Arkas Turizm Çerez Politikası

ARKAS TURİZM SEYAHAT ACENTASI A.Ş. (veri sorumlusu) olarak, kullanıcılarımızın internet (web) hizmetlerimizden güvenli ve eksiksiz şekilde yararlanmalarını sağlamak, kullanıcının uygulama ara yüzünde özelleştirebildiği tercihlerini depolamak ve kullanıcı deneyimini geliştirmek, istatistik bilgilerini derlemek ve ziyaretçilerimizin gizliliğini korumak için çeşitli çerez veri dosyaları kullanıyoruz. Veri sorumlusu sıfatıyla, çerezler vasıtasıyla kişisel veriler toplanmaktadır.

İnternet sayfamızı ziyaret ederek çerezlerin, bu İnternet Sitesi çerez Politikası ile uyumlu bir şekilde çalışmasına onay vermiş olursunuz. Sitemizde çerezlerin devre dışı bırakılmasını istiyorsanız, tarayıcınızın ayarlarında düzenleme yapabilirsiniz. Bununla birlikte tarayıcı çerezlerin kullanılmaması web sitemizdeki kullanıcı deneyiminizi etkileyebilir. Kalıcı veya oturum çerezlerinin kullanılmaması durumunda internet sitemizi bazı bileşenleri eksik olacak şekilde, sınırlı erişim olanaklarıyla görüntülemeye devam edebilirsiniz. İnternet sitemizden ve uygulamadan tam anlamıyla yararlanmak için çerezlere izin vermenizi öneririz.

Veri sorumlusu, 6698 sayılı Kişisel Verileri Koruma Kanunuşnun (Kanun) 5/2. maddesinde belirtilen şartları (hukuki sebepler) karşılamak şartıyla veya veri sahibinin açık rızası ile çerezler vasıtasıyla toplanan kişisel verileri işleyebilir.

Veri sorumlusu olarak, web sitemizde ve uygulamalarımızda kullandığımız çerezleri yürürlükten kaldırabilir, türlerini veya işlevlerini değiştirebiliriz. Aydınlatma metnimiz üzerinde yapılan olan her türlü güncelleme web sitemizde ve web uygulamalarımızda yayınlanmasıyla birlikte yürürlük kazanacaktır.

Web sitelerimizde ve uygulamalarımızda ne tür çerezler kullanıyoruz?

- *Oturum çerezleri* : üyelerimizin kullanıcı girişi aşamasında, şifrelerini sık sık yeniden girmelerini önlemek amacıyla kullanılmaktadır. Oturum çerezleri belirli bir süre için uygulama ve site için serbest dolaşım hakkı sağlarlar.
- *Görsel Tercih çerezleri* : üye davranış ve seçimlerine göre kişiselleştirilmiş içerik ve deneyim sunmak amacıyla kullanılırlar.
- *İstatistik çerezleri* : üyelerimizin ve konuklarımızın kullanım alışkanlıklarını analiz etmek ve uygulama istatistiklerini belirlemek için kullanılırlar.

Veri sahibi olarak sizin haklarınız nelerdir?

Kanun'a göre veri sahiplerinin,

- Kişisel veri işlenip işlenmediğini öğrenme,
- İşlendiği bildirilen kişisel verilerinize ilişkin bilgi talep etme,
- İşlenme amacını ve verilerin amacına uygun kullanılıp kullanılmadığını öğrenme,
- Eksik veya yanlış işlenmiş verilerin düzeltilmesini isteme ve kişisel verilerin aktarıldığı kişiler var ise bu kapsamda yapılan işlemlerin de bu kişilere bildirilmesini isteme,
- Yurt içinde ve yurt dışında kişisel verilerin varsa aktarıldığı üçüncü kişileri öğrenme,

- Toplanan verilerin silinmesini veya yok edilmesini talep etme ve kişisel verilerin aktarıldığı kişiler var ise bu kapsamda yapılan işlemlerin de bu kişilere bildirilmesini isteme,
- Yasaya aykırı işlenmiş veriler dolayısıyla oluşabilecek zararların giderilmesini talep etme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakları bulunmaktadır.

Bu haklarınıza ilişkin taleplerinizi, Kanun'un 11 inci maddesinde belirtilen haklar kapsamında yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletebilirsiniz. Ayrıca, veri sorumlusunun www.arkasturizm.com adlı web sitesinde yer alan "Başvuru Formu" ile tarafımıza iletebilirsiniz. Başvurularınız en kısa sürede ve tebliğ tarihinden itibaren en geç 30 (otuz) gün içerisinde değerlendirilerek sonuçlandırılacaktır.

Taleplere ilişkin olarak herhangi bir ücret talep edilmemesi esas olmakla birlikte veri sorumlusunun Kişisel Verileri Koruma Kurulşu tarafından belirlenen ücret tarifesi üzerinden ücret talep etme hakkı saklıdır.

Kişisel Verilen Korunması Aydınlatma Metni

VERİ SORUMLUSU: ARKAS TURİZM SEYAHAT ACENTASI A.Ş. çınarlı Mah. Ankara Asfaltı Cad. No:15/101 Konak, İzmir

ARKAS TURİZM SEYAHAT ACENTASI A.Ş. (Veri Sorumlusu) tarafından aşağıdaki kişisel verileriniz işlenmekte, saklanmakta ve korunmaktadır;

- **Kimlik Bilgileriniz:** Adınız soyadınız, anne-baba adınız, doğum tarihiniz, doğum yeriniz, cinsiyetiniz, uyruğunuz, TC kimlik numaranız, kimlik bilgileriniz, varsa kimlik fotokopiniz suretiyle elde edilen kan grubu ve din hanesi bilgisi, imza yetkilisi olup olmadığınız bilgisi, fotoğrafınız.
- **İletişim Bilgileriniz:** Adresiniz, telefon numaranız, e-posta adresiniz, varsa KEP adresiniz.
- **Müşteri Bilgileriniz:** Müşteri işlem bilgileriniz, imzanız, çalıştığınız şirket bilgileriniz, vergi bilgileriniz, banka hesabınıza ilişkin bilgiler, mesleki deneyim bilgileriniz, meslek, görev ve unvan bilgileriniz, araç bilgileriniz, hukuki işlemler kapsamında elde edilen bilgileriniz, vergi numaranız, talimat, talep ve şikayetlerinize ilişkin bilgiler, ürün ve hizmetlerimize ilişkin tercih ve alışkanlıklarınız.
- **İşlem Güvenliği Bilgileriniz:** MAC adresiniz, log kayıtlarınız.
- **Görsel ve İşitsel Bilgileriniz:** Fotoğraflarınız ve kamera kayıtlarınız.

Bu nedenle, 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında Veri Sorumlusu sıfatıyla sizleri aydınlatmak isteriz.

1. **Kişisel Verileri Toplama Yöntemi ve Hukuki Sebebi**

Kişisel verileriniz; bu aydınlatma metninde belirtilen amaç ve kapsamda, fiziki ve elektronik ortamlarda toplanan "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" ifade etmektedir.

Kişisel verileriniz, Kanun'un 5. Maddesinde belirtilen "kanunlarda açıkça öngörülmesi", "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması", "kişisel veri işlemenin veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması", "kişisel veri işlemenin bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" ve "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hukuki sebeplerine dayalı olarak işlenmektedir.

Belirtilen hukuki sebeplerden en az birisinin bulunmaması halinde, kişisel veri işlemeye ilişkin açık rızanız sorulacaktır. Açık rızanızın sorulduğu halleri "Açık Rıza Formunda" bulabilirsiniz.

1. **Kişisel Verilerin İşlenme Amaçları**

Toplanan kişisel verileriniz;

Acil durum yönetimi süreçlerinin yürütülmesi,

Bilgi güvenliği süreçlerinin yürütülmesi,

Denetim/etik faaliyetlerinin yürütülmesi,

Erişim yetkilerinin yürütülmesi,

Faaliyetlerin mevzuata uygun yürütülmesi,

Finans ve muhasebe işlerinin yürütülmesi,

Firma/ürün/hizmetlere bağlılık süreçlerinin yürütülmesi,

Fiziksel mekan güvenliğinin temini,

Görevlendirme süreçlerinin yürütülmesi,

Hukuk işlerinin takibi ve yürütülmesi,

İç denetim/soruşturma/istihbarat faaliyetlerinin yürütülmesi,

İletişim faaliyetlerinin yürütülmesi,

İş faaliyetlerinin yürütülmesi/denetimi,

İş sağlığı/güvenliği faaliyetlerinin yürütülmesi,

İş süreçlerinin iyileştirilmesine yönelik önerilerin alınması ve değerlendirilmesi,

İş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi,

Lojistik faaliyetlerinin yürütülmesi,

Mal/hizmet satın alım süreçlerinin yürütülmesi,

Mal/hizmet satış sonrası destek hizmetlerinin yürütülmesi,

Mal/hizmet satış süreçlerinin yürütülmesi,

Mal/hizmet üretim ve operasyon süreçlerinin yürütülmesi,

Müşteri ilişkileri yönetimi süreçlerinin yürütülmesi,

Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi,

Organizasyon ve etkinlik yönetimi,

Reklam/kampanya/promosyon süreçlerinin yürütülmesi,

Risk yönetimi süreçlerinin yürütülmesi,

Saklama ve arşiv faaliyetlerinin yürütülmesi,

Sosyal sorumluluk ve sivil toplum aktivitelerinin yürütülmesi,

Sözleşme süreçlerinin yürütülmesi,

Stratejik planlama faaliyetlerinin yürütülmesi,

Talep/şikayetlerin takibi,

Taşınır mal ve kaynakların güvenliğinin temini,

ürün/hizmetlerin pazarlama süreçlerinin yürütülmesi,

Veri sorumlusu operasyonlarının güvenliğinin temini,

Yatırım süreçlerinin yürütülmesi,

Yetkili kişi, kurum ve kuruluşlara bilgi verilmesi,

Yönetim faaliyetlerinin yürütülmesi,

Ziyaretçi kayıtlarının oluşturulması ve takibi amaçları ile işlenecektir.

Bununla birlikte, tarafımıza kişisel verilerinizin işlenmesine ilişkin onay vermeniz halinde, söz konusu kişisel verileriniz, ürün ve hizmetlerimizin ihtiyaçlarınız ve istekleriniz doğrultusunda özelleştirilebilmesi, ürün ve hizmetler hakkında memnuniyetinizin ölçülmesi, istek ve ihtiyaçlarınız doğrultusunda ürün ve hizmetlerimizin geliştirilmesi, çeşitlendirilmesi, şirketin ve bağlı şirket ve iştiraklerinin faaliyetleri konusunda tanıtım yapılabilmesi ve bilgi verilebilmesi, pazarlama analiz çalışmalarının yapılması, kişiye özel kampanya, reklam, promosyon çalışmalarının gerçekleştirilmesi amaçlarıyla da işlenecektir.

1. **Kişisel Verilerin Aktarılması:**

Kanun ve yukarıda yer alan maddeler uyarınca toplanan kişisel verileriniz; Kanun tarafından öngörülen temel ilkelere uygun olarak ve Kanun'un 8. ve 9. maddelerinde belirtilen kişisel veri işleme şartları ve amaçları dahilinde ve yukarıda yer alan amaçlarla, yurt içine ve yurt dışına, hizmet ilişkisi içerisinde olduğumuz iş ortakları ve tedarikçilerimize, Veri Sorumlusu iş ortaklarına, kanunen yetkili kamu kurum, kuruluş ve kişilere aktarılmaktadır.

1. **Kişisel Veri Sahibi Olarak Haklarınız**

Veri sahibi olarak Kanun'un ilgili kişinin haklarını düzenleyen 11.Maddesi kapsamındaki taleplerinizi, "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e" göre, yazılı ve ıslak imzalı olarak yukarıda belirtilen veri sorumlusu adresine, elektronik imzalı olarak arkasturizmseyahatacentasi@hs03.kep.tr'ye, varsa daha önce bizimle iletişime geçtiğiniz e-posta adresinizi kullanmak suretiyle kvkkirtibat@arkasturizm.com.tr üzerinden Veri Sorumlusu İrtibat Kişisine veya Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de yer alan diğer yöntemlerle Şirketimize iletebilirsiniz.

Veri Sorumlusu, talebinizin niteliğine göre en kısa sürede ve tebliğ tarihinden itibaren en geç 30 (otuz) gün içinde talebinizi sonuçlandıracaktır.

Kişisel verilerinizin işlenmesine ilişkin detaylı bilgi almak isterseniz, www.arkasturizm.com 'de yer alan "Kişisel Verilerin Korunması ve İşlenmesi Politikasına" göz atabilirsiniz.

Kişisel Verilerin Korunması ve İşlenmesi Politikası

1. **Giriş**

Bu politika ile 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ve ilgili ulusal mevzuat çerçevesinde; kişisel verilerin toplanması, işlenmesi, aktarılması, güncellenmesi ve yok edilmesi konusunda ARKAS TURİZM SEYAHAT ACENTASI A.Ş. (Veri Sorumlusu) tarafından benimsenen ilkeler ile uyulacak kurallar belirlenmiştir.

1. **Politikanın Sahibi**

Kişisel Verilerin Korunması ve İşlenmesi Politikası'nın sahibi Veri Sorumlusu ARKAS TURİZM SEYAHAT ACENTASI A.Ş. 'dir.

1. **Amaç**

Bu politika ile, Veri Sorumlusu tarafından kişisel verileri işleme faaliyeti ve kişisel verilerin korunmasına yönelik benimsenen kurallar konusunda açıklamalarda bulunmak; bu kapsamda, iş ortaklarımız, mevcut ve aday çalışanlarımız, mevcut ve potansiyel müşterilerimiz, şirket hissedarlarımız, ziyaretçilerimiz ve üçüncü kişiler başta olmak üzere kişisel verileri şirketimiz tarafından işlenen kişilerin bilgilendirilmesi ve şeffaflığın sağlanması amaçlanmaktadır.

1. **Kapsam**

Veri Sorumlusu hissedar ve ortaklarını, çalışanlarını, aday çalışanlarını, stajyerlerini, alt işverenlerini, tedarikçilerini, mevcut ve potansiyel müşterilerini, ziyaretçilerini ve kişisel verileri işlenen üçüncü kişileri kapsar.

1. **Güncelleme**

Kişisel Verilerin Korunması ve İşlenmesi Politikası kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilerek kayıt altına alınır. En güncel versiyonu veri sorumlusu internet sitesinde yayınlanır.

1. **Tanımlar**

Burada yer almayan tanımlar, Kanun ve ikincil düzenlemelerde tanımlandıkları şekilde kullanılacaktır.

- *Açık Rıza* : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.
- *Anonim Hale Getirme*: Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
- *Aydınlatma Yükümlülüğü*: Veri Sorumlusu'nun, kişisel verilerini işlediği kişilere, bu verilerinin kim tarafından, hangi amaçlarla ve hangi hukuki gerekçelere dayanarak işlenebileceği, kimlere hangi amaçlarla aktarılabileceği hususunda bilgi vermesi yükümlülüğüdür.
- *İlgili Kişi* : Kişisel verisi işlenen gerçek kişidir.
- *Kişisel Veri* : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Kişilerin adı, soyadı, doğum tarihi ve doğum yeri, kişinin fiziki, ailevi, ekonomik ve sair özelliklerine ilişkin bilgiler, isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası gibi veriler kişisel veridir.

