurumların düzenlemeleri gerekse hizmet sözleşmelerimiz nedeniyle sözlü, yazılı ya da elektronik kişisel verileri, toplanmakta ve işlenmektedir.

Şirketimiz, söz konusu kişisel verileri sadece; müşterilerimizin açık rızasına istinaden veya tabi olduğumuz mevzuat başta olmak üzere KVKK md. 5/f 'de öngörülen diğer hallerde, müşterilerimize katma değerli hizmetler, fırsat ve olanaklar sunulması ve hizmet kalitesinin artırılması amacıyla; Şirketimizin bağlı olduğu CottGroup Şirketleri "CottGroup olarak anılacaktır" (Grup şirketleri listesini işbu sözleşmede Ek-3'te görebilirsiniz) ile ileride CottGroup Şirketlerine dahil olacak yurt içinde ya da yurt dışındaki iştiraklerimizle ve doğrudan veya dolaylı bağlı şirketlerimizle ve ortak girişimlerimizle veya yasal bir zorunluluk gereği bu verileri talep etmeye yetkili olan kamu kurum veya kuruluşları ile ve yeterli önlemler alınmak kaydıyla, faaliyetlerimiz gereği anlaşmalı olduğumuz yurt içinde ya da yurt dışındaki kurumlar, tedarikçiler, yetkili satıcılar/bayiiler/iş ortaklarımız ile paylaşabilecektir. Şirketimizin ortakları, grup bünyesindeki şirketler ve iştirakleri için *http://www.cottgroup.com* internet adresinden bilgi edinebilirsiniz.

CottGroup şirketleri arasında Boss Yönetişim Hizmetleri A.Ş. gerekli tüm sertifikasyonlara sahip olarak grup şirketlerine ait kayıtları kendi veri ~~merkezinda~~merkezinde barındırmakta, saklamakta ve imha süreçlerini takip etmektedir.

Politika, ilgili mevzuat tarafından ortaya konulan kuralların Şirket uygulamaları kapsamında somutlaştırılarak düzenlenmesinden oluşturulmuştur. Şirketimiz, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("Kanun") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te ("Yönetmelik") öngörülen sürelere uygun hareket etmek üzere gerekli sistem ve hazırlıklarını yürütmektedir.

1.5. POLİTİKANIN YÜRÜRLÜĞÜ

Şirketimiz tarafından düzenlenen bu Politika 23 Ocak 2017~~8~~ tarihlidir. Politika'nın tamamının veya belirli maddelerinin yenilenmesi durumunda Politika'nın yürürlük tarihi güncellenecektir.

Politika Şirketimizin internet sitesinde yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

2. KİŞİSEL VERİLERİN SAKLANMASINA İLİŞKİN HUSUSLAR

Şirketimiz, Kanun'un 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli denetimleri yapmak veya yaptırmaktadır. Ayrıca tüm süreçler CottGroup veri merkezini yöneten Boss Yönetişim Hizmetleri A.Ş. 'ne ait ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında yürütülmektedir.

2.1. KİŞİSEL VERİLERİN GÜVENLİĞİNİN SAĞLANMASI

2.1.1. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan Teknik ve İdari Tedbirler

Şirketimiz, kişisel verilerin hukuka uygun işlenmesini sağlamak için, teknolojik imkânlar ve uygulama maliyetine göre teknik ve idari tedbirler almaktadır.

a) Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan Teknik Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka uygun işlenmesini sağlamak için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Şirketimiz bünyesinde gerçekleştirilen kişisel veri işleme faaliyetleri kurulan teknik sistemlerle denetlenmektedir.

- Alınan teknik önlemler iç denetim mekanizması gereği ilgilisine raporlanmaktadır.

- Teknik konularda bilgili personel istihdam edilmektedir.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri kullanılmakta ve bunların kayıtları muhafaza edilmektedir. Şirketimiz tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamakta ve personelini bilgi güvenliği ve tehditler hakkında düzenlemeler yapmaktadır. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi yönetimin aktif desteği ve personelin katılımcılığıyla ile en önemli varlıklarımız arasındadır.

b) Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak için Alınan İdari Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka uygun işlenmesini sağlamak için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar, kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmekte ve eğitilmektedir.

- Çalışanların şirketimizin ve ilişkili tarafların hangi bilgi varlıklara sahip olduğunu ve değerlerinin farkında olması sağlanır.

- Şirketimizin iş birimlerinin yürütmüş olduğu kişisel veri işleme faaliyetleri; bu faaliyetlerin Kanun'un aradığı kişisel veri işleme şartlarına uygunluğun sağlanması için yerine getirilecek olan gereklilikler her bir iş birimi ve yürütmüş olduğu detay faaliyet özelinde belirlenmektedir.

- İş birimlerimiz bazlı belirlenen hukuksal uyum gerekliliklerinin sağlanması için ilgili iş birimleri özelinde farkındalık yaratılmakta ve uygulama kuralları belirlenmekte; bu hususların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler politikalar ve eğitimler yoluyla hayata geçirilmektedir.

- Verilerin işlenmesi ile ilgili gerekli yazılım / donanım / sürüm / güncelleme değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesi için gereken tedbirler yönetim tarafından alınmaktadır.

- Bölüm Yöneticileri, Güvenlik Politika ve Prosedürleri, Risk Yönetimi konularında bölümlerini bilinçlendirmektedir.

- Teknoloji değişikliklerinin kurumun sistemlerine etkileri ayda bir kez Bilgi işlem müdürü tarafından gözden geçirilmektedir.

- Şirket Yönetimi, çalışanların hızla değişen bilişim güvenliği ve güvenlik tehlikeleri konusunda bilgilendirilmesini sağlayacak koşulları oluşturmaktadır.

2.1.2. Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik ve İdari Tedbirler

Şirketimiz, kişisel verilerin tedbirsizlikle veya yetkisiz olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerdeki tüm hukuka aykırı erişimi önlemek için korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre teknik ve idari tedbirler almaktadır.

a) Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Şirket yönetimi tarafından, sunulan hizmetlerin veri güvenliğini ve sürdürülebilirliğini en üst düzeyde tutmak ve olası bilgi kayıplarını en aza indirgemek için çalışan personelin fiziksel ve sistem erişim yetkileri ile ilgili sistemler sürekli denetlenmektedir.

- Teknolojideki gelişmelere uygun teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmekte ve yenilenmektedir.

- İş birim bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak erişim ve yetkilendirme teknik çözümleri devreye alınmaktadır.

- Alınan teknik önlemler iç denetim mekanizması gereği ilgilisine raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmektedir.

- Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.

- Şirket'e ait tüm giriş çıkışlar kayıt altına alınır. Kayıtlar İnsan Kaynakları Uzman Yardımcısı tarafından günlük olarak takip edilir. Kayıtlar ortak alanda sıralı, süzülebilir bir liste haline getirilir.

- Şirket içinde üretilen, muhafaza edilen ve iletilen bilginin uygun şekilde koruma altına alınması ve kontrol edilmesini sağlamak için gereken tedbirler alınmaktadır.

- Bilgisayarların kaybolması, çalınması durumunda, önemli verilerin istenmeyen kişiler tarafından okunmaması için tüm personellerin sabit diskleri Bitlocker ile şifrelenmektedir.

- Tüm personel, kendilerine tahsis edilen yetki çerçevesinde bilgilere erişerek ve kullanacaktır.

- Her bilgi için Veri Sahibi tanımlanmaktadır ve Veri Sahibinin izni olmadan; Bilgi İşlem Uzmanı, sahibi olmadığı elektronik ortamdaki veri üzerinde herhangi bir aksiyon ve işlem gerçekleştiremez.

- Her bölüm kendi odasında bulunan evraklardan sorumludur. Erişim yetki tablosunda belirtildiği şekilde bölümündeki evraklara erişebilir ve bölüm müdürünün onayı ile ilgili evrak, bölüm dışına çıkartılabilir. Erişim Yetki tablosunda, departmanların evrak erişimi ile ilgili tanımlamalar yapılmıştır.

- Güvenlik bilinçlendirme ve eğitimleri sürekli olacaktır.

- Ziyaretçi kabul ve taşınabilir ortam politikaları gibi ek düzenlemeler ile erişim kontrolü üst seviyeye çıkarılmıştır.

- Teknik konularda bilgili personel istihdam edilmektedir.

b) Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan İdari Tedbirler

Şirketimiz tarafından kişisel verilerin hukuka aykırı erişimini engellemek için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Çalışanlar, kişisel verilere hukuka aykırı erişimi engellemek için alınacak teknik tedbirler konusunda eğitilmektedir.

- İş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak Şirket içinde kişisel verilere erişim ve yetkilendirme süreçleri tasarlanmakta ve uygulanmaktadır.

- Çalışanlar, öğrendikleri kişisel verileri mevzuata aykırı olarak başkasına açıklayamayacağı, işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmaktadır.

- Bilgi varlıkları ve her türlü kişisel veri sınıflandırılmıştır.

- Tüm bilgiler, aksi onaylanmadığı veya etiketlenmediği sürece gizli bilgi olarak nitelendirilir.

- Bilginin çeşitli seviyelerde gizlilik içermesi durumunda, saklanan alan en yüksek gizlilik seviyesi içeren bilgilere göre etiketlenir.

- Bilginin gizliliği hangi seviyede olursa olsun, yöneticilerin bu bilgiye ulaşımı mutlaka olmalıdır.

- Ticari sırların neler olduğunu belirleyecek olan kişi Genel Müdürdür.

- Evraklar, dokümanlar için bir elden çıkartma tarihi belirlenmeli ve bu tarih Kayıtların Kontrolü Prosedürüne göre yönetilmelidir.

- Bilgiye atanan gizlilik seviye sınıflandırması senede en az bir defa gözden geçirilmelidir.

- Kullanılan çeşitli dosya tiplerinin birbirlerinden ayırt edilebilmesi için dosya isimlendirme hakkında bir sistem oluşturulmalıdır.

- Veri sınıflandırma etiketleri, şirketin etiketleme sistemi ile uyumlu olmalıdır. Bu konuda Dokümanların Kontrolü Prosedürü uygulanır.

- Kullanıcılar, sunucularda belirlenmiş olan klasörlere kendi bilgisayarlarının yedeklerini yüklemelidir.

- Sistemlere log-in olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

- Kullanıcı haklarını izleyebilmek üzere her kullanıcıya kendisine gizlilik içeren bilgilerin iletişimi hakkındaki her türlü bilgi, kontrollü ortamlarda, gizlilik sözleşmesi yapılmış kargo firmaları ile veya iadeli taahhütlü posta gönderimleri ile yollanmalıdır.

- Şirket ağına bağlı olan her varlık, BOSS dışındaki kişiler için herhangi bir anlam taşımayacak biçimde isimlendirilmelidir.

- Şirketin tüm bilgileri aşağıdaki beş sınıflandırma kategorisine ayrılmalıdır: "Çok gizli", "Gizli", "Genel Bilgi", "Halka açık" ve "Önemsiz bilgi".

- Şirketin tüm bilgileri yetki grupları bazında alt etiketlere ayrılır. Alt etiketler ile DLP çalışmaktadır. Ayrıca alt etiketlere yerel yasalarda belirlenen saklama süreleri politikaları bağlanmıştır.

- "Gizli" ve "Çok gizli" olması gereken bir dokümanın kullanıcı tarafından etiketlenmemesi durumunda; DLP bununla ilgili otomatik etiketleme gerçekleştirir. (Örneğin; İçerisinde bir Türk veya Avrupalı ID bilgisi, IBAN No, kredi kartı bilgisi bulunan dokümanlar.)

- Dış kaynaklardan elde edilen tüm bilgiler, bilgisayar depolama ortamı dahil, uygun biçimde tüm kurumda kullanılan sınıflandırma sistemi göz önünde bulundurularak etiketlenmelidir.

- Bir bilginin gizli olduğuna karar verilirse, bilginin gizlilik seviyesine göre görünebilir bir yerine uygun etiketler konulmalıdır.

- Gizli bilgiler içeren bir dokümanın içeriğini değiştiren kişi, uygun sınıflandırma etiketlemesini kullanmalıdır.

- Gizli bilgiler, sadece yetkili bilgi sahibi tarafından kopyalanmalıdır.

- Kopyalama işlemini yürüten kullanıcı, fotokopide bırakmış olduğu dokümanlardan sorumludur.

- Kişiler tarafından yazılmış herhangi bir resmi dokümanın silinmez mürekkeple yazılması ve uygun şekilde işaretlenmesi gerekir. Yapılacak herhangi bir değişikliğin altı çizilmeli, tarihlenmeli ve yeniden onaylanmalıdır.

- Gizli dokümanların tüm sayfalarına "GİZLİDİR" ifadesi basılmaktadır.