- *Kişisel Verinin 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, sınırlandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir
- *özel Nitelikli Kişisel Veri* : Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkümiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
- *Veri İşleyen* : Veri Sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, Veri Sorumlusu'nun organizasyonu dışındaki gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, Veri Sorumlusu'nun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem Veri Sorumlusu, hem de Veri İşleyen olabilir.
- *Veri Sorumlusu* : Kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
- *Veri Sorumluları Sicili (VERBİS)* : 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre Veri Sorumlusu olanların kaydolmak zorunda oldukları Kişisel Verilerin Korunması Kurumu (Kurum) Başkanlığı tarafından kamuya açık olarak tutulması öngörülen bir kayıt sistemidir.

1. **Roller ve Sorumluluklar**

Kişisel Verilerin Korunması ve İşlenmesi Politikası kapsamında birbirini tamamlayan, dört farklı rol tanımlanmıştır.

1. *Veri Yetkilisi*

Veri Sorumlusu için atanmış biri asıl diğeri yedek, iki "Veri Yetkilisi" bulunmaktadır. Veri Yetkilisi'nin aşağıda sıralanan sorumlulukları bulunmaktadır.

1. Veri Yetkilisi, bağlı bulunduğu Veri Sorumlusu'nun tüm çalışanlarıyla birlikte detaylı kişisel veri işleme envanteri oluşturmak ve ilişkili faaliyetleri koordine etmek.
2. Veri işleme faaliyetlerinde meydana gelen değişiklik ve düzenlemeleri takip etmek, envanteri güncel tutmak.
3. Olası değişiklikleri Veri Sorumlusu İrtibat Kişisi'ne aktarmak.
4. Şirket politika, prosedür ve talimatlarında belirtilen iş ve işlemleri yapmak.

1. *Veri Sorumlusu İrtibat Kişisi*

Her bir Veri Sorumlusu için atanmış bir "Veri Sorumlusu İrtibat Kişisi" bulunmaktadır. Veri Sorumlusu İrtibat Kişisi'nin aşağıda sıralanan sorumlulukları bulunmaktadır.

1. Veri Sorumlusu İrtibat Kişisi görevli olduğu Veri Sorumlusu içinde kişisel verilerin korunmasına dair tüm süreç ve faaliyetlerden haberdar olmak.
2. Resmi ve iç denetim süreçlerinde Veri Sorumlusunu temsil etmek, talep edilen, ihtiyaç duyulan aksiyonları almak, sonuçlandırılmasını sağlamak.
3. İlgili kişilerden gelen başvuruları yanıtlamak.
4. Veri ihlali durumunda şirket yönetimini, KVK Danışma Grubu'nu ve Hukuk Departmanı'nı bilgilendirmek.
5. Sorumluluk alanlarındaki Veri Sorumlusu ve ilgili birimlerinin bildirmiş oldukları veri işleme faaliyetlerinde meydana gelen değişiklik ve düzenlemeleri Veri Yetkilisi ile birlikte takip etmek, envanteri güncel tutmak.
6. VERBİS'de kayıtlı bilgilerde değişiklik olması halinde meydana gelen değişiklikleri, değişikliğin meydana geldiği tarihten itibaren yedi gün içerisinde VERBİS üzerinden Kurum'a bildirmek.
7. Kurum ile iletişimi sağlamak.
8. Veri ihlali durumunda yasal olarak gerekli bildirimleri usulüne uygun bir şekilde yapmak.
9. Şirket politika, prosedür ve talimatlarında belirtilen iş ve işlemleri yapmak.

1. *Veri Sorumlusu üst Yönetimi*

    1. Veri Sorumlusu üst Yönetimi'nin görevi (Yönetim Kurulu Başkanı, Genel Müdür vb.) Veri Sorumlusu İrtibat Kişisinin görevini, kanunda tarif edilen şekilde yerine getirdiğini denetlemektir.
    2. Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi değişiklik ve atamaları iş akdinin sona ermesiyle birlikte Veri Sorumlusu üst Yönetimi tarafından yapılır ve KVK Danışma Grubu'na bildirilir.

1. *KVK Danışma Grubu*

    1. KVK Danışma Grubu, Veri Sorumlusu için geçerli olacak KVKK politika ve prosedürlerinin hazırlanması, güncellenmesinden ve denetlenmesinden sorumludur.
    2. Kanun ile ilgili mevzuatta gerçekleşecek güncelleme ve değişiklikleri takip eder.
    3. İdari ve teknik tedbirlerde güncelleme gerektiren durumlar için gerekli aksiyonları alır.
    4. Arkas Grup şirketleri genelinde KVK danışmanlığı vermek.
    5. Veri Sorumlusu İrtibat Kişileri tarafından kendisine bildirilecek Kurum teftişi, ilgili kişi ihbarı, şikayeti vb. mevzuat kapsamına giren aksiyonlarla ilgili danışmanlık verir.

1. **Onaylama**

KVK Danışma Grubu tarafından hazırlanan politikayı Veri Sorumlusu adına ilgili üst yönetim temsilcileri onaylar.

1. **Kişisel Verileri İşlenen Kişiler**

çalışan adayı, çalışan, habere konu kişi, hissedar/ortak, potansiyel ürün veya hizmet alıcısı, stajyer, tedarikçi çalışanı, tedarikçi yetkilisi, ürün veya hizmet alan kişi, veli/vasi/temsilci, ziyaretçiler vb. gerçek kişilerin kişisel verisi işlenmektedir.

1. **Veri Kategorileri**

Kişisel veri işleme amacına uygun olarak belirtilen kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetim, finans, mesleki deneyim, pazarlama, görsel ve işitsel kayıtlar, felsefi inanç, din, mezhep ve diğer inançlar, dernek üyeliği, sağlık bilgileri, ceza mahkümiyeti ve güvenlik tedbirleri ve biyometrik veriler işlenmektedir.

1. **Kişisel Verilerin İşlenmesine ve Paylaşılmasına Yönelik Faaliyetler ve Amaçlar**

Kişisel veriler; acil durum yönetimi süreçlerinin yürütülmesi, bilgi güvenliği süreçlerinin yürütülmesi, çalışan memnuniyeti ve bağlılığı süreçlerinin yürütülmesi, çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi, çalışanlar için yan haklar ve menfaatleri

süreçlerinin yürütülmesi, denetim/etik faaliyetlerinin yürütülmesi, eğitim faaliyetlerinin yürütülmesi, erişim yetkilerinin yürütülmesi, faaliyetlerin mevzuata uygun yürütülmesi, finans ve muhasebe işlerinin yürütülmesi, fiziksel mekan güvenliğinin temini, görevlendirme süreçlerinin yürütülmesi, hukuk işlerinin takibi ve yürütülmesi, iç denetim/soruşturma/istihbarat faaliyetlerinin yürütülmesi, iletişim faaliyetlerinin yürütülmesi, insan kaynakları süreçlerinin planlanması, iş faaliyetlerinin yürütülmesi/denetimi, iş sağlığı/güvenliği faaliyetlerinin yürütülmesi, iş süreçlerinin iyileştirilmesine yönelik önerilerin alınması ve değerlendirilmesi, iş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi, lojistik faaliyetlerinin yürütülmesi, mal/hizmet satın alım süreçlerinin yürütülmesi, mal/hizmet satış süreçlerinin yürütülmesi, mal/hizmet üretim ve operasyon süreçlerinin yürütülmesi, organizasyon ve etkinlik yönetimi, performans değerlendirme süreçlerinin yürütülmesi, reklam/kampanya/promosyon süreçlerinin yürütülmesi, risk yönetimi süreçlerinin yürütülmesi, saklama ve arşiv faaliyetlerinin yürütülmesi, sosyal sorumluluk ve sivil toplum aktivitelerinin yürütülmesi, sözleşme süreçlerinin yürütülmesi, stratejik planlama faaliyetlerinin yürütülmesi, talep/şikayetlerin takibi, taşınır mal ve kaynakların güvenliğinin temini, ücret politikasının yürütülmesi, veri sorumlusu operasyonlarının güvenliğinin temini, eğer yabancı bir personel söz konusu ise, yabancı personel çalışma ve oturma izni işlemleri, yetkili kişi, kurum ve kuruluşlara bilgi verilmesi, yönetim faaliyetlerinin yürütülmesi faaliyetleriyle sınırlı olarak ve bunlara bağlı yukarıda sıralanan amaçlarla işlenecektir.

Kişisel verileriniz; Kanun tarafından öngörülen temel ilkelere uygun olarak ve Kanun'un 8. ve 9. maddelerinde belirtilen kişisel veri işleme şartları ve amaçları dâhilinde ve yukarıda yer alan amaçlarla, yurt içine ve yurt dışına, hizmet ilişkisi içerisinde olduğumuz iş ortakları ve tedarikçilerimize, Arkas Holding A.Ş. ve bağlı şirketleri/kuruluşlarına, kanunen yetkili kamu kurum, kuruluş ve kişilere aktarılmaktadır.

1. **üçüncü Parti Hizmet Sağlayıcılara Veri Aktarırken Alınan önlemler**

üçüncü parti hizmet sağlayıcılar ile yapılan sözleşmelere ve eklerine kişisel verilerin korunmasına yönelik maddeler eklenir, ayrı bir gizlilik sözleşmesi yapılır, ek taahhütname veya protokollerin düzenlenmesi ve söz konusu hizmet sağlayıcılar denetlenerek kişisel verilerin uygun şekilde korunup korunmadığı kontrol edilir. Ayrıca topluluk şirketleri ile iştirakler ve bağlı ortaklıklar arasında "çerçeve Veri Transferi Sözleşmesi" düzenlenerek topluluk içerisinde kişisel veri paylaşımı düzenlenir.

1. **Veri Koruma Politika ve Prosedürleri**

İşbu politika,Veri Sorumlusu bünyesinde kişisel verilerin korunması ve işlenmesinin genel şartlarını içerir.

1. "Kişisel Verileri Saklama ve İmha Politikası", Veri Sorumlusu bünyesinde, kişisel verilerin saklanması ve imha süreçlerine dair kural ve prosedürleri içerir.
2. "özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası" , Veri Sorumlusu bünyesinde, özel nitelikli kişisel verilere özgü işlenme şart ve yöntemleri düzenleyen kural ve prosedürleri içerir.

3. "çalışan Kişisel Verilerinin Korunması ve İşlenmesi Politikası", Veri Sorumlusu bünyesinde çalışan kişilere ait kişisel verilerin korunması ve işlenmesin şart ve yöntemleri düzenleyen kural ve prosedürleri içerir.
4. "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasının" ticari ve operasyonel her türlü elektronik, yazılı veya diğer ortamlardaki bilgi ve verilerin güvenliği ve gizliliğini sağlamayı amaçlar; çalışanlara yönelik kişisel verilerin işlenmesine dair genel prensipleri belirler.
5. Aydınlatma ve Açık Rıza metinleri ile ilgili kişilerin bilgilendirilmesi ve kişisel verilerinin işlenebilmesi süreçlerinin Kanun'a uygun şekilde yürütülmesi sağlanır.
6. İç eğitimler ile çalışanlar, Kanun konusunda bilgilendirilir ve farkındalık artırılması hedeflenir.
7. "İlgili Kişi Taleplerinin Yönetimi Prosedürü" Veri Sorumlusu bünyesinde, ilgili kişilerden gelen taleplerin araştırılması, bu taleplere yanıt verilmesi, bu taleplerle ilgili gerekli aksiyonların alınması süreçlerinin kural ve şartları belirlenir.
8. Veri Sorumlusu bünyesinde, kişisel veri işleme faaliyetleri düzenli olarak denetlenir.

1. **Risk Analizi**

İç Denetim Departmanı tarafından düzenli olarak gerçekleştirilen denetimler neticesinde ortaya çıkan risk bulguları KVK Danışma Grubu ile değerlendirilir. Alınması gereken aksiyonlarla veya değiştirilmesi gereken süreçlerle ilgili Arkas Holding A.Ş. ve bağlı şirketleri üst yönetimine bilgi verilir ve ilgili Veri Sorumlusu'nun gerekli tedbirleri alması sağlanır.

1. **Politika Dışı Durumlar**

İşbu politikada tarif edilenler dışında farklı uygulamalar tespit edilmesi durumunda, tespiti yapan kişiler Veri Sorumlusu İrtibat Kişisi ve Veri Yetkililerinden destek alarak KVK Danışma Grubu'na yazılı olarak bilgi verirler.

1. **Kişisel Verilerin İşlenme İlkeleri**

Kanun'a uyumluluğun sağlanması için kişisel veriler mevzuatta öngörülen genel ilke ve hükümlere uygun olarak işlenir. Bu kapsamda, Veri Sorumlusu; Kanun ve Kanun ile ilgili mevzuata uygun olarak kişisel verilerin işlenmesinde aşağıda sıralanan ilkelere uygun hareket ederler.

1. *Hukuka ve Dürüstlük Kuralına Uygun Kişisel Veri İşleme Faaliyetlerinde Bulunma*

Veri Sorumlusu; kişisel verilerin işlenmesi faaliyetleri kapsamında hukuka ve dürüstlük kurallarına uygun hareket eder.

1. *Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama*

Veri Sorumlusu; kişisel veri sahiplerinin temel haklarını ve kendi meşru menfaatlerini dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını sağlamak ve bu doğrultuda gerekli tedbirleri almak için gerekli sistemleri kurar.

1. *Belirli, Açık ve Meşru Amaçlarla İşleme*

Veri Sorumlusu; kişisel verilerin hangi amaçla işleneceğini belirler ve bu amaçları kişisel veriler işlenmeden önce veri sahiplerinin bilgisine sunar. Kişisel veriler belirtilen meşru ve hukuka uygun amaçlar dışında işlenmez.

1. *İşlendikleri Amaçla Bağlantılı, Sınırlı ve ölçülü Olma*

Veri Sorumlusu; kişisel verileri belirlenen amaçların gerçekleştirilmesine elverişli bir biçimde işler ve amacın gerçekleştirilmesi ile ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınır. Bu kapsamda, orantılılık gerekliliklerini dikkate alır ve kişisel verileri işleme amacı dışında kullanmaz.

1. *İlgili Mevzuatta öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Etme*

Veri Sorumlusu; öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit eder. Bir süre belirlenmişse bu süreye uygun davranır. Bir süre belirlenmemişse kişisel verileri işlendikleri amaç için gerekli olan süre kadar muhafaza eder.

1. *Bina Girişleri ve İçerisindeki Kişisel Veri İşleme Faaliyetleri ile Ağ ve İnternet Sitesi Kullanıcıları*

Veri Sorumlusu tarafından güvenliğin sağlanması amacıyla, Veri Sorumlusu binalarında ve tesislerinde güvenlik kamerasıyla izleme faaliyeti ile misafir giriş çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunulmaktadır. Güvenlik kameraları kullanılması ve misafir giriş çıkışlarının kayıt altına alınması yoluyla Veri Sorumlusu tarafından kişisel veri işleme faaliyeti yürütülmüş olmaktadır.

Veri Sorumlusu bina, tesis girişlerinde ve tesis içerisinde kamera ile izleme sistemi vasıtasıyla ziyaretçilerimizin ve tüm ilgili kişilerin görüntü kayıtları alınmakta; ad, soyad, TC kimlik numarası, ehliyet numarası, pasaport numarası, personel sicil numarası, unvan, iş alanı, cinsiyet, çalıştığı firma, giriş - çıkış tarih ve saati, motorlu taşıt plakası bilgilerini içeren ziyaretçi listesi tutulmaktadır.

Veri Sorumlusu, güvenlik kamerası ile izleme faaliyeti kapsamında; sunulan hizmetin kalitesini artırmak, güvenilirliğini sağlamak, Veri Sorumlusu'nun, müşterilerin ve üçüncü kişilerin güvenliğini sağlamak ve müşterilerin aldıkları hizmete ilişkin menfaatlerini koruma amacı taşımaktadır.

Veri Sorumlusu tarafından güvenlik amacıyla kamera ile izleme faaliyeti yürütülmesinde Kanun'da yer alan düzenlemelere ve 5188 sayılı "özel Güvenlik Hizmetlerine Dair Kanun" ve ilgili mevzuata uygun olarak sürdürülmektedir.

Kanun'un 12. maddesine uygun olarak, kamera ile izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır.

Veri Sorumlusu tarafından güvenliğin sağlanması ve bu politikada belirtilen amaçlarla, bina ve tesisler içerisinde kaldıkları süre boyunca talep eden ziyaretçilere internet erişimi sağlanabilmektedir. Bu durumda internet erişimlerine ilişkin log kayıtları 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ve buna göre düzenlenmiş olan mevzuatın amir hükümlerine göre kayıt altına alınmakta; bu kayıtlar ancak yetkili kamu kurum ve kuruluşları tarafından talep edilmesi veya Veri Sorumlusu bünyesinde gerçekleştirilecek denetim süreçlerinde ilgili hukuki yükümlülükleri yerine getirmek amacıyla işlenmektedir.

Dijital ortamda kaydedilen ve muhafaza edilen kayıtlara yalnızca sınırlı sayıda Bilgi Güvenliği Birimi personelinin erişimi bulunmaktadır.

Elde edilen log kayıtları değişmezlik ilkesini sağlamak için zaman damgasıyla birlikte kaydedilerek sınırlı sayıda Bilgi Güvenliği Birimi çalışanının erişimi ile saklanmaktadır.

1. *Müşteri ve İş Ortakları Verilerinin İşlenmesi*

Müşterilerle yukarıda belirtilen amaçlar doğrultusunda yazılı, sözlü her türden iletişime geçmek için kişisel veriler işlenebilir.

Sözleşmeden kaynaklanan ilişki dolayısıyla, mevcut ve potansiyel müşteri ve iş ortaklarına (iş ortağının tüzel kişi olması halinde iş ortağı yetkilisine) ait kişisel veri, ayrıca onay alınmadan bir sözleşmenin kurulması, uygulanması ve sonlandırılması için işlenebilir. Sözleşme öncesinde sözleşmeye başlama aşamasında kişisel veriler; teklif hazırlamak, satın alma formu hazırlamak ya da ilgili kişinin sözleşmenin uygulanmasıyla ilgili taleplerini karşılamak amacıyla işlenebilir.

Reklam amaçlı olarak kişisel veriler, reklam ya da pazar ve kamuoyu araştırmaları için ancak bu bilgilerin toplanma amacının söz konusu amaçlara uygun olması durumunda işlenmektedir. İlgili kişi bilgilerinin reklam amaçlı kullanılacağı hususunda bilgilendirilmektedir.

Yasal yükümlülüklerimiz veya kanunda açıkça öngörülmesi sebebiyle yapılan veri işlemleri dolayısıyla, kişisel veriler, işlemenin ilgili mevzuatta açıkça belirtilmesi veya mevzuatla belirlenen bir hukuki yükümlülüğün yerine getirilmesi amacıyla ayrıca onay alınmadan işlenebilir. Veri işlemlerinin tür ve kapsamı, yasal olarak izin verilen veri işleme faaliyeti için gerekli olmalı ve ilgili yasal hükümlere uygun olmalıdır.

özel nitelikli kişisel veriler, Kurum tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla ve Kanun hükümleri çerçevesinde işlenmektedir. Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri, açık rızası; açık rızanın bulunmaması halinde ise Kanun'da öngörülen istisnalar kapsamında işlenmektedir.

1. *çalışan ve çalışan Adaylarını Verilerinin İşlenmesi*

Veri Sorumlusu bünyesinde çalışan kişilere ait kişisel verilerin korunması ve işlenmesin şart ve yöntemleri düzenleyen kural ve prosedürler "çalışan Kişisel Verilerinin Korunması ve İşlenmesi Politikası" içinde yer almaktadır.

Bununla birlikte; iş sözleşmesinin kurulması, uygulanması ve sonlandırılmasına kadar geçen süreçte çalışanlara ait kişisel verilerin toplanması ve işlenmesi zorunludur. Bunlar için

çalışanların ayrıca açık rızaları alınmayabilir. Potansiyel çalışan adaylarının da kişisel verileri iş başvurularında işlenmektedir. Adayın iş başvurusunun reddi halinde, başvuru sırasında elde edilen kişisel veri saklama süresi kadar muhafaza edilmekte, bu sürenin sonunda silinmekte, yok edilmekte veya anonim hale getirilmektedir.

çalışana ait kişisel veriler, işlemenin ilgili mevzuatta açıkça belirtilmesi veya mevzuatla belirlenen bir hukuki yükümlülüğün yerine getirilmesi amacıyla ayrıca onay alınmadan işlenebilir.

çalışanlara ait kişisel veriler, veri sorumlusunun meşru bir menfaatinin bulunduğu hallerde ayrıca onay alınmadan işlenebilmektedir. çalışanlara ait verilerin veri sorumlusunun meşru menfaatine dayanılarak işlenmesi halinde bu işlemenin ölçülü olup olmadığı incelenir, meşru menfaatinin ilgili çalışanın korunması gereken bir hakkını ihlal etmediği kontrol edilir.

özel nitelikli kişisel veriler sadece belli koşullar altında işlenmektedir. Irk ve etnik köken, siyasi düşünce, din, felsefi inanç, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkümiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli veri olarak tanımlanmıştır. özel nitelikli kişisel veriler ancak çalışanın açık rızası olması halinde ve gerekli idari ve teknik tedbirler alınarak işlenebilir.

Aşağıda sıralanan haller bu hükmün istisnasını oluşturmakta olup, belirtilen hallerde çalışanın açık rızası bulunmasa da özel nitelikli kişisel verileri işlenebilecektir. çalışanın sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde; çalışanın 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 işlenebilir.

1. **Kişisel Verilerin İşlenme Şartları**

1. *Kişisel Verilerin Tespiti ve İşlenmesi*

Kanun uyarınca, kişisel veri "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Kişisel veri kavramı sadece ad, soyad, doğum yeri, doğum tarihi gibi kişilerin tanınmasını ve teşhisini sağlayan bilgilerden ibaret olmayıp ayrıca kişilerin fiziksel, sosyal, kültürel, ekonomik, psikolojik tüm bilgilerini de kapsamaktadır.

Kişinin kimlik bilgilerine ek olarak, vatandaşlık numarası, vergi numarası, pasaport numarası, sosyal güvenlik numarası, sürücü belgesi numarası, motorlu taşıt plakası, ev adresi, iş adresi, e-posta adresi, telefon numarası, faks numarası, özgeçmişi, fotoğrafı, videosu, genetik bilgileri, kan grubu, kriminal geçmişi ve adli sicil bilgileri gibi kişinin belirli veya belirlenebilir olmasını

sağlayan tüm bilgiler kişisel veri niteliği taşımaktadır ve kişisel verilerin korunması kapsamına girmektedir.

Bu tanım uyarınca, Veri Sorumlusu, Veri Sorumlusu'nun iş ortakları, çalışanları ve müşterileri başta olmak üzere üçüncü kişiler de dahil, topladıkları tüm verilerin kişisel veri kapsamına girip girmediğini tespit eder ve bu verileri Kanun'daki kurallara uygun olarak işler.

Kişisel verilerin işlenmesi; 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, elde edilebilir hale getirilmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsamaktadır.

1. *İstisnai Haller*

Veri Sorumlusu Kanun uyarınca kişisel verileri ilgili kişilerin açık rızası ile işler. Ancak, aşağıdaki şartlardan herhangi birinin var olması halinde, açık rıza aranmaksın kişisel verilerin işlenmesi mümkündür.

1. Kanunlarda açıkça öngörülmesi (vergi mevzuatı, iş mevzuatı, ticaret mevzuatı vb.).
2. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşme taraflarına ait kişisel verilerin işlenmesinin gerekli olması (İş akdi, satış sözleşmesi, taşıma sözleşmesi, eser sözleşmesi vb.).
3. Fiili imkansızlık nedeni ile rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişilerin kendileri veya bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu bir durum olması.
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olan durumlarda (mali denetimler, güvenlik mevzuatı, sektör odaklı regülasyonlarla uyum vb.).
5. Kişisel verinin ilgili kişisi tarafından alenileştirilmesi (ilgili kişilerin kendisine ait bilgileri umumun bilgisine sunması).
6. Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması (dava açılması, tescil işlemleri, her türlü tapu işlemi vb. işlerde kullanılması zorunlu veriler)
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydı ile veri sorumlusunun meşru menfaatleri için veri işlemesinin zorunlu olması.

1. *özel Nitelikli Kişisel Verilerin İşlenmesi*

Kanun kapsamında bir takım kişisel veriler "özel nitelikli kişisel veri" olarak adlandırılmaktadır. Veri Sorumlusu bu tür verileri ilgilisinin açık rızası olmaksızın işlemez. Açık rıza "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" dır.

Kanun; kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkümiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak saymıştır. Sayılan bu veriler Kanun'da tanımlandığı şekliyle sınırlı sayıda olup, yorum yoluyla artırılamaz.

Veri Sorumlusu, özel nitelikli kişisel verilerin işlenmesinde, Kişisel Verileri Koruma Kurulu (Kurul) tarafından belirlenen yeterli önlemleri de alacaktır.

Veri Sorumlusu; Kanun uyarınca özel nitelikli kişisel verileri ancak aşağıdaki şekilde işlemesi mümkündür.

1. Sahibinin Açık Rızasıyla.
2. Kanun Hükmüyle (sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir).
3. Kamu Sağlığı Gerekçesiyle, sağlık hizmetlerinin planlanması, yönetimi ve finansmanı (kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi).

1. *Kişisel Verilerin Aktarılmasına İlişkin Şartlar*

Veri Sorumlusu, hukuka uygun olan kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak, Kanun'un 5/2. ve 6/3. maddesinde belirtilen şartları (hukuki sebepler) karşılamak şartıyla veya veri sahibinin açık rızası ile kişisel verileri üçüncü kişilere aktarabilir. Aynı zamanda, Veri Sorumlusu, kişisel verileri Kanun'da öngörülen veri işleme şartlarına uygun olarak, açık rıza aranmaksızın üçüncü kişilere aktarabilir.

Veri Sorumlusu, açık rıza olmaksızın aktardığı verileri Kanun'daki sınırlamalara uygun olarak aktarmak amacıyla gerekli idari ve teknik önlemleri alır.

Veri Sorumlusu tarafından kişisel veriler Kurul tarafından yeterli korumaya sahip olduğu ilan edilen yabancı ülkelere veya yeterli korumanın bulunmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ettiği ve Kurul'un aktarım izni verdiği yabancı ülkelere aktarabilir.

1. **Veri Sorumlusunun Yükümlülükleri**

1. *Kişisel Veri Sahibini Aydınlatma Yükümlülüğü*

Veri Sorumlusu, kişisel verilerin elde edilmesi sırasında kişisel veri sahiplerini aşağıda yer alan hususlarda aydınlatır.

Bu yükümlülük uyarınca, Veri Sorumlusu hazırlamış olduğu aydınlatma metni ile ilgili kişileri bilgilendirir. Aydınlatma;ilgili kişi ile ilk iletişime geçildiği anda yapılır.

Kişisel verilerin ilgili kişiden elde edilmemesi halinde; Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında veya kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada aydınlatma yapılır.

1. *Kişisel Veri Sahiplerinin Başvurularını Sonuçlandırma Yükümlülüğü*

Kişisel veri sahipleri, Kanun uyarınca yazılı olarak veya Kurul'un belirleyeceği diğer yöntemlerle Veri Sorumlusu'na başvuruda bulunarak, bilgi talep edebilir.

Veri Sorumlusu, kişisel veri sahiplerinin haklarının değerlendirilmesi ve kişisel veri sahiplerine gereken bilgilendirmenin yapılması için Kanun'un 13. maddesi uyarınca başvuruları cevaplandırır. Sair idari ve teknik düzenlemelere ilişkin prosedürleri oluşturur ve uygular.

Kişisel veri sahiplerinin hakları şunlardır;

1. Kişisel verilerinin 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 verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme
6. İlgili mevzuatta öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme
7. İlgili mevzuat uyarınca yapılan kişisel verilerinin üzerinde yapılan işlemlerin, kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme
8. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhine bir sonucun ortaya çıkmasına itiraz etme
9. Kişisel verilerinin Kanun'a aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

Veri Sorumlusu, yazılı veya güvenli elektronik imzayla imzalanmış olarak kayıtlı elektronik posta adreslerine veya web sitesinde yer alan "Başvuru Formu" kullanılarak iletilen talepleri işleme alır. Kurul başkaca başvuru yöntemleri belirlediği takdirde bu yollar ile de başvuru kabul edilir.

Veri Sorumlusu, talebi niteliğine göre talebi en kısa sürede ve en geç 30 (otuz) gün içerisinde yanıtlar. Veri Sorumlusu, başvuruları kabul ederek gereken işlemleri gerçekleştirebilir ya da başvuruları gerekçeli olarak reddeder.

Kişisel veri sahibi, başvurusunun reddedilmesi, verilen cevabı yetersiz bulması veya başvuruya cevap verilmemesi hallerinde cevabı öğrendiği tarihten itibaren 30 (otuz) ve her halde başvuru tarihinden 60 (altmış) gün içerisinde Kurul'a şikayette bulunabilir.

Veri Sorumlusu, kişisel veri sahiplerine Kanun'un öngördüğü şekilde zamanında ve gerekçeli olarak cevap verir.

1. *Kişisel Verilerin Güvenliğini Sağlama Yükümlülüğü*

Veri Sorumlusu, işlemekte oldukları kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini engellemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri alır.

Kurul, ileride veri güvenliğine ilişkin yükümlülükler hakkında detaylı düzenlemeler getirebilecektir. Dolayısıyla Veri Sorumlusu, bu kapsamdaki yükümlülüklere de uyum sağlamak amacıyla gerekli özeni gösterir ve kişisel verilerin güvenliğini sağlar.

Veri Sorumlusu, alacağı teknik ve idari tedbirler bakımından tedbirlerin işleyişi ile ilgili olarak gerekli denetimleri yapmaya ve yaptırmaya yönelik sistemleri oluşturur. Bu denetim sonuçları Veri Sorumlusu bünyesinde görevli birimlerce incelenir ve gerekli önlemler alınır.

Veri Sorumlusu, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu öğrendiği tarihten itibaren en geç 72 saat (Yetmiş İki) içinde Kurul'a bildirir. Söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılır.

1. *Hukuka Uygun Veri İşlenmesinin Temini İçin Teknik ve İdari Tedbirlerin Alınması*

Veri Sorumlusu bünyesinde iş birimleri tarafından gerçekleştirilen kişisel veri işleme faaliyetlerine ilişkin tüm süreçler kişisel veri işleme envanterinde toplanır ve analiz edilir. İş birimleri tarafından verilerin toplanmasından silinmesine kadar gerçekleştirilen faaliyetlerin tümünün hukuka uygunluk denetimi yapılır.

Kişisel veri işleme faaliyetleri kurulan teknik sistemler ile denetlenir. Hukuka aykırılık tespit edildiğinde ilgilisine bildirilerek eksiklik ya da hukuka aykırılığın giderilmesi sağlanır.

Veri Sorumlusu, çalışanlarını kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilir ve eğitilir.