2.1.3. Kişisel Verilerin Güvenli Ortamlarda Saklanması

Şirketimiz, kişisel verilerin güvenli ortamlarda saklanması ve hukuka aykırı amaçlarla yok edilmesini, kaybolmasını veya değiştirilmesini önlemek için teknolojik imkânlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır.

a) Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan Teknik Tedbirler

Şirketimiz tarafından kişisel verilerin güvenli ortamlarda saklanması için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

- Kişisel verilerin güvenli ortamlarda saklanması için teknolojik gelişmelere uygun sistemler kullanılmaktadır.
- Teknik konularda uzman personel istihdam edilmektedir.
- Saklanma alanlarına yönelik teknik güvenlik sistemleri kurulmakta, alınan teknik önlemler iç denetim mekanizması gereği ilgilisine raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmektedir.
- Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için hukuka uygun bir biçimde yedekleme programları kullanılmaktadır.
- Bütün sistem seviyeli şifrelerin (örnek, root, administrator) 3 ayda bir sistem tarafından değişikliği istenmektedir.
- Sistem yöneticisi her sistem için farklı şifreler kullanılmaktadır.
- Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada güvensiz elektronik ortamlara yazmaması konusunda eğitilmektedir.
- Bir kullanıcı adı ve şifresi birim zamanda birden çok bilgisayarda kullanamamaktadır.
- Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, Web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen gösterilmektedir.
- Sunucular, fiziksel olarak güvenli ortamlarda tutulmaktadır. Sistem odalarına yetkisiz girişler engellenmiştir. Sistem odalarına giriş ve çıkışlar erişim kontrollü sağlanmaktadır.
- Sunuculara, kullanım amacına yönelik olarak işletim sistemi ve diğer yazılımlar kurulması yasaktır. Sunuculara kurulacak uygulamalar için Genel Müdür'den izin alınır.
- Sunucu üzerinde çalışan işletim sistemlerinin, sistem yazılımlarının ve güvenlik amaçlı yazılımların sürekli güncellenmesi sağlanmaktadır.
- Değişim Yönetim Politikası, sunucular için de uygulanmaktadır.
- Sunucu üzerinde kullanılmayan servisler kapatılmaktadır.
- Kritik ve önemli sunucular için aynı özellikte yedekleri tutulmakta, bir acil durum yaşanması durumunda bu yedek sunucu hemen devreye alınabilmektedir

- Şirketimiz, Bilişim Ağ ve Sistem Yöneticisi tarafından belirlendiği üzere, sunucu günlükleri (loglar) düzenli aralıklarla denetim ve izlemeye tabi tutulmaktadır.

- Sunucuların uzaktan yönetimi gerekiyor ise; yönetim konsolu ve sunucu arasındaki haberleşme VPN üzerinden SSL ile yapılmaktadır.

b) Kişisel Verilerin Güvenli Ortamlarda Saklanması için Alınan İdari Tedbirler

Şirketimiz tarafından kişisel verilerin güvenli ortamlarda saklanması için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

- Bilgi güvenliği ile ilgili uygulamalar; yasalara ve mevzuata uyumlu çalışılarak, anlaşmalardan doğan yükümlülüklere, iş yükümlülüklerine uyularak gerçekleştirilen tüm iş süreçlerimizi, çalışanlarımızı, müşterilerimizi, çözüm ortaklarımızı, tedarikçilerimizi ve yaptığımız işlerin sonuçlarından etkilenebilecek ilgili tarafların tümünü ilgilendirir.

- Şirketimize ait tüm varlıklar Varlık Envanteri içinde gösterilir. Varlık Envanteri zamanla ortaya çıkan değişiklikler ve gelişmeler çerçevesinde değişebilir. Varlık envanterinde, risk değerlendirme sonucunda elde edilen veriler, şirketimizde sürekli iyileştirmeye ve personelin eğitimine temel teşkil eder. Bilgi güvenliği uygulamaları gerçekleştirilen tüm faaliyetlerin vazgeçilmez bir boyutudur ve yılda en az bir kez gözden geçirilmektedir.

- Bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle Şirketimiz ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten çıkarılması, eğitilmesi, vb. konuların güvenlik ile ilgili boyutunu ne şekilde ele alacağını politika ve prosedürler ile belirler.

- Yürütülen tüm faaliyetlerde bilgi güvenliği yönetim sisteminin üç temel öğesinin sürekliliği sağlanmaktadır; Gizlilik: Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi, Bütünlük: Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi, Erişebilirlik: Yetkisi olanların gerektiği hallerde bilgiye ulaşabilirliğinin gösterilmesi, ilgili sistem standartları, sadece elektronik ortamda tutulan verilerin değil, yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği ile ilgilidir.

- Çalışanlar, kişisel verilerin güvenli bir biçimde saklanmasını sağlamak konusunda eğitilmektedirler.

- Herhangi bir kişiye telefonda şifre vermek yasaktır.

- Başkaları ile şifreleri paylaşmak yasaktır.

- Şifreler en az 90 günde bir değiştirilmektedir ancak müşterilerle ve partnerlerle dosya alışverişinde müşterinin/partnerin talebi üzerine parola kullanılmayabilir veya parolalar müşteri/partner talepleri doğrultusunda değiştirilebilir. 90 gün sonunda

müşteriye/partnere sunulan değişiklik talebinin reddedilmesi halinde müşteriyle/partnerle iletişimde süresi dolmuş parola kullanılmaya devam edilir.

- Veritabanı sunucuları, modemler, santral, anti-virüs programı, toplu eposta gönderim yazılımı erişim şifreleri sadece BT sorumlusu ve Genel Müdürün erişebildiği bir dökümanda saklanır.
- Şifrelerin değiştirilip değiştirilmediği kontrolünü sistem kendi yapmaktadır.
- Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmıştır.
- Kullanıcılara erişim haklarını açıklayan yazılı bildiriler verilmekte ve teyit alınmaktadır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi ile ilgili disiplin prosedürü uygulanmaktadır.
- Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmakta, beyan edilen akademik ve profesyonel bilgiler teyit deilmekte, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorgulaması yapılmaktadır.
- Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmaktadır.
- Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmektedir. Yıllık eğitim planlarında planlaması yapılarak eğitim kataloguna eklenmektedir.
- İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmektedir.

2.1.4 Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi

Şirketimiz, Kanun'un 12. maddesine uygun olarak, kendi bünyesinde gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları Şirketin iç işleyişi kapsamında konu ile ilgili bölüme raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

2.1.4. Kişisel Verilerin Yetkisiz Bir Şekilde İfşası Durumunda Alınacak Tedbirler

Şirketimiz, Kanun'un 12. maddesine uygun olarak işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede ilgili kişisel veri sahibine ve KVK Kurulu'na bildirilmesini sağlayan sistemi yürütmektedir.

KVK Kurulu tarafından gerekli görülmesi halinde, bu durum, KVK Kurulu'nun internet sitesinde veya başka bir yöntemle ilan edilebilecektir.

2.2. VERİ SAHİBİNİN HAKLARININ GÖZETİLMESİ; BU HAKLARI ŞİRKETİMİZE İLETECEĞİ KANALLARIN YARATILMASI VE VERİ SAHİPLERİNİN TALEPLERİNİN DEĞERLENDİRMESİ

Şirketimiz, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gereken bilgilendirmenin yapılması için Kanun'un 13. maddesine uygun olarak gerekli kanalları, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

Kişisel veri sahipleri aşağıda sıralanan haklarına ilişkin taleplerini yazılı olarak Şirketimize iletmeleri durumunda Şirketimiz talebin niteliğine göre talebi en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmaktadır. Ancak, işlemin ayrıca bir maliyeti veya çabayı gerektirmesi hâlinde, Şirketimiz tarafından KVK Kurulunca belirlenecek tarifedeki ücret, belirlenmemiş olması halinde makul bir ücret alınacaktır. Kişisel veri sahipleri;

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- Mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,
- Koşulların oluşması halinde kişisel verilerin imha edilmesini talep etme haklarına sahiptir.

Veri sahiplerinin hakları ile ilgili daha ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

2.3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI

Kanun ile bir takım kişisel verilere, hukuka aykırı olarak işlenildiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski nedeniyle özel önem atfedilmiştir.

Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Şirketimiz tarafından, Kanun ile "özel nitelikli" olarak belirlenen ve hukuka uygun olarak işlenen özel nitelikli kişisel verilerin korunmasında hassasiyetle davranılmaktadır. Bu kapsamda, Şirketimiz tarafından, kişisel verilerin korunması için alınan teknik ve idari tedbirler, özel nitelikli kişisel veriler bakımından özenle uygulanmakta ve Şirketimiz bünyesinde gerekli denetimler sağlanmaktadır.

Özel nitelikli kişisel verilerin işlenmesi ile ilgili ayrıntılı bilgiye bu Politika'nın 3. Bölümünde yer verilmiştir.

2.4. İŞ BİRİMLERİNİN KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ KONUSUNDA FARKINDALIKLARININ ARTTIRILMASI VE DENETİMİ

Şirketimiz, kişisel verilerin hukuka aykırı olarak işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemeye ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için iş birimlerine gerekli eğitimlerin düzenlenmesini sağlamaktadır.

Şirketimiz iş birimlerinin mevcut çalışanlarının ve iş birimi bünyesine yeni dâhil olmuş çalışanların kişisel verilerin korunması konusunda farkındalığının oluşması için gerekli sistemler kurulmakta, konuya ilişkin ihtiyaç duyulması halinde profesyonel kişiler ile çalışılmaktadır.

2.5. İŞ ORTAKLARI VE TEDARİKÇİLERİN KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ KONUSUNDAKİ FARKINDALIKLARININ ARTTIRILMASI VE DENETİMİ

Şirketimiz kişisel verilerin hukuka aykırı olarak işlenmesini önlenmesi, verilere hukuka aykırı olarak erişilmesini önlenmesi ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için iş ortaklarına yönelik eğitimler ve seminerler düzenlenmesini sağlamaktadır.

3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR

Şirketimiz, Anayasa'nın 20. maddesine ve Kanun'un 4. maddesine uygun olarak, kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmaktadır. Şirketimiz mevzuatta öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar kişisel verileri muhafaza etmektedir.

Şirketimiz, Anayasa'nın 20. ve Kanun'un 5. maddeleri gereğince kişisel verileri, kişisel verilerin işlenmesine ilişkin Kanun'un 5. maddesindeki şartlardan bir veya birkaçına dayalı olarak işlemektedir.

Şirketimiz, Anayasa'nın 20. ve Kanun'un 10. maddelerine uygun olarak kişisel veri sahiplerini aydınlatmakta ve kişisel veri sahiplerinin bilgi talep etmeleri durumunda gerekli bilgilendirmeyi yapmaktadır.

Şirketimiz, Kanun'un 6. maddesine uygun olarak özel nitelikli kişisel verilerin işlenmesi bakımından öngörülen düzenlemelere uygun hareket etmektedir.

Şirketimiz, Kanun'un 8. ve 9. maddelerine uygun olarak, kişisel verilerin aktarılması konusunda kanunda öngörülen ve KVK Kurulu tarafından ortaya konulan düzenlemelere uygun davranmaktadır.

3.1. KİŞİSEL VERİLERİN MEVZUATTA ÖNGÖRÜLEN İLKELERE UYGUN OLARAK İŞLENMESİ

3.1.1. Hukuka ve Dürüstlük Kuralına Uygun İşleme

Şirketimiz; kişisel verilerin işlenmesinde hukuksal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda Şirketimiz, kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta, kişisel verileri amacın gerektirdiği dışında kullanmamaktadır.

3.1.2. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama

Şirketimiz; kişisel veri sahiplerinin temel haklarını ve kendi meşru menfaatlerini dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını sağlamaktadır. Bu doğrultuda gerekli tedbirleri almaktadır. Örneğin, Şirket tarafından; kişisel veri sahiplerinin kişisel verilerini düzeltme ve doğruluğunu teyit etmelerine yönelik sistem kurulmuştur. Bu konu ile ilgili ayrıntılı bilgiye, bu Politika'nın 10. Bölümünde yer verilmiştir.

3.1.3. Belirli, Açık ve Meşru Amaçlarla İşleme

Şirketimiz, meşru ve hukuka uygun olan kişisel veri işleme amacını açık ve kesin olarak belirlemektedir. Şirketimiz, kişisel verileri sunmakta olduğu hizmetle bağlantılı ve bunlar için gerekli olan kadar işlemektedir. Şirketimiz tarafından kişisel verilerin hangi amaçla işleneceği henüz kişisel veri işleme faaliyeti başlamadan ortaya konulmaktadır.

3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Şirketimiz, kişisel verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işlemekte ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınmaktadır. Örneğin, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik kişisel veri işleme faaliyeti yürütülmemektedir.

3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Etme

Şirketimiz, kişisel verileri ancak ilgili mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza etmektedir. Bu kapsamda, Şirketimiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmakta, bir süre belirlenmemişse kişisel verileri işlendikleri amaç için gerekli olan süre kadar saklamaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler Şirketimiz tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir. Gelecekte kullanma ihtimali ile Şirketimiz tarafından kişisel veriler saklanmamaktadır. Bu konu ile ilgili ayrıntılı bilgiye, bu Politika'nın 9. Bölümünde yer verilmiştir.

3.2. KİŞİSEL VERİLERİN, KANUN'UN 5. MADDESİNDE BELİRTİLEN KİŞİSEL VERİ İŞLEME ŞARTLARINDAN BİR VEYA BİRKAÇINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLEME

Kişisel verilerin korunması Anayasal bir haktır. Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Anayasa'nın 20. maddesinin üçüncü fıkrası gereğince, kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilecektir. Şirketimiz bu doğrultuda ve Anayasa'ya uygun bir biçimde; kişisel verileri, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlemektedir. Bu konu ile ilgili ayrıntılı bilgiye, bu Politika'nın 7. Bölümünde yer verilmiştir.