Veri Sorumlusu ile Veri Sorumlusu'nun iş ortakları, çalışanları ve müşterileri arasındaki hukuki ilişkiyi yöneten sözleşme ve belgelere, Kanun'daki düzenlemelere aykırı biçimde kişisel verilerin işlenmemesi, ifşa edilmemesi ve kullanılmaması yükümlülüğünü getiren hükümler eklenir.

Her bir iş biriminin faaliyetlerinin Kanun'da belirtilen kişisel veri işleme şartlarına uygunluğunun sağlanmasına yönelik işlemler, her bir iş birimi ve yürütmekte olduğu faaliyet özelinde tespit edilir. İş birimleri özelinde uygulama kuralları belirlenir, bu kuralların denetimini ve uygulamanın sürekliliğini sağlamak için gerekli idari tedbirler alınıp prosedür oluşturularak eğitimler verilir.

1. *Kişisel Verilere Hukuka Aykırı Erişimi Engellemek İçin Teknik ve İdari Tedbirlerin Alınması*

Veri Sorumlusu, kişisel verilerin hukuka aykırı şekilde elde edilmesini, üçüncü kişilere açıklanmasını, görüntülenmesini ve aktarılmasını önlemek için korunacak verinin niteliğine göre gerekli idari ve teknik tedbirleri alır.Bu konuda gerekli işleyiş mekanizmaları geliştirir. Burada yer alan yükümlülüklerine uygun davranmak üzere ilgili iş birimlerini eğitir, görevlendirme ve farkındalıklarını sağlar.

Kişisel Verileri Saklama ve İmha Politikası

1. **Amaç**

1. Bu Kişisel Veri Saklama ve İmha Politikası (Politika) "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in" 5. maddesi

çerçevesinde veri sorumlusunun (Şirket) kişisel veri işleme envanterine uygun olarak hazırlanmıştır.

1. Bu Politika Şirket'in tabi olduğu kanun ve ikincil mevzuata uyumu sağlayabilmek adına Şirket'in kişisel veri saklama ve imhaya ilişkin ilkelerini belirlemektedir.

1. Bu Politika, Şirket tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin yapılması gerekenler hakkında usul ve esasları belirlemek amacıyla hazırlanmıştır.

1. Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (Kanun) belirlenen aşağıdaki ilkeleri gözetmektedir. Kanun uyarınca kişisel verilerin işlenmesinin;

2.

3.

    - Hukuka ve dürüstlük kurallarına uygun olması;
    - Doğru ve gerektiğinde güncel olması;
    - Belirli, açık ve meşru amaçlar için işlenmesi;
    - İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması;
    - İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir.

4.

1. Bu Politika, Şirket'in faaliyetleri çerçevesinde düzenlenmiş, asılları ve kopyaları dahil tüm fiziksel ve elektronik belgelere/ortamlara uygulanır.

1. Yürürlükteki mevzuat Şirket'in belli kayıtları, belli sürelerle saklamasını gerektirebilir. Bu saklama sürelerine uymamak Şirket'i cezalara ve yaptırımlara maruz bırakabilir, adaletin yerine getirilmesini engelleyebilir, yasal delillerin delil özelliklerini yitirmesine neden olabilir ve/veya hukuki süreçlerde Şirket'in konumunu önemli ölçüde zedeleyebilir. Bu yüzden Politika;

1. Yürürlükteki mevzuat kapsamında hazırlanan ve süreçler ile spesifik saklama sürelerini belirleyen bir "EK-A / Saklama ve İmha Süreleri Tablosunu" içermektedir.

2. Ayrıca, Veri Sorumlusu nezdinde saklama ve imha süreçleriyle Şirket içinde hangi kişilerin/birimlerin ilgili ve sorumlu olduğu ile bu kişilerin/birimlerin görevlerini belirleyen bir "EK-B / Saklama ve İmha Sürecinde Yer Alan Kişiler Tablosu" Politika içinde yer almaktadır.

1. Şirket çalışanları bu Politika'yı tam olarak anlamak ve uygulamakla yükümlüdür.

1. **Tanımlar**

özel isim olmadıkça ve Politika içerisinde ayrı bir yerde tanımlanmadıkça, aşağıda listelenen terimler, tanımlandıkları anlamlara gelirler:

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Alıcı Grubu	Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini ifade eder.
Aktif Kayıtlar	Şirket'in işleyişi, idaresi ve yönetimi için halen kullanılmakta olan kayıtları ifade eder.
Aktif Olmayan Kayıtlar	Kullanılmayan; ancak işlenmesi sonradan gerekebileceği için saklama süreleri sona ermemiş kayıtları ifade eder.
Anonim Hale Getirme	Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.
	Veri sorumlusu bünyesinde çalışan gerçek kişileri ifade eder.
•	
De-manyetize Etme	Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemini ifade eder.
Elektronik Ortam	Elektronik ortam, insan müdahalesi ihtiyacını asgari seviyeye indirilerek verilerin tutulduğu, mantıksal veya aritmetik işlemlerin uygulandığı, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya aktarılması gibi işlemlerin otomatik veya kısmen otomatik yöntemlerle gerçekleştirildiği ortamları ifade eder.
Elektronik Olmayan Ortam	Bir veri kayıt sistemine bağlı olarak otomatik olmayan yollarla işleme ise manuel olarak hazırlanan ancak erişimi ve anlamlandırmayı kolaylaştıran işleme faaliyetini ifade eder.
Fiziksel Yok Etme (*Elektronik Veriler İçin*)	Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesini ifade eder.

Hizmet Sağlayıcılar	Veri Sorumlusu'na ürün veya hizmet satmak amacıyla ticari faaliyette bulunan gerçek ve tüzel kişiler ile bu hizmetlere aracılık eden gerçek ve tüzel kişileri ifade eder.
İki Kademeli Kimlik Doğrulama	Kişinin kullanıcı adı ve şifresi ile, dışarıdan ayrı bir kimlik doğrulama sisteminin (cep telefonu, kişisel soru, kriptografik anahtar vb.) birleşiminden oluşan doğrulama sistemini ifade eder.
İkincil Mevzuat	Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan ya da alınan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüş anlamına gelir.
İlgili Kişi	Kişisel verisi işlenen gerçek kişiyi ifade eder.
İlgili Kullanıcılar	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere Veri Sorumlusu organizasyonu içerisinde veya Veri Sorumlusu'ndan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri ifade eder.
•	Silme, yok etme ve/veya anonim hale getirme işlemlerinden herhangi birini veya tümünü ifade eder.
•	6698 sayılı Kişisel Verileri Koruma Kanunu'nu ifade eder.
•	Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması, buzlanması, yıldızlanması gibi işlemleri ifade eder.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen Kişisel verilerin bulunduğu her türlü ortamı ifade eder.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kayıtlı Elektronik Posta (KEP)	Elektronik iletilerin, gönderimi ve teslimatı da dahil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şeklini ifade eder.
Kişisel Veri İşleme Envanteri	Veri Sorumlusu'nun iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçlarını, hukuki sebeplerini, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan muhafaza edilme sürelerini, yabancı ülkelere aktarımı öngörülen kişisel

	verileri ve veri güvenliğine ilişkin alınan tedbirleri detaylandıran envanteri ifade eder.
Kurul	Kişisel Verileri Koruma Kurulu'nu ifade eder.
Kurum	Kişisel Verileri Koruma Kurumu'nu ifade eder.
KVK Danışma Grubu	Şirket içerisinde Kanun'a uyumlulaştırma projesinin tamamlanması ve sonrasındaki danışmanlık hizmetlerini yürüten şirket çalışanlarını ifade eder.
özel Nitelikli Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri ifade eder.
Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama Ve İmha Politikası'nda belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini ifade eder.
•	Bu Kişisel Veri Saklama ve İmha Politikası'nı ifade eder.
Saklama ve İmha Süreleri Tablosu	Ek A'da yer alan "Saklama ve İmha Süreleri Tablosunu" ifade eder.
1.	Kriptografik ağ protokolü SSH kullanarak dosya transferi yapan bir dosya aktarım protokolüdür.
•	Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder.
•	Veri Sorumlusu'nu ifade eder.
üzerine Yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemini ifade eder.
•	Veri Sorumluları Sicili (VERBİS), veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir.
Veri İşleyen	Veri Sorumlusu'nun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, Veri Kayıt Sistemi'nin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
Veri Sorumlusu İrtibat Kişisi	Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.
Veri Yetkilisi	Veri Sorumlusu tarafından atanan ve Kanun'a uygun olarak Şirket kişisel veri envanterini oluşturan, güncel tutan ve gerekli değişiklikleri Veri Sorumlusu İrtibat Kişisine ileten şirket çalışanını ifade eder.
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi ifade eder.
•	28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan ve 1 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i ifade eder.

Burada yer almayan tanımların, Kanun ve ikincil düzenlemelerde belirtilen anlamları ile kullanıldığı kabul edilecektir.

1. **Kapsam**

1. Bu Politika, Şirket'in tamamına uygulanır ve gerekli yükümlülükleri düzenler. Şirket tarafından kişisel verileri işlenen tüm gerçek kişilere ilişkin kişisel veriler bu Politika kapsamındadır. Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları hakkında ve tüm veri işleme faaliyetlerinde bu Politika uygulanacaktır.

1. Şirket, Veri Sorumlusu olarak kişisel veri işlediğinde, bu Politika'da yer alan düzenlemelere uygun davranır.

1. Şirket, bir başkası namına Veri İşleyen olarak kişisel veri işlediği durumda bu Politika'da yer alan düzenlemelere ve varsa, söz konusu üçüncü kişi ile imzalanan her türden sözleşmedeki, Politika'ya aykırı olmayan, talimatlara uyar.

1. Politika'nın uygulanmasından ve Politika'ya uyumun sağlanmasından ilgili departman yöneticisi, Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi sorumludur.

1. Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Nedenler

    1. Şirketimiz;

- 213 Sayılı Vergi Usul Kanun'u,
- 2004 Sayılı İcra İflas Kanun'u,
- 4857 Sayılı İş Kanun'u,
- 5237 Sayılı Türk Ceza Kanun'u,
- 5510 Sayılı SSGSK Kanun'u,
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6201 Sayılı Türk Ticaret Kanun'u,
- 6098 Sayılı Borçlar Kanun'u,
- 6331 Sayılı İş Sağlığı ve Güvenliği Kanun'u,
- 6698 Sayılı Kişisel Verilerin Korunması Kanun'u, ilgili yönetmelikleri gereği ve bunlarla sınırlı olmamak üzere yayınlanan diğer mevzuat hükümleri,
- çalışma Bakanlığı ve SGK müfettişlerince yapılan denetimlerde,
- İstatistiksel çalışmalar için,
- Ayrıca mahkeme ve bilirkişi incelemelerinde sunmak üzere,
- Yerel kolluk kuvvetleri ve organize sanayi müdürlüklerince istenmesi durumunda,

kişisel veriler işlenebilir, saklamak ve gereği geldiğinde silmek üzere kayıt altına alınabilir.

1. Kişisel verilerin saklanmasını gerektiren işleme amaçları; insan kaynakları süreçlerini yürütmek, kurumsal iletişimi sağlamak, şirket güvenliğini sağlamak, istatistiksel çalışmalar yapabilmek, imzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak, şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak, iş sağlığı güvenliği süreçlerinin yürütülmesini sağlamak, bilgi sistemleri süreçlerini yürütmek, ziyaretçi, kamera ve toplantı kayıtlarını tutmak, müşteri verilerini işlemek, tedarik süreçlerini yönetmek, muhasebe ve finans süreçlerini yürütmek, seyahat süreçlerini takip etmek, posta, kargo, gönderi kayıtlarını işlemek tır.

1. - Kayıt Ortamları
2. - Fiziksel Kayıtlar
3. - Yazılı, basılı ortamlar ve manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) gibi fiziksel ortamlar, fiziksel kayıtlar, kağıt üzerindeki kayıtlar, fotoğraflar ve sözleşmeler gibi kağıt, mikro fiş ve benzeri ortamlarda bulunan kayıtlardan oluşur.

4. - Aktif olmayan kayıtlar Şirket'in arşivlerine gönderilir.
5. - Elektronik Kayıtlar
6. - Ses kayıtları, fotoğraflar, videolar ve görsel ve işitsel ortamlar dahil birçok ortamda yer alan kişisel veriler; doğru, güncel ve kişisel verileri işlemesi gereken kişilerce erişilebilir olacak şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli elektronik ortamlarda saklanabilir. Elektronik ortamlara örnek olarak;

- Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.),
- Yazılımlar (ofis yazılımları, portal vb.),
- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit, engelleme, günlük kayıt dosyası, anti virüs vb.),
- Yedekleme kartuşları,
- Kişisel bilgisayarlar (Masaüstü, dizüstü),
- Mobil cihazlar (telefon, tablet vb.),
- Optik diskler (CD, DVD vb.),
- çıkartılabilir bellekler (USB, hafıza kartı vb.),
- Yazıcı, tarayıcı, fotokopi makinesi vb. diğer elektronik veri kayıt ortamları sayılabilir.

1. Elektronik kayıtların, kaybedilmeye, değiştirilmeye ve izinsiz yok edilmeye, saklanma süreçlerinde erişime karşı korunmalarını sağlamak ve eksiksiz, doğru ve okunaklı olmasını temin etmek için yeterli koruma önlemleri alınmalı, süreçler oluşturulmalı ve Şirket tarafından uygulanmalıdır.

6.Saklama ve İmha Süreleri, Periyodik İmha 6.1.EK-A spesifik süreçlerle birlikte bunların saklama sürelerini içermektedir. EK-B bu süreçlerde kimlerin yer aldığını ve bu kişilerin/birimlerin görevlerini içermektedir. 6.2.Bu Politika bağlamında, saklama takvimi kaydın oluşturulduğu takvim yılının sonunda başlar. Saklama süresi dolmuş tüm kayıtlar yılda iki kez imha edilir. İlk periyodik imha takvim yılının sonunda, ikinci ise her yıl Haziran ayının sonunda yapılır ve Periyodik İmhalar arasında süre her halde altı ayı geçemez. Bir kişisel verinin işleme amacının ortadan kalktığı tarih bu iki dönemden hangisine daha yakınsa o dönemde İmha edilir. (örneğin; bir kayıt Mart 2010'da oluşturulduysa ve yedi yıl boyunca tutulması gerekiyorsa, Kayıt 30 Haziran 2017 tarihinde İmha edilir; eğer söz konusu kayıt Kasım 2010'da oluşturulmuş olsaydı 31 Aralık 2017 tarihinde İmha edilmesi gerekecekti.) 7.İmha

1. Kayıtlar, aşağıdaki hallerde imha edilmelidir.
    1. Kişisel verilerin aşağıdaki koşullardan hangisinin gerçekleşmesi halinde silineceği ve bu koşulların gerçekleşmesi halinde alınacak aksiyonlar, somut olayın koşullarına, Kanun, Yönetmelik ve İkincil Mevzuat hükümlerine göre üst Yönetim, Veri Sorumlusu İrtibat Kişisi ve KVK Danışma Grubu tarafından belirlenir ve şirket veri envanterlerinde güncel haliyle, saklama süreleri de belirtilerek, kayıt altına alınır.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş Sağlığı Güvenliği Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Faaliyetlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Süreçlerin Yürütülmesi	Başvuru sürecinin sona ermesinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Siber Güvenlik Olay Yönetimi	Kayıt altına alınmasını takiben 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	Kayıt altına alınmasını takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	Kayıt altına alınmasını takiben 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Ziyaretçi ve Toplantı Katılımcıların Kaydı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Verileri	Kayıt altına alınmasını takiben 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarik Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul ve Yönetim Kurulu İşlemleri	Kayıt altına alınmasını takiben 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Resmi ve Hukuki İşlemlerin Yürütülmesi	Kayıt altına alınmasını takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Seyahat Süreçleri	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Posta, Kargo, Gönderi Kayıtları	Kayıt altına alınmasını takiben 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

- Kişisel verileri işleme şartlarının tamamının ortadan kalkması koşuluyla İlgili Kişi, kişisel verisinin imhasını talep ettiğinde,
- İlgili Kişi, kişisel verisinin işlenmesi ile ilgili açık rızasını geri aldığında,
- Kişisel verilerin işlenmesine veya saklanmasına ilişkin gereklilikler ve/veya amaçlar ortadan kalktığında,
- Kişisel verilerin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası halinde,
- Kurum, usulüne uygun olarak kişisel verinin imhasını talep ettiğinde,
- Kişisel verinin saklama süresi sona erdiğinde imha edilir.

1. Kişisel verileri işleme şartlarının tamamının ortadan kalkmaması halinde İlgili Kişi'nin kişisel verisinin imhasını talep etmesi durumunda bu talep, Veri Sorumlusu İrtibat Kişisi tarafından hazırlanacak yazılı gerekçe ile reddedilebilir. Bu yazılı gerekçe şirkete, talebin tebliğ edildiği tarihten itibaren 30 (otuz) gün içerisinde talepte bulunan İlgili Kişi'ye gönderilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, talebe konu Kişisel Veriler imha edilir. Bu bağlamda İlgili Kişi'nin talebi tebliğ edildiği tarihten itibaren en geç 30 (otuz) gün içerisinde sonuçlandırılır ve İlgili Kişi'ye bilgi verilir.

1. Şirket, Veri Sorumlusu İrtibat Kişisi ve KVK Danışma Grubu aracılığı ile imha yöntemlerinden uygun olanı seçer. İlgili kişinin talebi durumunda ise, uygun yöntemi seçmesinin gerekçesini açıklar. Bu gerekçenin açıklaması Veri Sorumlusu İrtibat Kişisi tarafından yapılır ve İlgili Kişi'nin talebi halinde, Kanun, Yönetmelik ve ikincil mevzuata uygun şekilde İlgili Kişi'ye iletilir.

1. Kişisel Verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişiye aktarılmışsa bu durum üçüncü kişiye bildirilir ve üçüncü kişi nezdinde Yönetmelik kapsamında imha ile ilgili gerekli işlemlerin yapılması takip edilir.

1. Kayıtların Yok Edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi ile sağlanır. Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin hiçbir şekilde erişilememesini, geri getirilememesini ve tekrar kullanılamamasını sağlamak gerekir. Kişisel verilerin yok edilmesi faaliyeti, Veri Sorumlusu İrtibat Kişisi tarafından imzalanmış yok etme kararını aldıktan sonra, Şirket tarafından yerine getirilir. Veri Sorumlusu İrtibat Kişisi, yok etme faaliyetinden sorumlu kişileri, neden ilgili yok etmenin gerekli olduğu konusunda bilgilendirir.

1. *Elektronik Kayıtlar;*

- Elektronik kayıtlar de-manyetize etme, fiziksel yok etme ve üzerine yazma yollarıyla yok edilebilir.
- Ağ cihazlarının (switch, router vb.) içindeki saklama ortamları sabittir. ürünler, çoğu zaman silme komutuna sahiptir ama veriyi yok etme özelliği bulunmamaktadır. De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle veri yok edilir.
- Kişisel verilerin yer aldığı flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları için, destekleniyorsa yok etme komutunu

kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da de-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

- Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle veri yok edilir.
- CD, DVD gibi veri saklama ortamlarında yer alan kişisel veriler, yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.
- Kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimlerinde yer alan kişisel veriler için, tüm kayıt ortamlarının söküldüğü doğrulandıktan sonra birimin niteliğine göre uygun yok etme yöntemi seçilir.

1. *Fiziksel kayıtlar* ise kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta (mümkünse dikey ve yatay şekilde parçalanarak) veya okunmasını imkansız kılacak başka yöntemlerle (örneğin, kaydı birleştirilemeyecek ufak parçalara kesmek veya fiziksel kaydı uygun bir ortamda yakmak vb.) İmha edilir.

1. *Bulut sistemleri* için; bu sistemlerde yer alan kişisel verilerin depolanması için kullanılan veri tabanları kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

1. *Arızalanan ya da bakıma gönderilen cihazlar* için; bu cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin Şirket tarafından uygun görülen yöntemle yok edilmesi,
- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

çalışanlar, kaydın nasıl yok edileceğine ve yukarıda belirtilen yok etme yöntemlerine dair Veri Sorumlusu İrtibat Kişisi'nden tavsiye alabilirler.

1. Silme İşlemi

    1. Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi ile gerçekleştirilir. Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi,
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için İlgili kullanıcıların tespit edilmesi,

- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi,
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

1. *Bulut sunucu kullanan uygulamaların (Office 365 vb.) sunucularında yer alan kişisel veriler:* sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
2. *Fiziksel kayıtlarda yer alan kişisel veriler:* Fiziksel ortamda tutulan kişisel veriler arasında saklama süresi sona eren dokümanlar, evrak arşivinden sorumlu birim yöneticisi tarafından imha edilir veya hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
3. *Şirket sunucularında yer alan kişisel veriler*: Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır. Anılan işlem gerçekleştirilirken, ilgili kullanıcı aynı zamanda sistem yöneticisi ise, ilgili kişinin sistem yöneticisi yetkilerinin kaldırılması veya başka bir imha yöntemi gerçekleştirilmesi gerekir.
4. *Flash disk, harici HDD gibi taşınabilir medya ortamlarında yer alan kişisel veriler*, şifreli olarak saklanır ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.
5. *Veri tabanlarında bulunan kişisel veriler*, kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile ("delete" vb.) silinmesi suretiyle silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcı aynı zamanda veri tabanı yöneticisi ise ilgili kişinin veri tabanı yöneticisi yetkilerinin kaldırılması veya başka bir imha yöntemi gerçekleştirilmesi gerekir.
6. Anonim Hale Getirme

1. 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 uygulanması sonucunda elde edilen veriler, belirli bir kişiyi tanımlayamaz hale getirdiğinde anonim hale getirme gerçekleşmiş sayılır.

Kullanılabilecek anonim hale getirme yöntemlerinden bazıları örnek olarak aşağıda sıralanmıştır:

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:

1. *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. örneğin; kişilerin yaş, cinsiyet, posta kodu, gelir, din verilerinin yer aldığı bir tablodan "din" sütunun tamamen çıkartılması.

1. *Kayıtları çıkartma :* Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonim olma durumu 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; anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edildiyse, böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydın çıkartılması.

1. *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; bir tabloda yaş, cinsiyet ve meslek ayrımına göre hastalık durumunun belirtildiği düşünüldüğüne, bu tabloda yaş=3 olan kayıt bir çocuğa ait olduğundan istisnai bir durum yaratmakta ve tahmin edilebilirlik ve çocuğun ailesine dair varsayımlar yapılması riskini arttırmaktadır. Bu sebeple; bölgesel gizleme yöntemi ile bahsedilen kaydın yaş hanesi "bilinmiyor" olarak değiştirilirse, veri kümesine dair tahmin edilebilirlik riskinde azalma sağlanacaktır.

1. *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 numarası 12345678901 olan bir kişi e-ticaret platformundan bir ürün aldıktan sonra aynı zamanda başka bir ilişkili ürün de aldıysa, yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan ilk ürünü kişilerin %xx'i aynı zamanda ikinci ürünü de satın alıyor şeklinde bir sonuca ulaşılabilir.

1. *Alt ve üst Sınır Kodlama :* Alt ve üst sınır kodlama yöntemi belli bir değişken içi6.Saklama ve İmha Süreleri, Periyodikn 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. örneğin; kişilerin yıllık gelirlerinin yer aldığı bir tabloda yıllık gelirlerin birebir

yansıtılması yerine, alt sınırı 100.000, üst sınırı 120.000 alarak tabloda; 100.000 TL'den küçük ve eşit değerler, "düşük", 100.000 ve 120.000 arası değerler "orta", 120.000'den büyük ve eşit değerler "yüksek" olarak gruplandırılabilir.

1. *Global Kodlama:* Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya sayısal 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. örneğin; bir veri kümesinde tek bir birimdeki kadınların sayısına ait verinin meslek değişkeninde iki kategoride yığılma varsa (mesela o kümedeki kadınların çoğunluğu mimar veya mühendis ise) söz konusu iki kategorinin birleşiminden tek bir kategori elde edilebilir (ayrı ayrı "mimar" ve "mühendis" kategorileri yerine "mimar veya mühendis" adlı bir kategori üretilebilir).

1. *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 insanların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir insana dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan insanların 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 insanın nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

1. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

1. *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

Özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası

1. **Amaç**

İşbu özel Nitelikli Kişisel Verilerin İşlenmesi ve Korunması Politikası (Politika), şirketimizin belirlemiş olduğu, özel nitelikli kişisel verilerin işlenmesinde alınması gerekli önlemlere dair yürürlükteki mevzuata uyumunu temin etmeye yönelik prensipleri düzenlemektedir.

1. **Tanımlar**

İşbu Politika'da kullanılan terimler kendilerine aşağıda atfedilen anlamları haiz olacaklardır. Burada yer almayan tanımlar Kanun ve ikincil düzenlemelerde tanımlandıkları şekilde kullanılacaktır.

İki Kademeli Kimlik Doğrulama	Kişinin kullanıcı adı ve şifresi ile, dışarıdan ayrı bir kimlik doğrulama sisteminin (cep telefonu, kişisel soru, kriptografik anahtar vb.) birleşiminden oluşan doğrulama sistemini ifade eder.
Kayıtlı Elektronik Posta (KEP)	Elektronik iletilerin, gönderimi ve teslimatı da dahil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şeklini ifade eder.
Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kişisel Verilerin işlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.
özel Nitelikli Kişisel Veri (öNKV)	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
SFTP	Kriptografik ağ protokolü SSH kullanarak dosya transferi yapan bir dosya aktarım protokolüdür.
Sanal özel Ağ (VPN)	Sanal ağ uzantısı oluşturarak internet ya da başka bir açık ağ üzerinden özel bir ağa fiziksel olarak bağlıymışçasına o ağ üzerinden veri alışverişinde bulunmayı sağlayan bağlantı çeşidini ifade eder.
Sızma Testi	Bilişim sistemlerine mümkün olabilecek her yolun denenerek sızılmaya çalışma işlemlerini ifade eder.
Güvenli Ortam *(Secure vault)*	Hareketsiz değerli verinin okunmaya, değiştirilmeye ve taşınmaya karşı korunması amacıyla oluşturulmuş yazılım alanıdır.
Şirket	Veri Sorumlusu'nu ifade eder.
Uçtan Uca Şifreleme	Gönderilen iletinin şifrelenerek iletinin sadece gönderen ve gönderilen tarafça okunulmasını sağlayan şifreleme metotlarını ifade eder.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, Veri Kayıt Sistemi'nin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
Veri Sorumlusu İrtibat Kişisi	Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil

	düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.
	Veri Sorumlusu tarafından atanan ve Kanun'a uygun olarak Şirket kişisel veri envanterini oluşturan, güncel tutan ve gerekli değişiklikleri Veri Sorumlusu İrtibat Kişisine ileten şirket çalışanını ifade eder.
Veri Yetkilisi	Kişisel verilerin yer aldığı sistemlerde kullanıcıların erişim, kayıt oluşturma, görüntüleme, değiştirme gibi yetkilere sahip olup olmadıklarını gösteren bir matristir.

Yetki Matrisi

1. **Kapsam**

Kanun'un 12. maddesi uyarınca Şirket, veri sorumlusu olarak, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

Ayrıca, Kişisel Verileri Koruma Kurulu'nun (Kurul) "özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli önlemler" ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı (özel nitelikli kişisel verilere dair karar) uyarınca, kişisel verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması gerekmektedir.

İşbu Politika, Kanun ve özel nitelikli kişisel verilere dair ilke kararı uyarınca Şirket'in özel nitelikli kişisel verilerin işlenmesinde alması gereken önlemlere dair düzenlemeleri kapsar.

1. **özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken önlemlere Dair Esaslar**

    1. özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ve fiziki ortamlar envanterde belirtilir. özel nitelikli kişisel veriler yüksek risk içeren kişisel veriler olarak sınıflandırılır.
    2. özel nitelikli kişisel verilere erişim Şirket çalışanları ve alt-işveren çalışanları ile kısıtlıdır. Kanun'da öngörülen hukuki sebeplerin bulunması hali hariç, Şirket dışından hizmet sağlayıcılarına veya çalışanlarına özel nitelikli kişisel veri erişimi verilemez.
    3. Şirket çalışanlarının, kişisel verilerin ve özel nitelikli kişisel verilerin gizliliğine "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasını" imzalamış olmaları ve Kanun ve buna ikincil mevzuat ile özel nitelikli kişisel verilerin güvenliği konularında Şirket'in belirleyeceği eğitimi almış olmaları zorunludur. Şirket çalışanlarının farkındalığını arttırmak amacıyla Şirket bünyesinde kişisel verilerin korunmasına yönelik aktiviteler düzenler.
    4. özel nitelikli kişisel verilerin gizliliğine dair, tüm çalışanların uyması gereken prensipleri de içeren ve Şirket tarafından "Kişisel Verilerin Korunması ve İşlenmesi Politikası" ile "Kişisel Veri Saklama ve İmha Politikası" yayınlanmıştır.

Bunlarla birlikte, özel nitelikli kişisel verilerin gizliliğine dair uyulması gereken ana politika işbu politikadır.

5. Elektronik ortamda muhafaza edilen özel nitelikli kişisel veriler için,
    1. özel nitelikli kişisel verilerin kayıt edildiği kayıt ortamlarında kullanılacak kriptografik şifreleme metotları veya şifreleme sistemi içeren veri kayıt sistemi kullanılır.
    2. özel nitelikli kişisel verilerin aktarımlarında kullanılacak şifreleme yöntemleri en azından Uçtan Uca Şifreleme koruması içeren e-posta sistemlerinin kullanılması veya kurulumu sağlanır.
    3. Kriptografik anahtarlar güvenli ortamda *(secure vault)* tutulur.
    4. Veriler üzerinde gerçekleştirilen hareketlerin işlem kayıtları loglanır, zaman damgasıyla imzalanır ve güvenli ortamda erişim kontrolleri uygulanarak saklanır.
    5. üreticilerin yayınladığı güvenlik güncellemeleri veri sistemlerine uygulanır.
    6. Verilerin bulunduğu ortamlara ait güvenlik testleri yılda 1 kez yapılır ve test sonuçlarının kayıt altına alınması sağlanır.
    7. Verilere erişim için erişim yetki kontrol metotları uygulanır. Bu metotlar "Bilgi Sistemleri Erişim Kontrol Yönetim Politikasına" göre takip edilir.
6. Fiziksel ortamda işlenen, muhafaza edilen ve/veya erişilen öNKV için,
    1. özel nitelikli kişisel verilerin bulunduğu ortamlar ve nitelikleri her bir departman tarafından kişisel veri envanterinde belirlenir.
    2. özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre gerekli önlemlerin alındığından emin olunması gereklidir.
    3. Şirket, herhangi bir veri ihlali durumunda kanuni yükümlülüklerin yerine getirilebilmesi ve bu konudaki düzenlemelere uygun hareket edilebilmesi amacıyla "Kriz Müdahale Prosedürünü" işletmektedir.
    4. özel nitelikli kişisel verilerin bulunduğu tüm fiziksel ortamların güvenliğinin sağlanması için tüm ortamlara giriş çıkışlar kartlı sistem, şifreli sistem, parmak izi tarama, kilitli dolapta tutma vb. yöntemler ile kontrol altında tutulur ve yetkisiz giriş ve çıkışların engellenmesi sağlanır.
7. özel nitelikli kişisel verilerin aktarımında, aşağıda belirlenen aktarım yöntemleri uygulanır. Aktarım ancak özel nitelikli kişisel veri aktarmaya yetkili çalışanlar tarafından yapılır.