3.3. KİŞİSEL VERİ SAHİBİNİN AYDINLATILMASI VE BİLGİLENDİRİLMESİ

Şirketimiz, Kanun'un 10. maddesine uygun olarak kişisel verilerin elde edilmesi sırasında kişisel veri sahiplerini aydınlatmaktadır. Bu kapsamda Şirket ve varsa temsilcisinin kimliğini, kişisel verilerin hangi amaçla işleneceğini, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile kişisel veri sahibinin sahip olduğu hakları konusunda aydınlatma yapmaktadır. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

Anayasa'nın 20. maddesinde herkesin, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme hakkına sahip olduğu ortaya konulmuştur. Bu doğrultuda Kanun'un 11. maddesinde kişisel veri sahibinin hakları arasında "bilgi talep etme" de sayılmıştır. Şirketimiz bu kapsamda, Anayasa'nın 20. ve Kanun'un 11. maddelerine uygun olarak kişisel veri sahibinin bilgi talep etmesi durumunda gerekli bilgilendirmeyi yapmaktadır. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 10. Bölümünde yer verilmiştir.

3.4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

Şirketimiz tarafından, Kanun ile "özel nitelikli" olarak belirlenen kişisel verilerin işlenmesinde, Kanun'da öngörülen düzenlemelere hassasiyetle uygun davranılmaktadır.

Kanun'un 6. maddesinde, hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşıyan bir takım kişisel veri "özel nitelikli" olarak belirlenmiştir. Bu

veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Kanun'a uygun bir biçimde Şirketimiz tarafından; özel nitelikli kişisel veriler, KVK Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla aşağıdaki durumlarda işlenmektedir:

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;

– Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,

– Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmektedir.

3.5. KİŞİSEL VERİLERİN AKTARILMASI

Şirketimiz hukuka uygun olan kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak kişisel veri sahibinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere aktarabilmektedir. Şirketimiz bu doğrultuda Kanun'un 8. maddesinde öngörülen düzenlemelere uygun hareket etmektedir. Bu konu ile ilgili ayrıntılı bilgiye bu Politika'nın 6. Bölümünde yer verilmiştir.

3.5.1. Kişisel Verilerin Aktarılması

Şirketimiz meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda aşağıda sayılan Kanun'un 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak kişisel verileri üçüncü kişilere aktarabilmektedir:

- Kişisel veri sahibinin açık rızası var ise;
- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Şirketimizin hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Kişisel veriler, kişisel veri sahibi tarafından alenileştirilmiş ise,
- Kişisel veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Şirketimizin meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

3.5.2. Özel Nitelikli Kişisel Verilerin Aktarılması

Şirketimiz gerekli özeni göstererek, gerekli güvenlik tedbirlerini alarak ve KVK Kurulu tarafından öngörülecek yeterli önlemleri alarak; meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin özel nitelikli verilerini aşağıdaki durumlarda üçüncü kişilere aktarabilmektedir.

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;

– Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir), kanunlarda öngörülen hallerde,

– Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından.

4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SÜRELERİ

Şirketimiz, Kanun'un 10. maddesine uygun olarak aydınlatma yükümlülüğü kapsamında hangi kişisel veri sahibi gruplarının kişisel verilerini işlediğini, kişisel veri sahibinin kişisel verilerinin işlenme amaçlarını ve saklama sürelerini kişisel veri sahibine bildirmektedir.

4.1. KİŞİSEL VERİLERİN KATEGORİZASYONU

Şirketimiz nezdinde, Kanun'un 10. maddesi uyarınca ilgili kişiler bilgilendirilerek, Şirketimizin meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda Kanun'un 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak Kanun'da başta kişisel verilerin işlenmesine ilişkin 4. maddede belirtilen ilkeler olmak üzere Kanun'da belirtilen genel ilkelere ve Kanun'da düzenlenen bütün yükümlülüklere uyarak işbu Politika kapsamındaki süjelerle sınırlı olarak aşağıda belirtilen kategorilerdeki kişisel veriler işlenmektedir. Bu kategorilerde işlenen kişisel verilerin işbu Politika kapsamında düzenlenen hangi veri sahipleriyle ilişkili olduğu da işbu Politika'nın 5. Bölümünde belirtilmektedir.

KİŞİSEL VERİ KATEGORİZASYONU	AÇIKLAMA
Kimlik Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Ehliyet, Nüfus Cüzdanı, İkametgâh, Pasaport, Avukatlık Kimliği, Evlilik Cüzdanı gibi dokümanlarda yer alan tüm bilgiler

İletişim Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan; kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; telefon numarası, adres, e-posta gibi bilgiler
Müşteri Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; ticari faaliyetlerimiz ve bu çerçevede iş birimlerimizin yürüttüğü operasyonlar neticesinde ilgili kişi hakkında elde edilen ve üretilen bilgiler
Aile Bireyleri ve Yakın Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan ve veri kayıt sistemi içerisinde yer alan; sunduğumuz hizmetlerle ilgili veya Şirketin ve veri sahibinin hukuki menfaatlerini korumak amacıyla kişisel veri sahibinin aile bireyleri ve yakınları hakkındaki bilgiler
Müşteri İşlem Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan ve veri kayıt sistemi içerisinde yer alan; hizmetlerimizin kullanımına yönelik kayıtlar ile müşterinin hizmetleri kullanımı için gerekli olan talimatları ve talepleri gibi bilgiler
Fiziksel Mekân Güvenlik Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan ve veri kayıt sistemi içerisinde yer alan; fiziksel mekâna girişte, fiziksel mekanın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler
İşlem Güvenliği Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan ve veri kayıt sistemi içerisinde yer alan; ticari faaliyetlerimizi yürütürken teknik, idari, hukuki ve ticari güvenliğimizi sağlamamız için işlenen kişisel verileriniz
Risk Yönetimi Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan ve veri kayıt sistemi içerisinde yer alan; ticari, teknik ve idari risklerimizi yönetebilmemiz için bu alanlarda genel kabul görmüş hukuki, ticari teamül ve dürüstlük kuralına uygun olarak kullanılan yöntemler vasıtasıyla işlenilen kişisel veriler
Finansal Bilgi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; şirketimizin kişisel veri sahibi ile kurmuş olduğu hukuki ilişkinin tipine göre yaratılan her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler
Özlük Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; çalışanlarımızın veya Şirketimizle çalışma ilişkisi içerisinde olan gerçek kişilerin özlük haklarının oluşmasına temel olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veri

Çalışan Adayı Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirketimizin çalışanı olmak için başvuruda bulunmuş veya ticari teamül ve dürüstlük kuralları gereği şirketimizin insan kaynakları ihtiyaçları doğrultusunda çalışan adayı olarak değerlendirilmiş veya Şirketimizle çalışma ilişkisi içerisinde olan bireylerle ilgili işlenen kişisel veriler
Çalışan İşlem Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; çalışanlarımızın veya şirketimizle çalışma ilişkisi içerisinde olan gerçek kişilerin işle ilgili gerçekleştirdiği her türlü işleme ilişkin işlenen kişisel veriler
Çalışan Performans ve Kariyer Gelişim Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; çalışanlarımızın veya Şirketimizle çalışma ilişkisi içerisinde olan gerçek kişilerin performanslarının ölçülmesi ile kariyer gelişimlerinin şirketimizin insan kaynakları Politikası kapsamında planlanması ve yürütülmesi amacıyla işlenilen kişisel veriler
Yan Haklar ve Menfaatler Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Çalışanlara veya Şirketimizle çalışma ilişkisi içerisinde olan diğer gerçek kişilere sunduğumuz ve sunacağımız yan-haklar ve menfaatlerin planlanması, bunlara hak kazanımla ilgili objektif kriterlerin belirlenmesi ve bunlara hak edişlerin takibi işin işlenen kişisel verileriniz
Hukuki İşlem ve Uyum Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; hukuki alacak ve haklarımızın tespiti, takibi ve borçlarımızın ifası ile kanuni yükümlülüklerimiz ve şirketimizin politikalarına uyum kapsamında işlenen kişisel verileriniz
Denetim ve Teftiş Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirketimizin kanuni yükümlülükleri ve şirket politikalarına uyumu kapsamında işlenen kişisel verileriniz
Özel Nitelikli Kişisel Veri	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Kanun'un 6. maddesinde belirtilen veriler

Talep/Şikayet Yönetimi Bilgisi	Kimliği belirli veya belirlenebilir bir gerçek kişiye ait olduğu açık olan, kısmen veya tamamen otomatik şekilde veya veri kayıt sisteminin bir parçası olarak otomatik olmayan şekilde işlenen; Şirketimize yöneltilmiş olan her türlü talep veya şikayetin alınması ve değerlendirilmesine ilişkin kişisel veriler

4.2. KİŞİSEL VERİNİN İŞLENME AMAÇLARI

Şirketimiz Kanun'un 5. maddesinin 2. fıkrasında ve 6. maddenin 3. fıkrasında belirtilen kişisel veri işleme şartları içerisindeki amaçlarla ve koşullarla sınırlı olarak kişisel veriler işlemektedir. Bu amaçlar ve koşullar;

- Kişisel verilerinizin işlenmesine ilişkin Şirketimizin ilgili faaliyette bulunmasının mevzuatta açıkça öngörülmesi,
- Kişisel verilerinizin Şirketimiz tarafından işlenmesinin bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olması,
- Kişisel verilerinizin işlenmesinin Şirketimizin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Kişisel verilerinizin sizler tarafından alenileştirilmiş olması şartıyla; sizlerin alenileştirme amacıyla sınırlı bir şekilde Şirketimiz tarafından işlenmesi,
- Kişisel verilerinizin Şirketimiz tarafından işlenmesinin Şirketimizin veya sizlerin veya üçüncü kişilerin haklarının tesisi, kullanılması veya korunması için zorunlu olması,
- Sizlerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketimiz meşru menfaatleri için kişisel veri işleme faaliyetinde bulunulmasının zorunlu olması,
- Şirketimiz tarafından kişisel veri işleme faaliyetinde bulunulmasının kişisel veri sahibinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması ve bu durumda da kişisel veri sahibinin fiili imkânsızlık veya hukuki geçersizlik nedeniyle rızasını açıklayamayacak durumda bulunması,
- Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verilerin işlenmesinin kanunlarda öngörülmesi,
- Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesidir.

Bu şartların bulunmaması halinde; kişisel veri işleme faaliyetinde bulunmak için Şirket kişisel veri sahiplerinin açık rızalarına başvurmaktadır.

Yukarıda belirtilen koşullar altında; Şirketimiz kişisel verileri, bunlarla sınırlı olmamak üzere aşağıdaki amaçlarla işleyebilmektedir:

- Şirket tarafından yürütülen ticari faaliyetlerin gerçekleştirilmesi için ilgili iş birimlerimiz tarafından gerekli çalışmaların yapılması ve buna bağlı iş süreçlerinin yürütülmesi doğrultusunda; işbu faaliyetler ile ilgili şirketimizden hizmet alan müşterilerimizin veri sorumlusu sıfatıyla, kendi çalışanları ve ilgili kişilerden (veri sahibi) gerekli izinleri almaları ve kendi aydınlatma yükümlülükleri doğrultusunda hareket etmeleri zorunludur.

- İş faaliyetlerinin ve iş sürekliliğinin sağlanması faaliyetlerinin planlanması ve icrası,
- Finans ve/veya muhasebe işlerinin takibi,
- Etkinlik yöntemi,
- Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Operasyon süreçlerinin planlaması ve icrası
- İş ortakları ve/veya tedarikçilerin bilgiye erişim yetkililerinin planlanması ve icrası
- Her türlü insan kaynakları, danışmanlık, bordro hesaplaması, ücret yönetimi
- Her türlü yazılım hizmetlerinin icrası
- Çalışma izni, kayıtlı e-posta, e-imza ve benzeri hizmetlerin hukuki gereklilikleri.