Aktarım yolu	**Aktarım yöntemi**
E-posta yoluyla aktarım	Şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılır.

Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarım	Kriptografik yöntemlerle şifrelenir ve kriptografik anahtar farklı ortamda tutulur
Farklı fiziksel ortamlardaki sunucular arasında aktarım	Sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımının gerçekleştirilir.
Kağıt ortamı yoluyla aktarım	Verilerin evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı belirlenen önlemlere uyulur ve evrak "çOK GİZLİ" kaydıyla ilgiliye gönderilir.

1. çalışanların özel nitelikli kişisel verilere dair tüm yetkileri (erişim ve varsa aktarım yetkisi dahil) görevlerinin sona erdiği an itibariyle kaldırılır. Bu kapsamda, erişimin sona erdirilmiş olduğuna, yetkilerin kaldırıldığına, fiziki ortamda tutulan evrakların yetkililere teslim edildiğine dair kayıtları tutulur ve bu kişilerin kullanımına verilen şirket envanterindeki her unsur geri alınır.

1. **Diğer Güvenlik önlemleri**

Alınacak diğer güvenlik önlemleri "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" ile "Kişisel Veri Saklama ve İmha Politikasında" belirlenmektedir.

1. **Diğer Hukuki Düzenlemeler**

Ayrıca, bu Politika'nın uygulanması açısından, Kişisel Verileri Koruma Kurumu'nun (Kurum) internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberi'nde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler başta olmak üzere, sektör uygulamaları, mesleki kurallar ve sair düzenlemeler de dikkate alınır.

Şirket, işbu Politika kapsamında, Kanun ve özel nitelikli kişisel verilere dair ilke kararının uygulanmasını sağlamak amacıyla gerekli denetimleri düzenli olarak yapar veya yaptırır.

1. **İhlalin Bildirimi**

Bir özel nitelikli kişisel verinin ihlal edilmesi halinde ve özel nitelikli kişisel veriler de dahil herhangi bir kişisel veri ihlali durumunda "Kriz Müdahale Dokümanı" süreci işletilir.

Kanun'un 12. maddesi uyarınca, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, Şirket bu durumu 72 saat içinde ilgilisine ve Kurul'a bildirmekle yükümlüdür.

1. **Uygulama**

8.1.Yayımlama : Bu Politika çalışanlara Veri Sorumlusu tarafından sunulacaktır.

8.2. Yürürlük Tarihi : Bu Politika yayımlandığı anda yürürlüğe girer.

8.3. Değişiklikler : Bu Politika'da gerçekleştirilecek değişikliklerin öncesinde, Veri Sorumlusu İrtibat Kişisi veya Veri Yetkilisi, Veri Sorumlusu'ndan talepte bulunabilir. Politika değişiklikleri Veri Sorumlusu tarafından yapılır.

1. **Saklama**

Veri Sorumlusu, bu Politika'yı yayınlamak ve saklamakla yükümlüdür. Her departman yöneticisi bu Politika'nın uygulanmasından sorumludur. Bu Politika'nın uygulanmasıyla ilgili olan sorular Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi"ne yönlendirilmelidir.

Çalışan Kişisel Verilerinin Korunması ve İşlenmesi Politikası

1. **Giriş**

İşbu Politika kapsamında, www.arkasturizm.com yer alan "Kişisel Verilerin Korunması ve İşlenmesi Politikasında" belirtilen kişisel verilerin kategorize edilmesine ek olarak çalışanların aşağıda belirtilen kategorilerdeki kişisel verileri işlenmektedir.

çalışan Bilgisi : çalışanların istihdamları süresince şirketin ve çalışanların ticari ve hukuki güvenliğinin sağlanması amacıyla yürütülen faaliyetler kapsamında işlenen kişisel veriler (araç bilgisi, eğitim bilgisi, medeni durum bilgisi, referans bilgisi dahil). *çalışan Adayı Bilgisi* : çalışan adaylarının işe alım süreçlerinde uygun pozisyon için değerlendirilebilmesine temel olacak bilgilerin elde edilmesine yönelik işlenen her türlü kişisel veri (askerlik durum bilgisi, eğitim bilgisi, referans bilgisi dahil). *Performans ve Kariyer Gelişim Bilgisi* : Veri Sorumlusu çalışanlarının performanslarının ölçülmesi ile kariyer gelişimlerinin Şirketimizin insan kaynakları politikası kapsamında planlanması ve yürütülmesi ve söz konusu faaliyetlerin denetimi amacıyla işlenen kişisel veriler.

çalışanların iş faaliyetlerine ilişkin kişisel verilerinin işlenmesi sonucunda elde edilen veriler üzerinden bir çalışan aleyhinde şikayet prosedürü veya disiplin süreci başlatılmadan önce, çalışanlara elde edilmiş verileri görme, bu veriler hakkında açıklamada bulunma ve savunma hakkı verilir.

Kişisel Verilerin Kategorize Edilmesi

çalışanların iş faaliyetleriyle ilişkili işlenen kişisel verileri, Kanun'un 5. maddesinde belirtilen şartlara ve 4. maddesinde öngörülen kişisel verilerin işlenmesi ilkelerine uygun olarak, hukuka uygun başka amaçlar için de işlenebilir. Bu amaçların neler olduğu konusunda da çalışanlar, uygun usullerle Veri Sorumlusu tarafından bilgilendirilir.

çalışanların İş Faaliyetlerine ilişkin Kişisel Veri İşlenmesi Sonucunda Elde Edilen Bilgilere Karşı çalışanlara Savunma Hakkı Verilmesi

Veri Sorumlusu, çalışanları; işle ilgili gerçekleştirmiş olduğu faaliyetleri kapsamında ne şekilde bir kişisel veri işleme faaliyetinde bulundukları (e-mail kontrolü, araç takip cihazları kullanımı, kamera ile izleme gibi), bu kişisel verilerin işlenme amaçları ve prosedürleri hakkında bilgilendirir.

Veri Sorumlusu; iş saatleri içerisinde iş ve işyeri kurallarına uygun davranılıp davranılmadığının ve çalışanın görevlerini gereği gibi yerine getirip getirmediğinin tespiti ve işyeri ortamında huzur

ve düzeni bozacak hareketler yapılıp yapılmadığının takibi ve benzeri amaçlarla çalışanın kişisel verilerini işlemekteyse ilgili çalışanları açıkça ve detaylı olarak bilgilendirmesi gerekir.

çalışanların kendi iş faaliyetleriyle ilgili işvereni tarafından hangi kişisel veri işleme faaliyetleri yürüttüğünden haberdar edilmeleri ve farkındalık oluşması için Veri sorumlusu nezdinde, çalışma ortamının doğasına uygun olarak uyarılar yerleştirilir.

çalışanların İş Faaliyetlerine ilişkin Kişisel Veri İşlenmesi Sonucunda Elde Edilen Kişisel Verilerin Başka Amaçlarla Kullanılması

Veri Sorumlusu, çalışanların hangi iş faaliyetleri özelinde ve hangi amaçlarla kişisel verilerini işlediklerini (e-mail kontrolü, araç takip cihazları kullanımı, kamera ile izleme gibi) tespit eder ve kişisel verilerin işlenme amaçları ile sağlanmak istenen sonuca uygun olacak kişisel veri işleme yöntemlerini belirlerler.

Veri sorumlusu kendi bünyelerinde gerçekleştirecekleri değerlendirme sonucu, çalışanların iş faaliyetleri özelinde gerçekleştirilecek kişisel veri işleme amaçlarının veya yöntemlerinin kişisel verilerin korunması kurallarına uygunluğunu sağlar.

Veri sorumlusu, çalışanların iş faaliyetleri özelinde gerçekleştirilecek kişisel veri işleme faaliyetlerinde görevli çalışanlarını kişisel verilerin korunması ve konuya ilişkin diğer mevzuat, ilgili mevzuat kapsamında dikkat edilmesi gereken hususlar ve Veri Sorumlusu'nun mevzuattan kaynaklanan yükümlülükleri konusunda bilgilendirilir. Bu faaliyetler neticesinde elde edilen kişisel verilere erişimi olan çalışanlar ile yapılan sözleşmelere ilave gizlilik ve güvenlik yükümlülükleri eklenir veya bu kişiler tarafından gizlilik politikaları/taahhütnameleri imzalanması sağlanır.

çalışanların İş Faaliyetlerine ilişkin Veri Sorumlusu'nun Kişisel Veri İşleme Faaliyetleri Hakkında Bilgilendirilmesi

Bu bölüm altında çalışanların Veri Sorumlusu faaliyetlerinin yürütülmesi esnasında gerçekleştirdikleri işlemler özelinde, hangi kişisel verilerinin işlenebileceğine ilişkin (iletişim, araç kullanımı vb.) hususlar ile bu konuda Veri sorumlusu tarafından uyulması gereken esaslar detaylandırılmaktadır.

çalışanların Hangi Amaçlarla Hangi İş Faaliyetleri özelinde Kişisel Verilerinin İşleneceğinin Belirlenmesi

çalışan verilerinin güvenliğini sağlamak için Veri sorumlusu gereken tüm makul önlemleri alır. Alınan önlemler yetkisiz erişim risklerini, kaza ile veri kayıplarını, verilerin kasti silinmesini veya verilerin zarar görmesini engelleyecek şekilde kurgulanır.

Veri sorumlusu, çalışanların iş faaliyetleri özelinde gerçekleştirilecek kişisel veri işleme faaliyetleri için şirket içinde sorumlu çalışanlar tayin eder. çalışanların bu kapsamda kişisel veri işleme faaliyetinden sorumlu olacak ve bu işleme neticesinde elde edilen kişisel verilere erişim yetkisi olacak çalışan sayısı olabildiğince sınırlı tutulur. Bu kapsamda Veri sorumlusu, mevcut durumda bu verilere erişimi gereksiz olan çalışanlar var ise bu çalışanların erişim yetkilerini kaldırır veya sınırlar. çalışanların kişisel verilerine sadece erişim ile yetkili olan kişilerin erişmesini sağlamak adına gereken fiziki güvenlik önlemleri alınır. Bu kapsamda ayrıca erişim yetkili kişilerin gereksiz yere geniş yetki sahibi olması engellenir.

Bilgi sistemleri üzerinde 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği, kimlerin

çalışanların kişisel verilerine eriştiğinin tespit edilmesini sağlayacak denetim izi gibi önlemler alınır. Bu kapsamda oluşturulacak erişim kayıtları düzenli olarak kontrol edilir ve yetkisiz erişimlere yönelik soruşturma mekanizmaları oluşturulur.

çalışanların kişisel verilerine erişimi olan diğer çalışanların gerekli güvenlik kontrollerinden geçirilmeleri esastır. Bunun yanında bu kişilerin gerekli korumaları sağlayan gizlilik sözleşmesi/taahhütnamesi imzalaması veya iş sözleşmelerinde bu kapsamda hükümlere yer verilmesi ve bu kişilerin sorumlulukları hakkında sürekli olarak eğitilmesi sağlanır.

çalışanlara ait kişisel verilerin dizüstü bilgisayarlar gibi çeşitli vasıtalarla işyerinden çıkarılması halinde gerekli güvenlik önlemlerinin alınması ve bu önlemler hakkında ilgili çalışanların bilgilendirilmesi sağlanır.

çalışanların İşyerinde Gerçekleştirdiği Faaliyetlere İlişkin Kişisel Verilerin İşlenmesi Kişisel Verilerin Güvenliği

Veri Sorumlusu, çalışanların kişisel verilerinin işlenmesi konusunda dış hizmet sağlayıcılar kullanabilirler. Ancak Veri Sorumlusu dış hizmet sağlayıcılar konusunda aşağıdaki önlemleri almak zorundadır:

Dış hizmet sağlayıcının ilgili mevzuatın ve sektör uygulamalarının gerektirdiği teknik ve idari güvenlik önlemlerini almış olduklarının kontrol edilmesi, Dış hizmet sağlayıcının ilgili mevzuatın ve sektör uygulamalarının gerektirdiği teknik ve idari güvenlik önlemlerini almış olduklarını belirli aralıklarla denetlenmesi, Dış hizmet sağlayıcı ile gerekli teknik ve idari güvenlik önlemlerinin alınmasına yönelik şartlar içeren sözleşme yapılması, Kişisel verilerin yurtdışındaki dış hizmet sağlayıcılarına gönderilmesi halinde gerekli hukuki, idari ve teknik önlemlerin alınması.

Veri sorumlusu, çalışanların kişisel verilerini işlendikleri amaç için gerekli olan süre ve ilgili faaliyetin tabi olduğu yasal mevzuatta öngörülen minimum sürelere uygun olarak muhafaza etmektedir.

Bu kapsamda, Şirketimiz öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmaktadır. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır. Kişisel veriler belirlenen saklama sürelerinin sonunda periyodik imha sürelerine veya veri sahibi başvurusuna uygun olarak ve belirlenen imha yöntemleri (silme ve/veya yok etme ve/veya anonimleştirme) ile imha edilmektedir.

Kişisel Verilerin İşlenmesi Konusunda Dış Hizmet Sağlayıcı Kullanımı

Yıllık raporlar, yayınlar ya da internet siteleri gibi mecralarda bazı çalışanların isimlerinin ve diğer kişisel verilerin yayınlanması halinde, bu durumlar özel olarak değerlendirilir ve açık rıza alınması gereksinimi olup olmadığı belirlenir. Açık rıza alınması gerektiğine kanaat getirilmesi halinde ilgili çalışanların açık rızası kişisel verilerin yayınlanmasından önce alınır. Açık rıza alınması sırasında paylaşılacak kişisel veri tipleri tek tek çalışana bildirilir.

çalışanların Kişisel Verilerinin Saklanma Süresi

Veri sorumlusu, çalışanların kişisel verilerini ancak aşağıdaki şartlara dikkat ederek yayınlayabilirler:

Kişisel verilerin yayınlanması için hukuki bir hak veya yükümlülük bulunması veya çalışanın yayınlama için açık rıza vermiş olması, Kişisel verilerin yayınlanmaya açıkça elverişsiz olmaması.

Veri sorumlusu, kişisel verilerin yayınlanması neticesinde elde edilecek faydalar ile çalışanların gizliliğinin korunacağına ilişkin beklentileri dengeleyici bir yaklaşım ile hareket ederler.

çalışanların kişisel verilerinin üçüncü kişilerle paylaşılması halinde verilerin paylaşılmasından önce, veri paylaşımının Kanun'da yer alan şartlardan birisine dayalı olması aranır.

çalışanların, daha önce bilgilendirilmemiş ise, en geç paylaşım anında bu paylaşım ile ilgili olarak bilgilendirilmesi sağlanır. Ancak bu bilgilendirme hukuka aykırılık yaratıyorsa veya yetkili makamların yapacağı bir soruşturma hakkında önceden uyarı niteliği taşıyorsa ilgili çalışan konuya ilişkin bilgilendirilmez.

Rutin olarak gerçekleştirilmeyen çalışanların kişisel verilerinin şirket dışı paylaşım talepleri ve bu kapsamda yapılan paylaşımlar Veri sorumlusu tarafından kayıt altına alınabilir. Bu kapsamda asgari olarak paylaşıma onay veren kişi, paylaşım talebinde bulunan kişi, paylaşım gerekçesi, paylaşım tarih ve saati ile paylaşılan veri tipleri kayıt altına alınır. Bu kayıtların düzenli olarak kontrol edilmesi ve incelenmesi sağlanır.

Kişisel Verilerin Yayınlanması Kişisel Veri Paylaşımına ilişkin Bilgilendirme ve Kayıt Tutma Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkansızlık nedeniyle rızasını açıklayamayacak durumdaysa veya rızasına hukuki geçerlilik tanınmıyorsa; Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise, Hukuki bir yükümlülüğün yerine getirilmesi 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, ilgili grup şirketlerinin meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

Veri sorumlusu, çalışanların kişisel verilerinin paylaşımına ilişkin iç prosedürlerini belirler. Veri paylaşım taleplerinin bu konuda yetkin çalışanlarca cevaplanması sağlanır.

Şirket dışından gelen veri paylaşım taleplerinin (adli makamlar, idari makamlar, sigorta şirketi talepleri gibi) gerçekliği ve doğruluğunun teyidi konusunda gerekli önlemler alınır. Şirket dışından gelen veri paylaşım taleplerinin yazılı olarak gerçekleştirilmesi esastır.

çalışanların kişisel verilerinin gelen talep üzerine yurtdışına gönderilmesi halinde kişisel verilerin yurtdışına aktarılmasına ilişkin her türlü idari, hukuki ve teknik önlem alınır.

çalışanların kişisel verilerinin paylaşılması hukuki bir yükümlülük teşkil ediyorsa, yalnızca bu hukuki yükümlülüğün kapsamına uygun şekilde kişisel veri paylaşımı yapılabilir.

Uluslararası veri aktarımı ve özel nitelikli kişisel verilerin aktarımına ilişkin kanuni şartlar saklı kalmak kaydıyla; çalışanların kişisel verileri ancak aşağıdaki şartlardan birisinin varlığı halinde üçüncü kişilere aktarılabilir:

Veri sahibinin açık rızasının olması, Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise, Kişisel Veri Paylaşımına İlişkin Genel Kurallar

Veri sorumlusu, çalışanların kanuni haklarını kullanabilmelerini, gerekli başvuruların yapılabilmesini ve yapacakları başvurulara en geç 30 gün içerisinde cevap verilmesini sağlayacak her türlü idari, hukuki ve teknik önlemleri alır ve ilgili süreçleri tasarlayarak bu konuda çalışanları bilgilendirirler.

Veri sorumlusu tarafından kanuni haklarını kullanan çalışanlara verilecek cevaplarda üçüncü kişilerin kişisel verilerinin ifşa edilmemesi için gereken her türlü özen gösterilir.

çalışanların Kişisel Verilerinin üçüncü Kişilerle Paylaşımı çalışanların Kanuni Haklarını Kullanmalarına ilişkin Esaslar

çalışanlar aşağıda yer alan haklara sahiptirler:

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 halinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde 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 halinde zararın giderilmesini talep etme. çalışanların Kanuni Hakları

Veri sorumlusu tarafından çalışanlara araç tahsis edildiği durumlarda; tahsis edilen araçların kat edilen mesafenin belirlenmesi, akaryakıt kullanımı ölçümü, konum verisinin alınması ve benzeri amaçlarla takibi yapılabilir. Bu takip ile ilgili çalışanlar önceden bilgilendirilir.

çalışanların Kendileri Hakkında Toplanan Kişisel Verilere İlişkin Kanuni Hakları

Veri sorumlusu, işyerlerinin güvenliğini sağlamak amacıyla çeşitli noktalara güvenlik kameraları yerleştirebilmektedir. Bu güvenlik kameralarının görüntü alanlarının tüm işyerini değil; sadece özel risk taşıyan alanları, giriş - çıkış ve benzeri alanları kapsamasına özen gösterilir. Veri sorumlusu, çalışanları güvenlik kamerası ile çekim yapılan, güvenlik kameraları ile izlenen alanlar ve izlemenin amaçları hakkında bilgilendirmeye özen gösterir.

Şirket Tarafından Sağlanan Araçların Takibi

çalışanların iş faaliyetleriyle bağlantılı gerçekleştirdiği elektronik haberleşme işlemlerine ilişkin kişisel verilerin işlenmesiyle ilgili esaslar Veri Sorumlusu'nun " Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasında" belirtilmiştir.

İş Yerinde Güvenlik Kamerası Uygulaması

Veri Sorumlusu, çalışanların kişisel verilerine sadece disiplin soruşturmasının varlığı sebebiyle keyfi olarak erişilmesine engel olur. Bu kapsamda kişisel verilerin elde edilme amaçlarına uygun düşmüyorsa veya soruşturma konusunun ciddiyetine göre kişisel verilere erişmek orantısız bir işlem olarak değerlendiriliyorsa salt disiplin soruşturması nedeniyle çalışanların kişisel verilerine erişilemez.

çalışanların İş Faaliyetleriyle Bağlantılı Gerçekleştirdiği Elektronik Haberleşme İşlemlerine İlişkin Kişisel Verilerin İşlenmesi

Veri sorumlusu, disiplin soruşturmaları sırasında da çalışanların kişisel verilerinin korunmasına ilişkin yükümlülüklere aynen uymak zorundadırlar. Bu kapsamda özelikle aşağıdaki aksiyonlar alınır:

Disiplin soruşturmalarına ilişkin politika ve prosedürlerin kişisel verilerin korunmasına ilişkin yükümlülüklerle uyumlu hale getirilmesi, Disiplin soruşturmaları kapsamına giren kişisel verilere de çalışanların kişisel verilerine erişme hakkı kapsamında erişilebileceği konusunda disiplin soruşturmaları yapmaya yetkili kişilerin bilgilendirilmesi, Disiplin soruşturmaları sırasında hukuka aykırı yöntemlerle kişisel veri elde edilmemesini sağlayacak önlemlerin alınması, Disiplin soruşturmaları sırasında kullanılacak olan kişisel verilerin doğru ve güncel olmasına dikkat edilmesi, Disiplin soruşturmasına ilişkin kişisel verilerin ve kayıtların güvenli şekilde saklanması, çalışanlar hakkındaki asılsız iddiaların, eğer bunların silinmemesi için herhangi bir hukuki sebep bulunmuyorsa, çalışanların dosyalarından silinmesinin sağlanması.

Şirket birleşme ve devralmaları da dahil şirket yapısını değiştiren tüm işlemler bu bölüm altında değerlendirilmektedir.

Veri sorumlusu, şirket yapısı değişikliği amacıyla çalışanların kişisel verilerini paylaşma gereksinimi duyduklarında; öncelikle bu kişisel verilerin mümkün olduğu ölçüde anonimleştirilerek paylaşılmasını sağlar.

Anonimleştirilerek paylaşılması mümkün olmayan çalışan kişisel verileri için karşı taraftan sadece şirket yapısı değişikliği ile ilgili işlemleriyle sınırlı olarak bu kişisel verileri kullanacağı, kişisel verilerin Kanun'un veri güvenliği hükümleri uyarınca korunacağı ve Kanun'un ilgili hükümlerine uygun olarak işleneceği, kişisel verilerin üçüncü kişilere aktarılmayacağı ve ilgili işlemler tamamlandıktan sonra kişisel verilerin silineceği veya yok edileceğini konularında taahhüt alınır.

Disiplin Soruşturmalarında çalışanların Kişisel Verilerinin İşlenmesi Şirket Birleşme ve Devralmaları İle Şirket Yapısını Değiştiren Diğer İşlemlerde çalışanların Kişisel Verilerinin İşlenmesi

Veri sorumlusu, çalışanların usulsüz işlemlerini engellemek adına değişik birimlerde bulunan kişisel veri setlerini karşılaştırabilir. Usulsüzlüklerle mücadele kapsamında yapılacak kişisel veri seti karşılaştırma işlemleri için kurallar veri sorumlusu tarafından belirlenir. Veri sorumlusu usulsüz işlemlerin tespiti amacıyla çalışanlarının kişisel verilerini ancak aşağıdaki koşullar veya benzeri koşullardan birinin varlığı halinde paylaşır:

Hukuken ilgili çalışanın kişisel verilerinin paylaşılmasının zorunlu olması, çalışanın kişisel verilerinin paylaşılmaması halinde bir suçun önlenmesinin ya da tespit edilmesinin mümkün olmayacağına dair güçlü şüphe bulunması, Veri Sorumlusu, Politika ve Prosedürlerinin gereği gibi uygulanabilmesi için veri paylaşımının gerekli olması

Veri sorumlusu çalışanlar arasında fırsat eşitliğini sağlamak amacıyla gerekli olduğu ölçüde kişisel veri işleyebilir. Bu kapsamda Veri sorumlusu, işe alım, terfi, çalışma koşulları, şirket içi kariyer planlama ve geliştirme gibi süreçlerdeki eşitsizlikleri tespit ederek ve eşitlikçi uygulama örnekleri belirleyerek çalışanları arasındaki fırsat eşitliğinin sağlanmasını amaçlar. İş yaşamında kadın-erkek eşitliğinin sağlanabilmesi, bu kapsamda gerek yasal olarak zorunlu olan (emzirme odası, kreş açılması gibi), gerekse Veri sorumlusu tarafından tespit edilen uygulamaların hayata geçirilmesi amaçlarıyla kişisel veri işlenebilir.

Fırsat eşitliğinin sağlanması için işlenen kişisel veriler belirli aralıklarla kontrol edilir. Fırsat eşitliğinin sağlanması amacıyla işlenen kişisel veriler mümkün olan en geniş kapsamda anonimleştirilerek kullanılır.

Usulsüzlüklerle Mücadele Kapsamında çalışanların Kişisel Verilerinin İşlenmesi

özel sağlık sigortası, hayat sigortası, ferdi kaza sigortası, şirket aracı, bireysel emeklilik, esnek yan fayda programı ya da benzeri faydalar bu başlık altında yan haklar ve menfaatler olarak adlandırılır.

Veri sorumlusu, çalışanların kişisel verilerinin çalışanlara yan haklar ve menfaatler sağlamak için hizmet alınan üçüncü kişilerle paylaşılmasında, asgari düzeyde veri paylaşmaya özen gösterir. Bahsi geçen üçüncü kişilerle sadece, ilgili yan hak ve menfaatin sağlanması için zorunlu olan kişisel veriler paylaşılır. Ayrıca, bu kapsamda toplanan kişisel verilerin başka bir amaçla kullanılmaması için gerekli tedbirler alınır.

Hizmet alınan üçüncü kişilerle paylaşılacak kişisel verilerin özel nitelikli kişisel veri olup olmadıkları paylaşımdan önce değerlendirilir.

Hizmet alınan üçüncü kişiler ile yapılacak kişisel veri paylaşımları hakkında çalışanların bilgilendirilmesi sağlanır. Bu kapsamda, çalışanların hangi kişisel verilerinin paylaşıldığı ve bunların ne amaçla kullanılacağı çalışana açıklanır.

Fırsat Eşitliğinin Gözetilmesi Kapsamında çalışanların Kişisel Verilerinin İşlenmesi Yan Haklar ve Menfaatlerin Sağlandığı Durumlarda çalışanların Kişisel Verilerinin İşlenmesi

Veri Sorumlusu, çalışan kişisel verilerinin bahsi geçen amaçlarla işlenmek üzere Kanun ve ilgili mevzuat kapsamında öngörülen bilgilendirmeleri yapacak ve gerekmesi halinde ilgili açık rızaları temin edecektir.

çalışanların Kişisel Verilerinin İşlendiği özel Durumlar

Veri Sorumlusu, aşağıda belirtilen amaçlarla çalışan kişisel verilerini temin etmekte ve işlemektedir:

Veri Sorumlusu'nun çalışanlarının performans değerlendirme kriterlerinin belirlenmesi ve takibi süreçlerine destek olunması, Veri Sorumlusu'nun yabancı çalışanlarının çalışma/oturma izni başvuru süreçlerine destek olunması, Veri Sorumlusu'nun çalışanlarına sağlanan yan hakların ve menfaatlerin planlanması ve takibi süreçlerine destek olunması, Veri Sorumlusu çalışanlarının ücret yönetimi ve prim süreçlerinin planlanması ve icrası konusunda Veri Sorumlusu'na destek olunması, Stratejik insan kaynaklarının planlanması, yedekleme süreçleri ve organizasyonel gelişim faaliyetleri konusunda destek olunması, üst düzey yöneticilerinin atama, terfi ve işten ayrılma kararlarının uygulanması ve ilgili duyuruların yapılması, üst düzey yöneticilerinin ücret ve prim paketlerinin belirlenmesi konusunda destek olunması, çalışan bağlılığının ölçümlenmesi süreçlerinin planlanması ve yürütülmesine destek olunması, Veri Sorumlusu'nun çalışanlarının kariyer gelişimi, eğitim ve yetenek yönetimi faaliyetlerinin planlanması ve icrası süreçlerine destek olunması, İşe alım süreçlerine destek olunması, Şirketler ve ortaklık hukuku işlemlerinin gerçekleştirilmesi konusunda destek olunması, Veri Sorumlusu'na tabi olduğu mevzuata uyum konusunda destek olunması, Topluluk itibarının korunmasına yönelik çalışmaların, sürdürülebilirlik ve sosyal sorumluluk çalışmalarının yürütülmesi, Veri Sorumlusu'nun genelinde etkinlikler düzenlenmesi, Veri Sorumlusu

faaliyetlerinin diğer Veri Sorumlusu politikalarına ve ilgili mevzuata uygun olarak yürütülmesi konusunda denetim faaliyetlerinin yürütülmesi, Veri Sorumlusu'nun çalışanlarına yönelik iletişim, haberleşme faaliyetlerinin yürütülmesi, çalışan memnuniyeti ve bağlılığının sağlanması süreçlerinin yürütülmesi.

Veri Sorumlusu, sağlık kontrollerinin ve testlerin hangi amaçla gerçekleştirildiği konusunda çalışanları açıkça bilgilendirir.

Veri Sorumlusu hiçbir şekilde çalışandan gizli bir şekilde ona ait biyometrik/genetik numunelerini (parmak izi, saç teli vs.) toplayamaz. Kanuni sebeplere dayalı olarak gerçekleştirilen faaliyetler istisna oluşturur.

çalışan Verilerinin İşlenme Amaçları

Veri Sorumlusu adına Veri Sorumlusu Sağlık Yetkilileri, iş sağlığı ve güvenliği programı kapsamında tıbbi muayene ve testler aracılığıyla çalışanlara ait sağlık verilerini toplayabilir.

Veri sorumlusu, muayene ve testlerin hangi amaçlarla yürütüleceğini önceden belirler. Veri sorumlusu, amaçlarını da göz önünde bulundurarak kişinin sağlık verilerine daha az müdahil olunabilecek yöntemleri izler. örneğin, çalışanın sağlık verilerini öğrenmek için muayene sonuçlarına bakmak yerine sağlık anketi yapabilir.