• Şirket tarafından hizmetlerden ilgili kişileri faydalandırmak için gerekli çalışmaların iş birimlerimiz tarafından yapılması ve ilgili iş süreçlerinin yürütülmesi doğrultusunda;

- Müşteri ilişkileri yönetimi süreçlerinin planlanması ve icrası,
- Müşteri talep ve/veya şikayetlerinin takibi,
- Hizmetlerin pazarlama süreçlerinin planlanması ve icrası,
- Sözleşme süreçlerinin ve/veya hukuki taleplerin takibi,

• Şirketimizin insan kaynakları politikalarının yürütülmesinin temini amacı doğrultusunda;

- İş sağlığı ve güvenliği çerçevesinde yükümlülüklerin yerine getirilmesi ve gerekli tedbirlerin alınması
- Şirketimizin insan kaynakları politikalarına uygun şekilde işe başvuruların değerlendirilmesi,
- Şirket çalışanları için iş akdi ve/veya mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
- Personel işe giriş-çıkış işlemlerinin yapılması,
- Ücret-performans sürecinin değerlendirilmesi,
- Ücret ve bordroların yönetilmesi,
- Şirket içi eğitim faaliyetlerinin planlanması ve/veya icrası ve
- Diğer insan kaynakları operasyonlarının yürütülmesi,

• Şirketimizin ve şirketimizle iş ilişkisi içerisinde olan kişilerin hukuki ve ticari güvenliğinin temini amacı doğrultusunda;

- Şirketin hukuk işlerinin takibi,
- Şirket faaliyetlerinin şirket prosedürleri ve/veya ilgili mevzuata uygun olarak yürütülmesinin temini için gerekli operasyonel faaliyetlerinin planlanması ve icrası,
- Ziyaretçi kayıtlarının oluşturulması ve takibi,
- Şirket demirbaşlarının ve/veya kaynaklarının güvenliğinin temini,
- Şirket operasyonlarının güvenliğinin temini,
- Acil durum yönetimi süreçlerinin planlanması ve icrası,
- Şirketin finansal risk süreçlerinin planlanması ve/veya icrası,

• Şirketimizin ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda;

- Şirketimiz tarafından yürütülen finans operasyonları, iletişim, pazar araştırması ve sosyal sorumluluk aktiviteleri, satın alma operasyonları, ürün/proje/imalat/yatırım kalite süreçleri ve operasyonları,
- Şirket içi sistem ve uygulama yönetimi operasyonları
- Şirket dışı eğitim faaliyetlerinin planlanması ve/veya icrası,
- İş ortakları ve/veya tedarikçilerle olan ilişkilerin yönetimi

gibi amaçlar olarak sıralanabilmektedir.

Kişisel veri sahibinin açık rızasını vermemesi durumunda yukarıda amaca giren ilgili iş birimlerimizin tüm kişisel veri işleme faaliyetlerin yapılamaması değil; ilk paragrafta belirtilen kişisel veri sahibinin veri işlemeye yönelik açık rızasına gerek olmayan aynı amaç kapsamı içindeki kişisel veri işleme faaliyetlerinin dışında kalan ve bu amaca yönelmiş ilgili iş birimlerimizin kişisel veri işleme faaliyetlerinin yapılamayacağı anlamı çıkmalıdır.

4.3. KİŞİSEL VERİLERİN SAKLANMA SÜRELERİ

Şirketimiz, ilgili kanunlarda ve mevzuatlarda öngörülmesi durumunda kişisel verileri bu mevzuatlarda belirtilen süre boyunca saklanmaktadır.

Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre düzenlenmemişse, kişisel veriler şirketimizin o veriyi işlerken sunduğu hizmetlerle bağlı olarak Şirketimizin uygulamaları ve ticari yaşamının teamülleri uyarınca işlenmesini gerektiren süre kadar işlenmekte daha sonra silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu konu ile ilgili ayrıntılı bilgiye bu Politikanın 9. Bölümünde yer verilmiştir.

Kişisel verilerin işlenme amacı sona ermiş; ilgili mevzuat ve şirketin belirlediği saklama sürelerinin de sonuna gelinmişse; kişisel veriler yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zamanaşımı süreleri ile zamanaşımı sürelerinin geçmesine rağmen daha önce aynı konularda Şirketimize yöneltilen taleplerdeki örnekler esas alınarak saklama süreleri belirlenmektedir. Bu durumda saklanan kişisel verilere başka bir amaçla erişilememekte ve ancak ilgili hukuki uyuşmazlıkta kullanılması gerektiği zaman ilgili kişisel verilere erişim sağlanmaktadır. Burada da bahsi geçen süre sona erdikten sonra kişisel veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

5. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN SAHİPLERİNE İLİŞKİN KATEGORİZASYON

5.1. KİŞİSEL VERİ KATEGORİZASYONU

Şirketimiz tarafından, aşağıda sıralanan kişisel veri sahibi kategorilerinin kişisel verileri işlenmekle birlikte, işbu Politika'nın uygulama kapsamı müşterilerimizin, potansiyel müşterilerimizin, çalışan adaylarımızın, şirket hissedarlarının, şirket yetkililerinin,

ziyaretçilerimizin, iş birliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkililerinin ve üçüncü kişilerle sınırlıdır.

Şirketimiz tarafından kişisel verileri işlenen kişilerin kategorileri yukarıda belirtilen kapsamda olmakla birlikte, bu kategorilerin dışında yer alan kişiler de Kanun kapsamında Şirketimize taleplerini yöneltebilecek olup; bu kişilerin talepleri de bu Politika kapsamında değerlendirmeye alınacaktır.

Aşağıda işbu Politika kapsamında yer alan üçüncü kişilerle ilgili kavramla açıklık getirilmektedir.

Kişisel Veri Sahibi Kategorisi	Açıklaması
Müşteri	Şirketimizle herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirketimizin sunmuş olduğu hizmetleri kullanan veya kullanmış olan gerçek kişiler
Potansiyel Müşteri	Hizmetlerimizi kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişiler
Ziyaretçi	Şirketimize fiziksel olarak çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler
Üçüncü Kişi	Şirketimizin yukarıda bahsi geçen taraflarla arasındaki ticari işlem güvenliğini sağlamak veya bahsi geçen kişilerin haklarını korumak ve menfaat temin etmek üzere bu kişilerle ilişkili olan üçüncü taraf gerçek kişiler
Çalışan Adayı	Şirketimize herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini şirketimizin incelemesine açmış olan gerçek kişiler
Şirket Hissedarı	Şirketimizin hissedarı gerçek kişi(ler)
Şirket Yetkilisi	Şirketimizin yönetim kurulu üyesi ve diğer yetkili gerçek kişi(ler)
İş birliği İçerisinde Olduğumuz Kurumların Çalışanları, Hissedarları ve Yetkilileri	Şirketimizin her türlü iş ilişkisi içerisinde bulunduğu kurumlarda (iş ortağı, tedarikçi gibi, ancak bunlarla sınırlı olmaksızın) çalışan, bu kurumların hissedarları ve yetkilileri dahil olmak üzere, gerçek kişiler

6. ŞİRKETİMİZ TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI

6.1. AKTARIM ARAÇLARI

Şirketimiz, Kanun'un 10. maddesine uygun olarak kişisel verilerin aktarıldığı kişi gruplarını kişisel veri sahibine bildirmektedir.

Şirketimiz Kanun'un 8. ve 9. maddelerine uygun olarak müşterilerin kişisel verilerini aşağıda sıralanan kişi kategorilerine aktarılabilir:

(i) iş ortaklarına
(ii) tedarikçilerine
(iii) iştiraklerine
(iv) hissedarlarına
(v) hukuken yetkili kamu kurum ve kuruluşlarına
(vi) hukuken yetkili özel hukuk kişilerine

Şirketimiz tarafından gerçekleştirilen aktarımlarda Politika'nın 2. ve 3. Bölümlerinde düzenlenmiş hususlara uygun olarak hareket edilmektedir.

7. KİŞİSEL VERİLERİN KANUNDAKİ İŞLEME ŞARTLARINA DAYALI VE BU ŞARTLARLA SINIRLI OLARAK İŞLENMESİ

Şirketimiz, Kanun'un 10. maddesine uygun olarak işlediği kişisel veriler hakkında kişisel veri sahibini aydınlatmaktadır.

7.1. KİŞİSEL VERİLERİN VE ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

7.1.1. Kişisel Verilerin İşlenmesi

Kişisel veri sahibinin açık rıza vermesi, kişisel verilerin hukuka uygun olarak işlenmesini mümkün kılan hukuki dayanaklardan yalnızca bir tanesidir. Açık rıza dışında, aşağıda yazan diğer şartlardan birinin varlığı durumunda da kişisel veriler işlenebilir. Kişisel veri işleme faaliyetinin dayanağı aşağıda belirtilen şartlardan yalnızca biri olabildiği gibi bu şartlardan birden fazlası da aynı kişisel veri işleme faaliyetinin dayanağı olabilir. İşlenen verilerin özel nitelikli kişisel veri olması halinde; aşağıda bu bölüm altında yer alan şartlar uygulanır.

Şirketimiz tarafından kişisel verilerin işlenmesine yönelik hukuki dayanaklar farklılık gösterse de, her türlü kişisel veri işleme faaliyetinde Kanun'un 4. maddesinde belirtilen genel ilkelere uygun olarak hareket edilmektedir.

(i) Kişisel Veri Sahibinin Açık Rızasının Bulunması

Kişisel verilerin işlenme şartlarından biri sahibinin açık rızasıdır. Kişisel veri sahibinin açık rızası belirli bir konuya ilişkin, bilgilendirilmeye dayalı olarak ve özgür iradeyle açıklanmalıdır.

Kişisel verilerin elde edilme sebeplerine yönelik işleme amacının (birincil işleme) dışındaki kişisel veri işleme faaliyetleri (ikincil işleme) işbu başlığın (ii), (iii), (iv) (v), (vi), (vii) ve (viii)'de yer alan şartlardan en az biri aranmakta; bu şartlardan biri yok ise, Şirketimiz tarafından bu kişisel veri işleme faaliyetleri kişisel veri sahibinin bu işleme faaliyetlerine yönelik açık rızasına dayalı olarak gerçekleştirilmektedir.

Kişisel verilerin, kişisel veri sahibinin açık rıza vermesine bağlı olarak işlenmesi için, müşteri, potansiyel müşteri ve ziyaretçilerden ilgili yöntemler ile açık rızaları alınmaktadır.

(ii) Kanunlarda Açıkça Öngörülmesi

Veri sahibinin kişisel verileri, kanunda açıkça öngörülmesi halinde hukuka uygun olarak işlenebilecektir.

(iii) Fiili İmkânsızlık Sebebiyle İlgilinin Açık Rızasının Alınamaması

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda olan veya rızasına geçerlilik tanınamayacak olan kişinin kendisinin ya da başka bir kişinin hayatı veya beden bütünlüğünü korumak için kişisel verisinin işlenmesinin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

(iv) Sözleşmenin Kurulması veya İfasıyla Doğrudan İlgi Olması

Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması halinde kişisel verilerin işlenmesi mümkündür.

(v) Şirketin Hukuki Yükümlülüğünü Yerine Getirmesi

Şirketimizin veri sorumlusu olarak hukuki yükümlülüklerini yerine getirmesi için işlemenin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

(vi) Kişisel Veri Sahibinin Kişisel Verisini Alenileştirmesi

Veri sahibinin, kişisel verisini kendisi tarafından alenileştirilmiş olması halinde ilgili kişisel veriler işlenebilecektir.

(vii) Bir Hakkın Tesisi veya Korunması için Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

(viii) Şirketimizin Meşru Menfaati için Veri İşlemenin Zorunlu Olması

Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketimizin meşru menfaatleri için veri işlemesinin zorunlu olması halinde veri sahibinin kişisel verileri işlenebilecektir.

7.1.2. Özel Nitelikli Kişisel Verilerin İşlenmesi

Şirketimiz tarafından; özel nitelikli kişisel veriler kişisel veri sahibinin açık rızası yok ise ancak, KVK Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla aşağıdaki durumlarda işlenmektedir:

(i) Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,

(ii) Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından.

(iii) İnsan kaynakları ve bordrolama süreçleri ile ilgili hizmetlerin sağlanabilmesi için vizite, rapor, hastalık izni, hamilelik izni ve iş kanunu , saosyal güvenlik ve iş sağlığı hükümlerince özlük bakımından takibi zorunlu haller.

8. BİNA İÇERİSİNDE YAPILAN KİŞİSEL VERİ İŞLEME FAALİYETLERİ

Bu bölümde Şirketimizin kamera ile izleme sistemine ilişkin açıklamalar yapılacak ve kişisel verilerin, gizliliğinin ve kişinin temel haklarının nasıl korumaya alındığına ilişkin bilgilendirme yapılacaktır.

Şirketimiz, güvenlik kamerası ile izleme faaliyeti kapsamında; sunulan hizmetin kalitesini artırmak, güvenilirliğini sağlamak, şirketin, müşterilerin ve diğer kişilerin güvenliğini sağlamak ve müşterilerin aldıkları hizmete ilişkin menfaatlerini korumak gibi amaçlar taşımaktadır.

Hırsızlık –Sabotaj – Vandalizm ' önlemleri:

Hırsızlık ve terörizm'e karşı bina güvenliği, bina yönetimi tarafından sağlanmaktadır. Şirketimiz'e girişler Kamera kaydı ile kontrol edilmektedir..

* Kapalı devre kamera sistemleri, ses kayıt cihazları,

Kapalı Devre (Closed Circuit TV) dışarı görüntü vermemektedir. LCD TV'den izlenmektedir.

Internet Üzerinden Şirket Yöneticileri tarafından görüntülenmaktedir.

Hareket dedektörleri , hırsız alarmları,

8.1. iZLEME FAALİYETLERİ

8.1.1. Kamera ile İzleme Faaliyetinin Yasal Dayanağı

Şirketimiz tarafından yürütülen kamera ile izleme faaliyeti, Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata uygun olarak sürdürülmektedir.

8.1.2. KVK Hukukuna Göre Güvenlik Kamerası ile İzleme Faaliyeti Yürütülmesi

Şirketimiz tarafından güvenlik amacıyla kamera ile izleme faaliyeti yürütülmesinde Kanun'da yer alan düzenlemelere uygun hareket edilmektedir.

Şirketimiz, güvenliğin sağlanması amacıyla, kanunlarda öngörülen amaçlarla ve Kanun'da sayılan kişisel veri işleme şartlarına uygun olarak güvenlik kamerası izleme faaliyetinde bulunmaktadır.

8.1.3. Kamera ile İzleme Faaliyetinin Duyurulması

Şirketimiz tarafından Kanun'un 10. maddesine uygun olarak kişisel veri sahibi aydınlatılmaktadır.

Şirketimiz, genel hususlara ilişkin olarak yaptığı aydınlatmanın (Bkz. Bölüm 3/Başlık 3.3) yanı sıra AB'deki mehaz düzenlemelere uygun olarak kamera ile izleme faaliyetine ilişkin birden fazla yöntem ile bildirimde bulunmaktadır.

Böylelikle, kişisel veri sahibinin temel hak ve özgürlüklerine zarar verilmesinin engellenmesi, şeffaflığın ve kişisel veri sahibinin aydınlatılmasının sağlanması amaçlanmaktadır.

8.1.4. Kamera ile İzleme Faaliyetinin Yürütülme Amacı ve Amaçla Sınırlılık

Şirketimiz, Kanun'un 4. maddesine uygun olarak, kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işlemektedir.

Şirketimiz tarafından video kamera ile izleme faaliyetinin sürdürülmesindeki amaç bu Politika'da sayılan amaçlarla sınırlıdır. Bu doğrultuda, güvenlik kameralarının izleme alanları, sayısı ve ne zaman izleme yapılacağı, güvenlik amacına ulaşmak için yeterli ve bu amaçla sınırlı olarak uygulamaya alınmaktadır. Kişinin mahremiyetini güvenlik amaçlarını aşan şekilde müdahale sonucu doğurabilecek alanlarda (örneğin, tuvaletler) izlemeye tabi tutulmamaktadır.

8.1.5. Elde Edilen Verilerin Güvenliğinin Sağlanması

Şirketimiz tarafından Kanun'un 12. maddesine uygun olarak, kamera ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır. (Bkz. Bölüm 2/Başlık 2.1)

8.1.6. Kamera ile İzleme Faaliyeti ile Elde Edilen Kişisel Verilerin Muhafaza Süresi

Şirketimizin, kamera ile izleme faaliyeti ile elde edilen kişisel verileri muhafaza süresi ile ilgili ayrıntılı bilgiye bu Politika'nın Kişisel Verilerin Saklanma Süreleri isimli 4.3. maddesinde yer verilmiştir.

8.1.7. İzleme Sonucunda Elde Edilen Bilgilere Kimlerin Erişebildiği ve Bu Bilgilerin Kimlere Aktarıldığı

Dijital ortamda kaydedilen ve muhafaza edilen kayıtlara yalnızca sınırlı sayıda çalışanının erişimi bulunmaktadır.

8.2. BİNA İÇERİSİNDE YÜRÜTÜLEN MİSAFİR GİRİŞ ÇIKIŞLARININ TAKİBİ

Şirketimiz tarafından; güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla, misafir giriş çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunulmaktadır.

Misafir olarak binaya gelen kişilerin isim ve soyadları elde edilirken ya da Şirket nezdinde asılan ya da diğer şekillerde misafirlerin erişimine sunulan metinler aracılığıyla söz konusu kişisel veri

sahipleri bu kapsamda aydınlatılmaktadırlar. Misafir giriş-çıkış takibi yapılması amacıyla elde edilen veriler yalnızca bu amaçla işlenmekte, ve ilgili kişisel veriler fiziki ortamda veri kayıt sistemine kaydedilmektedir.

8.3. BİNA ZİYARETÇİLERİMİZE SAĞLANAN İNTERNET ERİŞİMLERİNE İLİŞKİN KAYITLARIN SAKLANMASI

Şirketimiz tarafından güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla; Şirketimiz tarafından talep eden Ziyaretçilerimize internet erişimi sağlanabilmektedir. Bu durumda internet erişimlerinize ilişkin log kayıtları 5651 Sayılı Kanun ve bu Kanuna göre düzenlenmiş olan mevzuatın amir hükümlerine göre kayıt altına alınmakta; bu kayıtlar ancak yetkili kamu kurum ve kuruluşları tarafından talep edilmesi veya Şirket içinde gerçekleştirilecek denetim süreçlerinde ilgili hukuki yükümlülüğümüzü yerine getirmek amacıyla işlenmektedir.

Bu çerçevede elde edilen log kayıtlarına yalnızca sınırlı sayıda çalışanın erişimi bulunmaktadır. Bahsi geçen kayıtlara erişimi olan Şirket çalışanları bu kayıtları yalnızca yetkili kamu kurum ve kuruluşundan gelen talep veya denetim süreçlerinde kullanmak üzere erişmekte ve hukuken yetkili olan kişilerle paylaşmaktadır. Kayıtlara erişimi olan sınırlı sayıda kişi gizlilik taahhütnamesi ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

8.4. YANGIN

Duman, disklerinin kafalarına, optik disklere ve teyp sürücülerine etki eder. Duman konusunda en tehlikeli kaynak sigaradır. Sistem odasında sigara içilmesine izin verilmemektedir.

Sistem odasındaki yangın ve duman detektörlerinin çalışır durumda olduğu kontrol edilmelidir. Alarm durumunda ilgili kişilere e-mail, SMS, telefon vb. yollarıyla alarmların ulaşması sağlanmalıdır. Otomatik yangın alarm sisteminin yanlış alarm ve acil durumlarda durdurulabilir olduğu denetlenmektedir.

Taşınabilir yangın söndürücülerin kapıya olabildiğince yakın olması ve sistem odasına girme yetkisine sahip personelin bu söndürücüyü kullanabilme konusunda yeterli deneyime sahib olması, yangın söndürücülerin doluluğunun aylık olarak kontrol edilmesi sağlanmaktadır.

Sistem odalarında özellikle otomatik gazlı yangın söndürme sistemleri tercih edilmelidir.Eğer yangın söndürme sistemi CO^2, FM200, NAF-S–III, Halon gibi gazlı bir sistem ise, yangın alarmı ile birlikte sistem odasına girecek personelin gazdan etkilenmemesi için yapması gerekenleri gösteren uyarı panosununda sistem odasının dış kapısına ya da uygun bir yere yerleştirilmesi sağlanmaktadır.

Cep telefonları, walkie-talkie'ler, her türlü radyo alıcı ve vericileri bilgisayar sistemlerine zarar verir. Özellikle güçlü vericiler, bilgisayar sistemlerine kalıcı zararlar verebilirler. Bazı gazlı yangın söndürücü sistemleri belirtilen alıcı-vericilerin yakın çevresinde iken patlama eğilimi gösterebilirler. Bu tür yangın söndürücülerin bulundugu ortamlarda kesinlikle alıcı ve vericiler kullanılmamaktdır. Her türlü alıcı ve verici, bilgisayar sistemlerinden, kablolardan ve çevre birimlerinden en az 2.5 m uzakta tutulmaktadır.

8.5. SICAKLIK

İnsanlar gibi bilgisayar donanımlarıda belirli sıcaklık değerleri arasında işlevselliklerini sürdürebilirler. Birçok donanım için 10-25 °C arası oda sıcaklıklarının korunması uygun olacaktır. Eğer donanımların içinde bulunduğu ortamın sıcaklığı çok yüksek ise, sistemlerin fanları yeterli gelmeyecek, donanımların bileşenleri zarar görebilecek veya sistemler koruma durumuna geçecektir. Eğer sıcaklık çok düserse, donanımlar açıldığında termal şoka uğrayarak elektronik devrelerinin çatlaması nedeniyle çalısmaz hale gelebilecektir.

Donanımların kullanım klavuzlarından faydalanarak uygun sıcaklık aralıkları tespit edilip (genelde 20-25 °C), klima ve iklimlendirme sistemleriyle uygun oda sıcaklığı dengelenmektedir.

Sistem odasına termal ısı dedektörleri yerleştirerek çok sıcak ve çok soğuk durumlarda alarmların oluşturulması sağlanmalıdır. Alarm durumunda ilgili kişilere e-mail, SMS, telefon vb. yollarla alarmların ulaşması sağlanmaktadır.

Duvarlara çok yakın yerleştirilen donanımlar, havalandırmayı engelleyerek, sistemlerin iç ısılarının yükselmesine neden olabilir. Bu nedenle, donanımların duvarlara çok yakın yerleştirilmemesine özen gösterilmektedir.

8.6. DEPREM VE PATLAMA

Titreşim, insanları rahatsız etmeyecek kadar az da olsa, uzun sürede bilgisayar sistemlerine zarar verebilir. En hafif titreşim bile, zamanla sabit disklerin kafa ayarlarının bozulmasına sebeb olabilir. Çok yüksek titreşimlerin olduğu bir bölgedeyseniz, sistem odası zeminine kauçuk veya lastik türevi maddeler kullanılması düşünülülebilir.

Her deprem, sistemlere doğrudan zarar vermesede, dolaylı olarak donanımların zarar görmesiyle sonuçlanacak bir etkiye sebep olabilir. Olası büyük bir depremde iş sürekliliğinin sağlanması için;

- Donanımların, zeminden çok yükseğe yerleştirilmesinden kaçınılmaktadır.
- Rack'lerin yere, tavana, kendi aralarında rack mount kitlerle sabitlenmesi sağlanmaktadır.
- Rack'lerin içindeki tüm donanımların vidalarla ve kablo bağlarıyla sabitlenmesi sağlanmaktadır.
- Donanımlar özellikle zeminin üzerindeki katlarda, pencerelerden uzak tutulmaktadır.

Her ne kadar bilgisayar sistemleri patlamaya meyilli olmasalarda, bu sistemlerin içinde bulunduğu binaların özellikle doğal gaz ve yanıcı bileşenlerin depolandığı binalarda patlama oluşma ihtimali vardır. Deprem, patlama ihtimaline karşı, donanımların özel çelik kasa veya konstrüksiyon içerisinde saklaması düşünülebilir.

Sistem odasının yeri, patlama için merkez olabilecek istasyonlardan uzak olacak biçimde seçilmiştir. Yedekler patlamaya ve depreme dayanabilecek kasalar içerisinde ya da kurum dışındaki başka güvenli mekanlarda saklanmaktadır. Sistem yedeklerinin farklı lokasyonlarda tutulmasıyla ve farklı sunucu yada disaster recovery merkezlerinde alternatif aynalama yöntemlerinin oluşturulmasıyla iş sürekliliği sağlanmaktadır.

9. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI

Şirketimiz, Türk Ceza Kanunu'nun 138. maddesinde ve Kanun'un 7. maddesinde ve Yönetmelik'te düzenlendiği üzere ilgili hükümlere uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Şirketimizin kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir.

9.1. KİŞİSEL VERİLERİ SİLME, YOK ETME VE ANONİMLEŞTİRME YÜKÜMLÜLÜĞÜ

Türk Ceza Kanunu'nun 138. maddesinde ve Kanun'un 7. Maddesinde ve Yönetmelik'te düzenlendiği üzere ilgili hükümlere uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Şirketimizin kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hâle getirilir. Bu kapsamda Şirketimiz ilgili yükümlülüğünü bu bölümde açıklanan yöntemlerle yerine getirmektedir.

9.2. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ TEKNİKLERİ

Kayıt ortamları l: Hizmet verdiğimiz, Veri Sorumlularına ve Veri sahiplerine ait kişisel veriler, Şirketimiz tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Elektronik Ortamlar

- Firewall'lar
- DHCP
- DC
- File Server
- SQL Server1
- SQL Server2
- Application Server1
- Application Server2
- Application Server3
- Application Server4
- Application Server5
- Storage Server
- TFS Server
- Terminal Server

- Web Application Server1
- Web Application Server2
- Web Application Server3 (SOLLinux)
- WSUS
- MAIN Sunucu
- Replika Sunucu1
- Replika Sunucu2

Fiziksel Ortamlar

- Birim Dolapları
- Sistem Odası
- Arşiv Odaları
- Arşiv Tedarikçisi Şirketler

Yazılımlar

- Informasoft
- Bordromat
- Logo
- Delta
- Global Partnerlerin Sistemleri
- X2
- Luca
- Microsoft Office Ortamları

9.2.1. Kişisel Verilerin Silinmesi

Şirketimiz ilgili hükümlere uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir veya yok edebilir. Şirketimiz tarafından en çok kullanılan silme veya yok etme teknikleri aşağıda sıralanmaktadır:

Şirketimiz çalışanlarının şirkete ait taşınabilir ortamlarda kişisel veri tutması yasaklanmış ve bu husus politika ve prosedürler ile takip edilmektedir.

Taşınabilir ortamların çalınmasına karşın, çeşitli gelişmiş crypto ve kilitleme (yazılımsal) teknikleri kullanılmaktadır.

(i) Fiziksel Olarak Silme

Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu alanda fiziksel verinin türüne göre farklı yöntemler belirlenebilir. Genel olarak, **ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması, dosyadan**

alınması ve okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi yöntemi kullanılabilir.

(ii) Yazılımdan Güvenli Olarak Silme (Secure Deletion Softare)

Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut ortamlarda ilgili verilerin silinmesi; **merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması**, kısıtlanması; veri tabanlarında ilgili satırların veri tabanı sorguları ile silinmesi; veya taşınabilir medyada bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

– Başka herhangi bir kurum, kuruluş veyahut kişinin kullanımına ve erişimine kapalı olması,

– Kişisel verilere yalnızca şirketimiz ile ilişkili yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

(iii) Uzman Tarafından Güvenli Olarak Silme (Sending to a Specialist for Secure Deletion)

Şirketimiz bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile iş birliği yapabilir. Bu durumda kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

9.2.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi ihtiyacında aşağıdaki yöntemleri bir ya da birkaçı kullanılabilir.

De-manyetize Etme (Degaussing): Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Genel olarak Degaussing olarak adlandırılan proses ile istenmeyen datanın veri kayıt ortamında bozulmaya uğratılmasıdır. Bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.

Fiziksel Olarak Yok Etme (Physical Destruction):

Bazı veriler kağıt ortamında bulunabilir(Personel özlük dosyaları gibi). Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Bu alanda fiziksel verinin türüne göre farklı yöntemler belirlenebilir. Genel olarak, ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması, dosyadan alınması ve geri döndürülemeyecek, okunamayacak şekilde kağıt imha cihazından geçirilmesi yöntemi uygulanır.

Manyetik veri ortamları'nın fiziksel olarak kimyasal işlemler ve hard-disk kırıcı, kesiciler ile yok edilmesinde, cihaz ve medya politikalarındaki yönergelerden yararlanılır.

Üzerine Yazma (overwrite): Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler

yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

9.2.3. Kişisel Verileri Anonim Hale Getirme Teknikleri

Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Şirketimiz, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

Kanun'un 28. Maddesine ve Yönetmelik'e uygun olarak; **anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir**. Bu tür işlemeler Kanun ve Yönetmelik kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır. Anonim hale getirilerek işlenen kişisel veriler Kanun ve Yönetmelik kapsamı dışında olacağından Politika'nın 10. Bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler,

anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan

önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan

gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen

bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin

uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki tabloda gösterilmektedir:

Yöntem	Uygulama
Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri	• Değişkenleri Çıkartma • Kayıtları Çıkartma • Bölgesel Gizleme • Genelleştirme • Alt ve Üst Sınır Kodlama • Global Kodlama • Örnekleme
Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme • Tekrar Örnekleme

Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

9.2.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar. Değer düzensizliği sağlamayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır.

a) Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

Yaş	Cinsiyet	Posta Kodu	Gelir	Din
20	**K**	**SO17**	20,000	Budist
38	**E**	**SO18**	22,000	Müslüman
29	**E**	**SO16**	32,000	Hristiyan
31	**K**	**SO17**	31,000	Müslüman
44	**K**	**SO15**	68,000	Yahudi
78	**E**	**SO14**	28,000	Yahudi

Değişkenleri çıkartma örneği

b) Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.

Örneğin organizayon – Departman – bölüm sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

Yaş	Cinsiyet	Doğum Y.	Departman	Bölüm
31	K	İstanbul	Muhasebe	**Genel**
31	E	İstanbul	Muhasebe	**Genel**

31	E	Ankara	Satış	**Perakende**
43	K	Ankara	Satış	**Toptan**
51	E	Eskişehir	Finans	Tahsilat

Kayıtları çıkartma örneği

c) Bölgesel Gizleme

Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

Örneğin alttaki tabloda yaş, cinsiyet ve meslek ayrımına göre Özürlülük durumu görülmektedir. Bu tabloda Yaş=54 olan istisnai bir durum yaratmakta ve tahmin edilebilirlik ve varsayımlar yapılması riskini arttırmaktadır.

Yaş	Cinsiyet	Meslek	Özürlülük Durumu
27	K	Öğretmen	**YOK**
28	E	Mimar	**YOK**
16	E	Öğretmen	**YOK**
30	K	Mali Müşavir	**YOK**
54	K	Mühendis	**1.Derece**
52	K	Mühendis	**Pozitif**

Bölgesel gizleme orjinal veri kümesi

Bu sebeple; bölgesel gizleme yöntemi ile bahsedilen kaydın yaş vemeslek hanesi "bilinmiyor" olarak değiştirilirse ve yeni durum elde edilirse, veri kümesine dair tahmin edilebilirlik riskinde azalma sağlanacaktır.

Yaş	Cinsiyet	Meslek	Özürlülük Durumu
27	K	Öğretmen	**YOK**
28	E	Mimar	**YOK**
16	E	Öğretmen	**YOK**
30	K	Mali Müşavir	**YOK**
Bilinmiyor	K	Bilinmiyor	**1.Derece**
52	K	Mühendis	**Pozitif**

Bölgesel gizleme sonrası dağılım

d) Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkansız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

Örneğin TC Kimlik No 12345678901 olan bir kişi İstanbul Avrupa Yakasında oturuyor ve aynı zamanda . şirketin Anadolu yakasındaki iş yerinde çalışıyor olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak İnsan Kaynakları Platformunda Avrupa Yakasında Oturan çalışanların %xx'i Anadolu Yakasındaki işyerinde çalışıyor şeklinde bir sonuca ulaşılabilir.

e) Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

Aşağıdaki örnekde Tablo 1 orijinal veri kümesini, Tablo 2 ise seçilen değişkenlerin alt ve üst sınır kodlaması yapılarak yeniden tasarlanmış ve anonim hale getirilmiş şeklini göstermektedir.

Yaş	Cinsiyet	Meslek	Yıllık Brüt Ücret	Şehir	Harcamalar (Aylık)
3*	K	Mühendis	92.000	İstanbul	**8.000**
4*	E	Mimar	110.000	İstanbul	**9.600**
4*	E	Doktor	149.000	İstanbul	**10.000**
5*	K	Doktor	123.000	Ankara	**10.800**
5*	E	Doktor	125.000	Ankara	**11.100**
2*	E	Eczacı	85.000	Ankara	**16.300**

Tablo 1 Alt ve üst sınır kodlama orijinal veri kümesi

Tablodaki Gelir ve Harcamalar (Aylık) değişkenlerine ait değerler alt ve üst sınır kodlama yöntemi ile aşağıdaki şekilde değiştirilir;

Gelir (Yıllık): Düşük = 100.000'den küçük ve eşit değerler; Orta = 100.000 ve 120.000 arası değerler; Yüksek = 120.000'den büyük ve eşit değerler,

Harcamalar (Aylık): Düşük = 10.000'den küçük ve eşit değerler;

Orta = 10.000 ve 11.000 arası değerler; Yüksek = 11.000'den yüksek ve eşit değerler,

Bu kodlamaya göre anonim hale getirilmiş tablo aşağıdaki şekli alacaktır.

Yaş	Cinsiyet	Meslek	Yıllık Brüt Ücret	Şehir	Harcamalar (Aylık)
3*	K	Mühendis	Düşük	İstanbul	**Düşük**
4*	E	Mimar	Orta	İstanbul	**Düşük**
4*	E	Doktor	Yüksek	İstanbul	**Orta**
5*	K	Doktor	Yüksek	Ankara	**Orta**
5*	E	Doktor	Yüksek	Ankara	**Yüksek**

2*	E	Eczacı	Düşük	Ankara	**Yüksek**

Tablo 2 Alt ve üst sınır kodlama sonrası anonim hale getirilmiş veri kümesi

f) Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

Aşağıdaki örnekte Tablo 1 orijinal veri kümesini, Tablo 2 ise global kodlama uygulamasından sonraki anonim hale getirilmiş veri kümesini göstermektedir.

Cinsiyet Durum	Meslek	İlçe	Medeni
K	Mimar	Çankaya	**Evli**
K	Mühendis	Çankaya	**Bekar**
K	Mimar	Çankaya	**Boşanmış**
K	Mimar	Çankaya	**Bekar**
K	Mühendis	Çankaya	**Bekar**
K	Mühendis	Çankaya	**Boşanmış**
K	Mühendis	Çankaya	**Evli**

Tablo 1 Global kodlama orijinal veri kümesi

Bu veri kümesinde tek bir ilçedeki kadınların nüfusuna ait verinin meslek değişkeninde iki kategoride yığılma görüldüğünden söz konusu iki kategorinin birleşiminden tek bir kategori elde edilebilir ve bu durumda veri daha güvenli hale getirilmiş olur.

Cinsiyet Durum	Meslek	İlçe	Medeni
K	Mimar veya Mühendis	Çankaya	**Evli**
K	Mimar veya Mühendis	Çankaya	**Bekar**
K	Mimar veya Mühendis	Çankaya	**Boşanmış**
K	Mimar veya Mühendis	Çankaya	**Bekar**
K	Mimar veya Mühendis	Çankaya	**Bekar**
K	Mimar veya Mühendis	Çankaya	**Boşanmış**
K	Mimar veya Mühendis	Çankaya	**Evli**

Tablo 2 Global kodlama sonrası meslek alanı anonim hale getirilmiş veri kümesi

g) Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin

üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır.

Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir.

Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

9.2.3.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır.

a) Mikro Birleştirme

Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

Aşağıdaki Tablo 1'deki kayıtlar "Gelir" sütunundaki değerlerine göre birbirine yakın olan üçerli gruplara ayrılmış ve gruplar renk kodlarıyla işaretlenmiştir. Her grup, içindeki değerlerin aritmetik ortalaması alınmış ve gruptaki tüm kayıtlara, bulunan yeni değerler atanarak orijinal değeri tespit edebilmek engellenmiştir.

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	**25.000**
37	K	1559	**28.000**
41	E	1559	**37.000**
25	K	1557	**49.000**
34	E	1558	**56.000**
48	E	1556	**60.000**

Tablo 1 Mikro birleştirme orjinal veri kümesi

Grup 1 için mikro birleştirme sonucunda yeni değer : (25.000 + 28.000 + 37.000) / 3 = 30.000

Grup 2 için mikro birleştirme sonucunda yeni değer : (49.000 + 56.000 + 60.000) / 3 = 55.000

Yaş	Cinsiyet	Posta Kodu	Gelir
23	K	1556	**30.000**
37	K	1559	**30.000**
41	E	1559	**30.000**
25	K	1557	**55.000**
34	E	1558	**55.000**
48	E	1556	**55.000**

Tablo 2 Mikro birleştirme sonucu elde edilen yeni veri kümesi

b) Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

Yaş	Cinsiyet	İl	Gelir
21	K	İstanbul	**20.000**
24	K	Ankara	**30.000**
35	E	İzmir	**30.000**
36	K	İstanbul	**25.000**
45	E	İzmir	**55.000**
50	E	İzmir	**15.000**

Tablo1 Veri değiş tokuşu orjinal veri kümesi

Tablo 1 orijinal değerleri içeren kayıtlara sahiptir. Tablo 2'de veri değiş tokuşu işlemi sonucunda elde edilen yeni veri kümesini içermektedir. Söz konusu tablodan görüleceği üzere Yaş="24", Cinsiyet="K", İl="Ankara" olan kayda ait gelir bilgisi ile Yaş="45", Cinsiyet="E", İl="İzmir" olan kaydın gelir bilgisi birbirleriyle değiştirilmiştir. Aynı şekilde Yaş="35", Cinsiyet="E", İl="İzmir" olan kayda ait gelir bilgisi ile Yaş="50", Cinsiyet="E", İl="İzmir" olan kayıtların gelir bilgisi birbirleriyle değiştirilmiş ve yeni veri kümesi oluşturulmuştur.

Yaş	Cinsiyet	İl	Gelir
21	K	İstanbul	**25.000**
24	K	Ankara	**55.000**
35	E	İzmir	**15.000**
36	K	İstanbul	**20.000**
45	E	İzmir	**30.000**
50	E	İzmir	**30.000**

Tablo 2 Veri değiş tokuşu sonucu elde edilen yeni veri kümesi

c) Gürültü Ekleme

Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	**45.000**
24	K	Ankara	**20.000**
35	E	Ankara	**123.000**
36	K	Ankara	**18.000**
45	E	İstanbul	**75.000**
50	E	İstanbul	**7.000**

Tablo 1 Gürültü ekleme orjinal veri kümesi

Tablo 1'deki gelir değişkenleri için her bir kaydın değerlerine -5.000 işlemi uygulanmış ve Tablo 2'deki yeni değişkenler oluşmuştur.

Yaş	Cinsiyet	İl	Gelir
21	K	İzmir	**40.000**
24	K	Ankara	**15.000**
35	E	Ankara	**118.000**
36	K	Ankara	**13.000**
45	E	İstanbul	**70.000**
50	E	İstanbul	**2.000**

Tablo 2 Gürültü ekleme sonucu elde edilen veri kümesi

9.3. Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir.

Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

a) K-Anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir.

K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak,

belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır. Örneğin; Tablo 1'de ad-soyad, doğum tarihi, cinsiyet, okul ve posta kodu gibi değişkenler vardır.

Ad Soyad	Doğum Tarihi	Cinsiyet	Posta Kodu	Okul
*	1983	E	3440*	**İTÜ**
*	1982	E	3440*	**ODTÜ**
*	1983	E	3440*	**ODTÜ**
*	1980	E	3440*	**ODTÜ**
*	1982	K	3440*	**İstanbul Üniversitesi**
*	1983	E	3440*	**Bursa Uludağ**
*	1983	E	3440*	**Yıldız Üniversitesi**
*	1980	K	3440*	**Bilgi Üniversitesi**
*	1983	E	3440*	**Bilgi Üniversitesi**

Tablo 1. K-Anonimlik orjinal veri kümesi

Tabloda ad-soyad ve posta kodu değişkenlerine dair değerlerde maskeleme uygulanarak veri anonim hale getirilmiş olmakla birlikte, böyle bir anonimleştirme yapılırken aynı değerleri içeren sadece bir kayıt varsa bu kayıtla doğru kişiyi tespit mümkün olacaktır. Ancak kayıtların çoklanması halinde, tekillik yaratabilecek değişkenlere dair belli bir çeşitlilik sağlanmış olacaktır. Örneğin; Tablo 1 ' de 1983 yılında doğmuş, cinsiyeti erkek ve posta kodu 3440 ile başlayan 6 adet kayıt için "Okul" alanında altı ayrı okul çeşitliliği sağlanmış olduğundan 1983 yılında doğmuş cinsiyeti erkek olan ve posta kodu 3440 ile başlayan bir kişinin bu 6 okuldan hangisine sahip olduğuna dair tahmin yürütmek mümkün değildir.

Bu nedenle, Tablo 2'de olduğu gibi çerçeve içerisinde yer alan doğum tarihi, cinsiyet ve posta kodu verileri aynı değerleri içeren kayıtların açıklanması ya da paylaşılması halinde 1983 yılında doğmuş cinsiyeti erkek olan ve posta kodu 3440 ile başlayan bir kişinin bu 6 okuldan hangisine sahip olduğuna dair tahmin yürütmek mümkün değildir.

Ad Soyad	Doğum Tarihi	Cinsiyet	Posta Kodu	Okul
*	1980	K	3440*	**ODTÜ**
*	1982	E	3440*	**ODTÜ**
*	1980	K	3440*	**Bilgi Üniversitesi**
*	1982	E	3440*	**İstanbul**

				Üniversitesi
*	1983	E	3440*	**İTÜ**
*	1983	E	3440*	**ODTÜ**
*	1983	E	3440*	**Bursa Uludağ**
*	1983	E	3440*	**Yıldız Üniversitesi**
*	1983	E	3440*	**Bilgi Üniversitesi**

Tablo 2. K-Anonimlik uygulanmış veri kümesi

b) L-Çeşitlilik

K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır. Tablo 1'de, şirkette çalışmakta olan kişilere ait departman bilgisi verilirken bu kişilerin ad soyad veya kimlik numarası verilmeyerek K-anonimlik uygulanmış olmakla birlikte posta kodu, yaş ve etnik köken bilgisi paylaşılmış olduğundan tespit edilebilme ihtimali bulunmaktadır.

Posta Kodu	Yaş	Uyruk	Departman
13053	28	Rus	**Üretim**
13068	29	Amerikalı	**Üretim**
13068	21	Çinli	**Muhasebe**
13053	23	Amerikalı	**Muhasebe**
14853	50	İngiliz	**Dış Ticaret**
14853	55	Rus	**Dış Ticaret**
14850	47	Amerikalı	**Dış Ticaret**
14850	49	Amerikalı	**Dış Ticaret**
13053	31	Amerikalı	**Kalite Kontrol**
13053	37	İngiliz	**Kalite Kontrol**
13068	36	Japon	**Kalite Kontrol**
13068	35	Amerikalı	**Kalite Kontrol**

Tablo 1. L-Çeşitlilik orjinal veri kümesi

Posta Kodu	Yaş	Uyruk	Departman
130**	< 30	*	**Üretim**
130**	< 30	*	**Üretim**
130**	< 30	*	**Muhasebe**
130**	< 30	*	**Muhasebe**
1485*	≥ 40	*	**Dış Ticaret**
1485*	≥ 40	*	**Dış Ticaret**
1485*	≥ 40	*	**Dış Ticaret**
1485*	≥ 40	*	**Dış Ticaret**

130**	3*	*	**Kalite Kontrol**
130**	3*	*	**Kalite Kontrol**
130**	3*	*	**Kalite Kontrol**
130**	**3***	*	**Kalite Kontrol**

Tablo 2. K=4 Anonimleştirme uygulanması sonucu elde edilen veri kümesi

Tablo 2'den görüleceği üzere, Tablo 1'de yer alan bilgiler maskeleme mantığı (posta kodu ve yaş bilgisinden maskelemeyle 4'erli gruplar yaratılmıştır) içerisinde gruplanarak öncelikle K=4 anonimlik yöntemiyle anonimliği kuvvetlendirilmiştir.

Ancak ilk işlem sonucunda tablodan görüleceği gibi son 4 kayıttaki grupta tüm "Departman" değerleri "Dış Ticaret" olarak gruplanmıştır. Bu durum posta kodu 130 ile başlayan 30'lu yaşlardaki herkesin uyruğundan bağımsız olarak "Dış Ticaret" departmanında çalıştığı bilgisini paylaşmaktadır.

Bu iki bilgiye sahip olan bir kullanıcı, tanıdığı bu özellikte bir kişinin dış ticaret departmanın olduğu sonucuna kolaylıkla varabilecektir. Bu nedenle her bir grubun içinde belli bir çeşitlilik yaratılmasına dikkat edilerek maskeleme yöntemi kullanılmalıdır.

Tablo 3'de, aşağıdaki şekilde gruplanarak anonimleştirilmiş bir veri kümesinde K=4 olacak şekilde gruplar oluşturulmuştur ve aynı zamanda her bir grubun içinde de L=3 olacak şekilde (yani en az 3 çeşit departman tutturularak) çeşitlilik elde edilmiştir.

Her grubun içinde 4 kayıt ve 3 farklı çeşit departman yer alması sağlanarak anonimleştirme yapılmıştır. Bu işlem anonimleştirme işlemini kuvvetlendirmiş, dış bilgiye sahip kullanıcının tahmin gücünü azaltmıştır.

Posta Kodu	Yaş	Uyruk	Departman
1305*	≤ 40	*	**Üretim**
1305*	≤ 40	*	**Üretim**
1305*	≤ 40	*	**Muhasebe**
1305*	≤ 40	*	**Muhasebe**
1485*	> 40	*	**Dış Ticaret**
1485*	> 40	*	**Dış Ticaret**
1485*	> 40	*	**Dış Ticaret**
1485*	> 40	*	**Gümrük**
1306*	≤ 40	*	**Kalite Kontrol**
1306*	≤ 40	*	**Kalite Kontrol**
1306*	≤ 40	*	**Kalite Kontrol**
1306*	≤ 40	*	**Kalite Kontrol**

Tablo 3. K=4 Anonimlik ve L=3 Çeşitlilik uygulanması sonucu elde edilen veri kümesi

c) T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır.

Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

Tablo 1'de; doğum tarihi, cinsiyet ve posta kodu alanlarına göre K=3 olacak şeklinde K-anonimlik ve L=3 olacak şekilde L-çeşitlilik sağlanmasına rağmen 197O yılında doğmuş, 3440* adresinde oturan ve cinsiyeti erkek olan bir kişinin departmanı, Muhasebe, Finans, Kalite, Lojistik, İnsan Kaynakları, Yönetim olduğu için, bu grupta söz konusu kişinin departmaının ne olduğu tahmin edilebilir.

Doğum Tarihi	Cinsiyet	Posta Kodu	Departman	Çalışan Sayısı
198*	E	3440*	Muhasebe	80
198*	E	3440*	Kalite	20
198*	E	3440*	Finans	70
197*	E	3440*	Lojistik	10
197*	E	3440*	İnsan Kaynakları	10
197*	E	3440*	Yönetim	10

Tablo 1. K=3 Anonimlik ve L=3 Çeşitlilik uygulanmış veri kümesi

Bu tahmin gücünü azaltabilmek için de anonimleştirme içindeki gruplamalarda Tablo 2' de görülebileceği üzere öyle bir düzenleme yapılmıştır ki üçerli kayıtlardan oluşan gruplarda (K=3) en az 3 farklı (L=3) departman tipi olacak şekilde ayarlanmış ancak bir araya gelen bu 3 farklı departmanında da hepsinin operasyonel departman olmaması sağlanarak (diğer kısımların operasyonel olmadığı varsayımıyla) o gruptaki çalışanlara dair tahminler azaltılmıştır.

Doğum Tarihi	Cinsiyet	Posta Kodu	Departman	Çalışan Sayısı
≥ 1970	E	3440*	Muhasebe	80
≥ 1970	E	3440*	Kalite	20
≥ 1970	E	3440*	Finans	70
1975 ≤ x ≤1985	E	3440*	Lojistik	10
1975 ≤ x ≤1985	E	3440*	İnsan Kaynakları	10
1975 ≤ x ≤1985	E	3440*	Yönetim	10

Tablo 2. T-Yakınlık sonucu elde edilen veri kümesi

9.4. KİŞİSEL VERİLERİN SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİNE VE GÖREV TANIMLARI

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 6. Maddesinin (f) bendi uyarınca kişisel verileri saklama ve imha süreçlerinde yer alanların

unvanlarının, birimlerinin ve görev tanımlarının gösterildiği Yetki Matriksi, Politika'da EK-1 olarak yer almaktadır.

9.5. KİŞİSEL VERİLERİN PERİYODİK İMHA SÜRELERİ

Veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

Genel kural bu olmakla birlikte Şirketimiz altı ayda bir gerekli periyodik imhayı gerçekleştirmektedir.

9.6. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI; BU HAKLARIN KULLANILMASI VE DEĞERLENDİRİLMESİ METODOLOJİSİ

Şirketimiz, Kanun'un 10. maddesine uygun olarak kişisel veri sahibinin haklarını kendisine bildirmekte, bu hakların nasıl kullanılacağı konusunda kişisel veri sahibine yol göstermektedir ve Şirketimiz, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gereken bilgilendirmenin yapılması için Kanun'un 13. maddesine uygun olarak gerekli kanalları, iç işleyişi, idari ve teknik düzenlemeleri yürütmektedir.

10. VERİ SAHİBİNİN HAKLARI VE BU HAKLARINI KULLANMASI

10.1. Kişisel Veri Sahibinin Hakları

Kişisel veri sahipleri aşağıda yer alan haklara sahiptirler:

(1) Kişisel veri işlenip işlenmediğini öğrenme,

(2) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

(3) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

(4) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

(5) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

(6) Kanun, Yönetmelik ve ilgili hükümlere uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

(7) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

(8) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

10.2. Kişisel Veri Sahibinin Haklarını İleri Süremeyeceği Haller

Kişisel veri sahipleri, Kanun'un 28. maddesi gereğince aşağıdaki haller Kanun kapsamı dışında tutulduğundan, kişisel veri sahiplerinin bu konularda 10.01 'de sayılan haklarını ileri süremezler:

(1) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

(2) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

(3) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

(4) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

Kanun'un 28/2 maddesi gereğince; aşağıda sıralanan hallerde kişisel veri sahipleri zararın giderilmesini talep etme hakkı hariç, 10.1.1.'de sayılan diğer haklarını ileri süremezler:

(1) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

(2) Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

(3) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

(4) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

10.3. Kişisel Veri Sahibinin Haklarını Kullanması

Kişisel veri sahipleri bu bölümün 10.01 Başlığı altında sıralanan haklarına ilişkin taleplerini, www.cottgroup.com adresinde iletişim bilgilerini kullanarak ıslak imzalı veya güvenli elektronik imzalı belgeyi göndererek Şirkete iletebileceklerdir.

Kişisel veri sahipleri adına üçüncü kişiler tarafından talepte bulunulması mümkün değildir.

Kişisel veri sahibinin kendisi dışında bir kişinin talepte bulunması için konuya ilişkin olarak kişisel veri sahibi tarafından başvuruda bulunacak kişi adına düzenlenmiş özel vekâletname bulunmalıdır.

10.4. Kişisel Veri Sahibinin KVK Kurulu'na Şikâyette Bulunma Hakkı

Kişisel veri sahibi Kanun'un 14. maddesi gereğince başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; Şirketimizin cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde KVK Kurulu'na şikâyette bulunabilir.

10.5. ŞİRKET'İN BAŞVURULARA CEVAP VERMESİ

10.5.1. Şirketimizin Başvurulara Cevap Verme Usulü ve Süresi

Kişisel veri sahibinin, bu bölümün 10.1.3. başlıklı kısmında yer alan usule uygun olarak talebini Şirketimize iletmesi durumunda Şirketimiz talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ilgili talebi ücretsiz olarak sonuçlandıracaktır.

Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Şirketimiz tarafından başvuru sahibinden KVK Kurulunca belirlenen tarifedeki ücret alınacaktır.

10.5.2. Şirketimizin Başvuruda Bulunan Kişisel Veri Sahibinden Talep Edebileceği Bilgiler

Şirketimiz, başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir.

Şirketimiz, kişisel veri sahibinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

10.5.3. Şirketimizin, Kişisel Veri Sahibinin Başvurusunu Reddetme Hakkı

Şirketimiz aşağıda yer alan hallerde başvuruda bulunan kişinin başvurusunu, gerekçesini açıklayarak reddedebilir:

(1) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

(2) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

(3) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

(4) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

(5) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

(6) Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

(7) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

(8) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

(9) Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması

(10) Orantısız çaba gerektiren taleplerde bulunulmuş olması.

(11) Talep edilen bilginin kamuya açık bir bilgi olması.

10.6. ŞİRKET KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASININ DİĞER POLİTİKALARLA OLAN İLİŞKİSİ VE YASAL UYUMLULUK

Şirketin işbu Politika ile ortaya koymuş olduğu esasların ilişkili olduğu Kişisel verilerin korunması ve işlenmesi konusunda kaleme alınmış temel politikalar aşağıda belirtilmektedir. Bu politikaların Şirketin diğer alanlarda yürüttüğü temel politikalarla da bağı kurularak, Şirketin benzer amaçlarla farklı politika esaslarıyla işlettiği süreçler arasında harmonizasyon da sağlanmaktadır.

Aşağıdaki tabloda belirtilen politikaların bir kısmı Şirket içi kullanıma yöneliktir. Şirket içi politikalarının esasları ilgili olduğu ölçüde kamuoyuna açık Politikalara yansıtılarak, ilgililerinin bu çerçevede bilgilenmesi ve Şirketin yürütmüş olduğu kişisel veri işleme faaliyetleri hakkında şeffaflık ve hesap verilebilirliğin sağlanması hedeflenmiştir.

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk ve farklılıklar olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanır.

Boss Yönetişim Hizmetleri A.Ş. tarafından hazırlanan işbu Politika 29.12.2017 tarihinde yürürlüğe girmiştir.

Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir. Güncelleme tablosu işbu sözleşmeye eklenmiştir.

İLGİLİ POLİTİKA VE PROSEDÜRLER		
Bilgi Güvenlik Sistemi El Kitabı	PL.01 E - POSTA GÜVENLİĞİ POLİTİKASI	PL.02 ŞİFRE GÜVENLİĞİ POLİTİKASI
PL.03 ANTİVİRÜS POLİTİKASI	PL.04 İNTERNET ERİŞİM POLİTİKASI	PL.05 BİLGİ SİSTEMLERİ YEDEKLEME POLİTİKASI
PL.06 KABLOSUZ İLETİŞİM POLİTİKASI	PL.07 KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI	PL.08 PERSONEL GÜVENLİK POLİTİKASI
PL.09 UZAKTAN ERİŞİM POLİTİKASI	PL.10 TEMİZ MASA TEMİZ EKRAN POLİTİKASI	PL.11 ZİYARETÇİ KABUL POLİTİKASI
PL.12 TAŞINABİLİR CİHAZ POLİTİKASI	PL.13 DEĞİŞİM YÖNETİMİ POLİTİKASI	PL.14 SUNUCU GÜVENLİĞİ POLİTİKASI
PL.15 KÖTÜ KODLARDAN VE SALDIRILARDAN KORUNMA POLİTİKASI	PL.16 TASİNABİLİR-ORTAMİN-İMHASİ-POLİTİKASİ	PL.17 TECHİZATIN ELDEN ÇIKARILMASI POLİTİKASİ
PL.18 AĞ ERİŞİM POLİTİKASI	PL.19 BİLGİ VE YAZILIM ALIŞVERİŞİ POLİTİKASI	PL.20 ERİŞİM POLTİKASI
PL.21 FİZİKSEL GÜVENLİK POLİTİKASI	PL.22 İNTERNET KULLANIM POLİTİKASI	PL.23 LAPTOP KULLANIM POLİTİKASI
PL.24 AĞA UZAKTAN BAĞLANTI POLİTİKASI	PL.25 ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI	PL.26 VARLIKLARA YÖNELİK SORUMLULUK POLİTİKASI

PL.27 YAZILIM GELİŞTİRME GÜVENLİĞİ POLİTİKASI	PL.28 ZARARLI YAZILIMLARA KARŞI KORUNMA POLİTİKASI	PL.29 BASILI ÇIKTI VE DAĞITIM POLİTİKASI
PL.30 BİLGİ KORUMA POLİTİKASI	PL.31 GÜVENLİK BİLİNCİ POLİTİKASI	PL.32 KABUL EDİLEBİLİR KULLANIM POLİTİKASI
PL.33 PAROLA KORUMA POLİTİKASI	PL.34 BİLGİ SINIFLANDIRMA VE ETİKETLEME POLİTİKASI	P08 İNSAN KAYNAKLARI PROSEDÜRÜ.
P09 RİSK YÖNETİM PROSEDÜRÜ	P10 ÖLÇÜM VE KONTROL YÖNTEMLERİNİ BELİRLEME PROSEDÜRÜ	P11 İŞ SÜREKLİLİĞİ VE ACİL DURUM YÖNETİMİ PROSEDÜRÜ
P12 KULLANICI HESABI YÖNETİMİ PROSEDÜRÜ	P13 CİHAZ VE MEDYA KONTROLÜ PROSEDÜRÜ.	P14 E-POSTA GÜVENLİĞİ PROSEDÜRÜ
P15 MÜŞTERİ ŞİKAYETLERİ YÖNETİMİ PROSEDÜRÜ	P16 DİSİPLİN PROSEDÜRÜ	P17 OLAY İHLAL PROSEDÜRÜ
P18 TEÇHİZAT TAKİP PROSEDÜRÜ	P19 SİSTEM ODASI KULLANMA PROSEDÜRÜ.	P20 İLETİŞİM PROSEDÜRÜ
T1001 ANTİVİRÜS TALİMATI	T1002 VPN GÜVENLİĞİ TALİMATI	T1003 YAMA GÜVENLİĞİ TALİMATI
T101 Yedek Alma Talimatı	T1101 BİLGİ GÜVENLİĞİ TESTLERİ UYGULAMA TALİMATI	T1201 AKTİF DİZİN GÜVENLİĞİ TALİMATI
T1301 YÜKLEME VE KURULUM TALİMATI	T1901 SUNUCU BAKIM TALİMATI.	T801 KURUM KULTURU TALIMAT
T802_MAAŞ VE İŞ AVANSI TALİMATI	T803 İŞGÜCÜ YEDEKLEME TALİMATI	TL 2701_ GÜVENLİ GELİŞTİRME ORTAMI TALİMATI
TL 2702_ GÜVENLİ SİSTEM MÜHENDİSLİĞİ TALİMATI	DRP_FELAKET YÖNETİM PLANI	DRP- SENARYOLARI
F11.01- İŞ SÜREKLİLİĞİ VE ACİL EYLEM PLANI	F11.02-ACİL DURUM GENEL KORUNMA PLANI	F11.03 -ARANACAKLAR LİSTESİ
F9.01-VARLIK ÜSTLENME BEYANI ve BİLGİ GÜVENLİĞİ SORUMLULUKLARININ TAHSİSİ	F9.02-ARTIK RİSK ONAYI	İŞ ETKİ ANALİZİ
YETKİ MATRİSLERİ		

EK - 1

PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ

PERSONEL / DANIŞMAN	GÖREV	SORUMLULUK
Bilgi İşlem Müdürü	**Bilgi Teknolojileri Departmanı** Kişisel veri saklama ve imha politikası uygulanması. Silme, yoketme, anonimleştirme tekniklerinin geliştirilmesi. Gerekli yazılım ve veri saklama ortamlarının politikanın uygulanmasına elverişli şekillerde hazır tutulması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi ve konuyla ilgili uygulamaları geliştirmek, araştırma ve iyileştirmeler yapmak.
Bilgi İşlem Destek Uzmanı	**Bilgi Teknolojileri Departmanı** Kişisel veri saklama ve imha politikası uygulanması. Silme, yoketme, anonimleştirme işlemlerinin yapılması. Gerekli kayıtların tutulması. Sistemlerin politikalar doğrultusunda hazır ve elverişli olarak tutulması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin yürütülmesi. Kayıtların yönetime düzenli olarak raporlanması.

Operasyon Müdürleri	**Operasyon Departmanı** Kişisel veri saklama ve imha politikası uygulanması. İmha sürelerinin takibi ve Bilgi İşlem ile koordinasyon halinde gereken kayıtların imhasının sağlanması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin takibi, yürütülmesi. Eksikliklerin ve iyileştirme gereken alanların yönetime raporlanması
İnsan Kaynakları Müdürü	**İnsan Kaynakları Departmanı** Kişisel veri saklama ve imha politikası uygulanması. Personel ile ilgili bilgi, belge, dokümanların imha sürelerinin takibi ve Bilgi İşlem ile koordinasyon halinde gereken kayıtların imhasının sağlanması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin takibi, yürütülmesi. Eksikliklerin ve iyileştirme gereken alanların yönetime raporlanması. Log kayıtlarının bir kopyasının tutulması.
Muhasebe Müdürleri	**Muhasebe Departmanı** Kişisel veri saklama ve imha politikası uygulanması. İmha sürelerinin takibi ve Bilgi İşlem ile koordinasyon halinde gereken kayıtların imhasının sağlanması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin takibi, yürütülmesi. Eksikliklerin ve iyileştirme gereken alanların yönetime raporlanması
Finans Müdürleri	**Finans Departmanı** Kişisel veri saklama ve imha politikası uygulanması. Tedarikçiler ile yapılan sözleşmelerin KVKK kapsamında değerlendirilmesi ve yönetimi. İmha sürelerinin takibi ve Bilgi İşlem ile koordinasyon halinde gereken kayıtların imhasının sağlanması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin takibi, yürütülmesi. Eksikliklerin ve iyileştirme gereken alanların yönetime raporlanması
İş Geliştirme ve Müşteri İlişkileri Müdürleri ve Danışmanlar	**Müşteri İlişkileri Departmanı** Kişisel veri saklama ve imha politikası uygulanması. Müşterilerin konu ile ilgili	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha

	aydınlatılması. Sözleşme ve protokollerin KVKK kanunu kapsamında hazırlanmasının sağlanması. İmha sürelerinin takibi ve Bilgi İşlem ile koordinasyon halinde gereken kayıtların imhasının sağlanması.	süreçlerinin takibi, yürütülmesi. Eksikliklerin ve iyileştirme gereken alanların yönetime raporlanması
Yönetici Ortaklar	Kişisel veri saklama ve imha politikası uygulanması.	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha süreçlerinin yönetilmesi ve denetimi. Bu alandaki gerekli yatırımların ve envanterlerin takibi. Logların izlenmesi.
Avukat	KVKK kapsamında Kişisel veri saklama ve imha politikası'nın göncellenmesinin sağlanması.	Mevzuat ve uygulamalar konusunda bilgilendirme ve danışmanlık. Sözleşmelerin hazırlanması.

EK - 2

Şirketimiz tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde işlem ve süreç bazında tespit edilmiş olup, ilgili Envanter'e [----------] linki üzerinden erişilebilecektir.

İşlem / Süreç	Yasal Saklama Süresi	İmha Süresi
Şirket Personeli Bordro İşlemleri ve Bordrolama	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşterilere ait çalışanların bordro, özlük ve hizmete ilişkin bilimu kayıtlar	Türk Borçlar Kanunu ve sair mevzuat çerçevesinde genel hukuki sorumluluk süresi kadar söz konusu kişisel veriler saklanacak ve işlenecek olup, akabinde 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile sair mevzuata	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşterilere ait çalışma iznine esas teşkil eden kayıtlar		Saklama süresinin bitimini takiben 180 gün içerisinde

	uygun bir şekilde kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde resen veyahut ilgili kişinin talebi üzerine söz konusu veriler silinecek, yok edilecek veyahut anonim hale getirilecektir. Saklama Süresi 10 yıldır	
Genel Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İhale/işyeri açma/bakanlıklarmüsteşarlıklar evrak hazırlama süreçleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel Kayıtlarının Active Directory ve diğer sistemlerde muhasfazası	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ödeme ve benzeri finans işlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Eğitim Kayıtları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri / Tedariki cari hesap kayıtları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Toplantı notları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Active Directory kayıtları ve gerekli Log kayıtları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kamera ve İzleme Kayıtları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

EK - 3

Firma	Adres	Vergi dairesi	Vergi Numarası	Ticaret Sicil No	Mersis No
Boss Yönetişim Hizmetleri A.Ş. Yönetim Ofisi www.boss.com.tr	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli /	Zincirlikuyu	1800379183	555770	0180037918300011

	İstanbul / Türkiye				
İstanbul Uluslararası Denetim ve SMMM Ltd. Şti. www.istanbulcpa.com	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	4810544399	673098	0481054439900018
Netkey Bilişim Sistemleri San. Ve Tic. Ltd. Şti. www.netkeysoftware.com	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	6310446636	551045	0631044663600010
Pera Kariyer Çözümleri Danışmanlık Ltd. Şti. www.perakariyer.com	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	7390463365	596859	0739046336500017
UP İnsan Kaynakları Eğitim ve Yönetim Dan.Hiz.Tic.Ltd.Şti. www.upandlearn.com	Demircikara Mahallesi 1419 Sokak B Blok Apt. No:1 B/7 Muratpaşa / Antalya / Türkiye	Antalya Kurumlar	8930275247	745547	0893027524700018

EDI Global Danışmanlık Tercüme ve Çeviri Hiz. Ltd. Şti. www.ediglobal.com.tr	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	4640563770	810405	0464056377000013
Ikon Informatics Consultancy Ltd	Sofia 1309, Vazrazhdane District, 70 Tzaribrodska Str, fl. 2, office 3	Bulgaristan	BG201052169	N/A	N/A