Muayeneden Elde Edilen Numunelerin Belirtilen İşleme Amacı Dışında Kullanılmaması

Veri Sorumlusu, işe alınması muhtemel olan adayların söz konusu işe uygun olup olmadığına karar vermek için ilgili adaya testler yapılmasını talep edebilir. Bu testleri aynı zamanda herhangi bir kanuni yükümlülüğünü yerine getirmek için veya muhtemel çalışanın tabi olacağı sigorta türünü belirlemek için de yapabilir.

Veri Sorumlusu, muayene ve testlerin hangi amaçlarla yürütüleceğini önceden belirler.

Veri Sorumlusu, amaçlarını da göz önünde bulundurarak kişinin sağlık verilerine daha az müdahil olunabilecek yöntemleri izler.

İşe alım sürecinde tıbbi muayene veya sağlık testi sadece kişinin gerçekten işe alımı kesin ise (sağlıkla ilgili ilgili işi yapmasına engel bir durum çıkmadığı sürece) yapılır.

Veri Sorumlusu, iş başvurusu sürecinin ilk zamanlarında, işe alınma ihtimalinin yüksek olması halinde sağlık muayenesi veya testi yapılabileceğine dair adayı bilgilendirir.

çalışanların Muayene ve Testler Aracılığıyla Sağlık Verilerinin Toplanması

Veri Sorumlusu, çalışanların sağlık verilerinin işlenmesine ilişkin izlenen politikaların şeffaf olmasına özen gösterir.

Veri Sorumlusu; sağlık testlerinin yapılacağı yerlere, testlerin niteliğine, test sonucu elde edilen verilerin nasıl kullanılacağı ve korunacağına ilişkin şartları belirler. Bu şartlar hakkında çalışanları bilgilendirmeye özen gösterir.

İşe Alınması Muhtemel Olan Adayların Muayene ve Testler Aracılığıyla Sağlık Verilerinin İşlenmesi

Genel prensip olarak Veri Sorumlusu'nun yetkilendirdiği sır saklama yükümlülüğüne haiz işyeri hekimi, hemşire vb. yetkili kişiler (Veri Sorumlusu Sağlık Yetkilileri), muayene ve testlerden elde edilen sağlık verilerinin işlenmesinden sorumludur. Bu verilerin toplanmasına ve işlenmesine

ilişkin esaslar için "özel Nitelikli Kişisel Verilerin İşlenmesi Ve Korunması Politikası" hükümleri uygulanacaktır.

Sağlık Verilerinin İşlenmesine İlişkin Şirket Politikasının çalışanlara Bildirilmesi

Sağlık verilerinin paylaşımında özel nitelikli kişisel veriler için getirilen yasal yükümlülükler dikkate alınarak ve bu yükümlülüklere uygun olarak bu paylaşım işlemleri yürütülür.

Veri Sorumlusu, çalışanların sağlık verileri ile ilgilenen kişilerin yukarıdaki durumlar hakkında bilgilendirilmesini ve eğitilmesini düzenli aralıklarla sağlar. Ayrıca Veri Sorumlusu'nun kişisel verilerin korunması konusunda görevlendirilen yetkililerinden gerekli desteği alabilmesine yönelik düzenlemeler yapılır.

Veri Sorumlusu, kural olarak, çalışanların sağlık verilerini diğer çalışanların erişimine açmazlar. Ancak kanunen zorunlu olması halinde hukuken Veri Sorumlusu'nun meşru menfaatleri gereği bir işin ve bu işle ilgili olarak da bu verilerin işlenmesi zorunlu ise; bu işle görevli olan personelin işin gereğini yerine getirmekle sınırlı olmak kaydıyla bu kişisel verileri işlemeleri için gerekli idari ve teknik tedbirler alınarak kendilerine erişim hakkı sağlanır.

Muayene ve Testlerden Elde Edilen Sağlık Verilerinin İşlenmesi

çalışanların sağlık verilerini işleyecek veya işlemeye yetkilendirecek Veri Sorumlusu çalışanlarının ilgili mevzuat ve oluşturulan gizlilik politikası hakkında bilgi sahibi olması sağlanır.

çalışanın sağlık verileri bu işi yapmaya yetkin kişiler tarafından analiz edilir. Veri Sorumlusu, çalışanlara, sağlık verilerinin hangi amaçlar çerçevesinde kullanıldığını ve bu verilere kimin, ne amaçla eriştiğini anlaşılır bir biçimde bildirmeye özen gösterir.

Sağlık Verilerinin Paylaşımı ve Bu Verilere Erişim

Veri sorumlusu, çalışanlara yapılacak sağlık anketlerinde, sadece gerçekten gereken bilgilerin toplandığından emin olur ve gereksiz bilgi talep edilmemesi hususuna özen gösterir.

Veri sorumlusu, çalışanlardan tüm sağlık verilerini şirket ile paylaşması için genel bir açık rıza vermesini isteyemez. Şirketler, sadece belirtilen amaç için gerçekten gerekli olduğu düşünülen sağlık verilerinin şirketle paylaşılmasını isteyebilir.

Sağlık Verilerini İşleyecek Kişilerin Belirlenmesi

Sağlık verileri, özel nitelikli kişisel veriler arasında yer almaktadır. Başta çalışanların kaza ve hastalık raporları olmak üzere çalışanların sağlık verileri, diğer kişisel verilerinden ayrı olarak saklanır. çalışanın işe gelmediği günlere ya da karıştığı kaza ve diğer olaylara ilişkin bilgiler kullanılırken çalışanın sağlık verilerinin kullanılmasından mümkün olduğunca kaçınılır.

Sağlık Verilerinin Belirtilen Amaçla Bağlantılı, Sınırlı ve ölçülü Olarak İşlenmesi çalışanların Sağlık Verilerinin İşlenmesine İlişkin Genel Yaklaşım

1. Sağlık Verilerinin Zorunlu Olmadıkça İşlenmemesi ve Ayrı Saklanması

çalışanların Sağlığına İlişkin Veriler

Kişisel verilerin bir kısmı, KVK Kanunu kapsamında "özel nitelikli kişisel veri" olarak ayrı şekilde düzenlenmekte ve özel bir korumaya tabi olmaktadır. özel nitelikli kişisel 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 mahkumiyeti ilgili veriler ile biyometrik ve genetik verilerdir.

Veri sorumlusu, sağlık verilerini, çalışanın açık rızası bulunmayan durumlarda Kişisel Verileri Koruma Kurulu tarafından belirlenecek olan yeterli önlemlerin alınması kaydıyla aşağıdaki durumlarda işleyebilir:

çalışanın sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri, sadece kanunlarda öngörülen hallerde, çalışanın sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise 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 eliyle; çalışanın açık rızası bulunması durumunda işleyebilir.

Veri sorumlusu, çalışanların kişisel verilerinin güncelliğini sağlamak adına gerekli önlemleri alır. Bu kapsamda; çalışanların, değişme ihtimali olan kişisel verileri (adres, telefon, aile/yakın bilgisi vb.) tespit edilir, değişme ihtimali olan kişisel verilerin elektronik ortamda herkes tarafından değil; sadece ilgili çalışanın kendisi ve diğer erişim yetkilileri tarafından görülmesi sağlanır, çalışanların değişme ihtimali olan kişisel verileri elektronik ortamda görmesi imkanı bulunmuyorsa; bu kişisel verilerin fiziki ortamda gösterilebilmesi için gereken tedbirler alınır; çalışanların değişme ihtimali olan kişisel verilerini güncel tutmaları sağlanır.

Bu yöntemler haricinde veri sorumlusu; kendine özgü koşullara göre çalışanların işlenmekte olan kişisel verilerini güncel tutmak için gerekli önlemleri alır.

özel Nitelikli çalışan Verilerinin İşlenmesi

Veri sorumlusu, mutlaka açık ve öngörülebilir bir ihtiyaç üzerine çalışanlardan kişisel veri toplar, toplanan verilerin bahsi geçen ihtiyaçları karşılama konusunda elverişli olmasını sağlar.

Yukarıda belirtilen prensibe uyumluluğu sağlamak amacıyla çalışanların kişisel veri girişi yaptığı her türlü form ve girdi yöntemi denetlenir. Bu denetim, mevcut form ve girdi yöntemleri için en kısa sürede; yeni oluşturulacak form ve girdi yöntemleri için bunların kullanılmasına başlanmadan önce tamamlanır.

Yapılacak denetim neticesinde gereksiz veri toplanmasını sağlayan kısımlar ilgili form ve girdi yönteminden çıkarılır.

Kişisel Verilerin Güncelliğinin Sağlanması

Bu şartlardan en az birisinin varlığı halinde kişisel veri işleme faaliyeti gerçekleştirilebilir. Veri işleme faaliyeti, şartlardan birisine veya birden fazlasına dayalı olarak gerçekleştirilebilir.

Açık rıza alınması gereken durumlarda, söz konusu açık rıza alma işlemi, kişisel verilerin işlenmesinden önce tamamlanır.

Veri sorumlusu, kişisel verilerinin saklanması, kullanılması ve paylaşılmasına ilişkin olarak çalışanların bilgilendirilmesi konusunda, kendilerine özgü şartlara göre en faydalı yöntemi tespit eder ve uygular.

İhtiyaçlar Doğrultusunda Gerektiği Kadar Kişisel Veri Toplanması

Veri sorumlusu, çalışanlarını; kendileri hakkında işlenen kişisel verilerin hangileri olduğu, kişisel verilerin hangi amaçlarla ve sebeplerle işleneceğini, kişisel verilerin hangi kaynaklardan

toplandığını, bu kişisel verilerin kimlerle paylaşılacağı ve nasıl kullanılacağı hakkında bilgilendirir.

Veri sorumlusu, işledikleri kişisel verileri değerlendirerek, Kanun'da yer alan şartlardan en az birisine dayalı olarak bu verileri işlerler. Bu şartlar;

çalışanın açık rızasının olması, Veri işlemenin ilgili kanunlarda açıkça öngörülmesi, Fiili imkansızlık sebebiyle çalışanın açık rızasının alınamaması, Veri işlemenin bir sözleşmenin kurulması veya ifasıyla doğrudan ilgi olması, Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması, Kişisel verinin kişisel veri sahibinin kendisi tarafından alenileştirilmiş olması, Bir hakkın tesisi veya korunması için veri işlemenin zorunlu olması, Meşru menfaate dayalı olarak verilerin işlenmesidir. çalışanların Kişisel Verilerinin İşlenmesinde Genel Yaklaşım

1. çalışanların Bilgilendirilmesi ve Kişisel Veri İşleme Şartları

Veri sorumlusu başarıyla sonuçlanmayan başvuruları ileride açılabilecek pozisyonlar için değerlendirmek isterlerse, kayıtlarda adayların kişisel verilerini tutabilirler. Bu amaçla kişisel veri tutulacaksa; iş başvuru formunda veya ek açıklayıcı belgelerde adayları bu konuda bilgilendirir ve talep etmeleri durumunda bilgilerin kayıtlardan silinebileceğini belirtirler.

çalışan Verilerinin İşlenmesi

Veri sorumlusu açık pozisyona kabul edilen başarılı adayların özlük dosyalarına, adaylık süreci boyunca elde edilen kişisel verilerden hangi verilerin aktarılacağını özenle belirler.

Başvurusu Kabul Edilmeyen Adayların Kişisel Verileri

Veri sorumlusu işe alım sürecine ilişkin kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini engellemek adına her türlü teknik, idari ve hukuki tedbiri alır.

Veri sorumlusu işe alım sürecine ilişkin adayın kişisel verilerini, bu verilerin işlenme amaçlarına uygun olan bir süre boyunca saklar. İş hukuku ve diğer ilgili düzenlemelere uyumlu olarak, işlenmesini gerektiren sebeplerin ortadan kalkması durumunda, kişisel veriler, veri sorumlusu tarafından veya adayın talebi üzerine silinir, yok edilir veya anonim hale getirilir.

Geçerli bir sebep olmadığı takdirde (muhtemel uyuşmazlıkların çözümü gibi), veri sorumlusu ilgili kişisel verileri işe alım sürecinden dolayı doğabilecek taleplerin zamanaşımı süresi bitiminden sonra muhafaza etmezler.

İşe alım sürecinde adayın durumu hakkında araştırma yapılmış veya herhangi bir şekilde üçüncü kişilerden veri temin edilmiş ise, üçüncü kişilerden elde edilen bilgiler en kısa sürede silinir.

İşe Alınan Adayların çalışan Kayıtlarına Aktarılması Gereken Kişisel Verileri

İşe alım sürecinde Veri sorumlusu, çalışanların kişisel verilerinin korunmasına ilişkin gösterdiği özeni aynı şekilde işe başvuran adaylara da gösterir. Bu kapsamda; başvurular dijital ortamda iletiliyor ise, veri sorumlusu güvenli bir sistem kullanır, elektronik ortamda iletilen başvurular sadece işe alım sürecinden sorumlu olan kişiler tarafından erişilebilen dizin veya sistemlere kaydedilir, başvurular posta ve faks aracılığıyla iletiliyor ise, insan kaynaklarından sorumlu yetkili kişiye başvuruların iletilmesi sağlanır. Elde edilen fiziki belgelerin güvenliği sağlanır.

Veri sorumlusu adayların kişisel verilerine erişimi, işe alım süreçlerini yürütmekle görevli olan kişilerle sınırlar. Söz konusu kişiler, adaylara ait kişisel verilerin işlenmesi ile alınacak güvenlik önlemleri hakkında düzenli aralıklarla bilgilendirilir.

İşe Alım Sürecine ilişkin Kişisel Verilerin Saklanma Süresi

Araştırma sırasında üçüncü bir kişiden bilgi ve belgenin toplanması adayın rızasına bağlı ise veri sorumlusu adaydan açık rıza almalıdır. üçüncü kişinin adaydan açık rıza alması yerine, doğrudan adaydan alması yöntemi mümkün olduğunca tercih edilir.

Adayların Kişisel Verilerinin Saklanması ve Güvenliği

Veri sorumlusu aday hakkında araştırma yaparken; önceki iş tecrübeleri ve eğitim sürecinde yer alan ve adayla bire bir iş/eğitim ilişkisi bulunan kişilere ulaşılır. Araştırma sonucu elde edilen bilgi, kaynağın güvenilirliğine göre değerlendirilir, hiçbir istihdam kararı güvenilirliği şüpheli olan bir kaynağa dayanmaz. Veri sorumlusu, kendi bünyesindeki ilgili çalışanı veya araştırmayı üstlenecek olan kişileri araştırma yöntemi hakkında bilgilendirir, araştırma sırasında adaydan farklı bir kişiye ilişkin kişisel veri elde edilmemesine özen gösterir.

Araştırma İçin

Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası

1. **Amaç**

Güvenlik, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç unsurdan oluşur. Bu güvenlik öğelerinden herhangi biri zarar görürse kurumsal güvenlik zaafiyeti oluşur.

- *Gizlilik* : Bilginin yetkisiz kişilerin eline geçmemesini,
- *Bütünlük* : Bilginin yetkisiz kişiler tarafından değiştirilmemesini,
- *Erişilebilirlik* : Bilginin ilgili ve yetkili kişilerce ulaşılabilir ve kullanılabilirliğini ifade eder.

Bu politikanın amacı;

1. Veri Sorumlusu bünyesinde, ticari ve operasyonel her türlü fiziki veya elektronik ortamlardaki bilgi ve verilerin güvenliği ve gizliliğini sağlamak,
2. Veri Sorumlusu'na ait olan tüm elektronik bilgi sistem ekipmanlarının fiziksel emniyetini sağlamak,
3. Veri Sorumlusu tarafından genel olarak işlerin yürütülmesi amacıyla her türlü yoldan tedarik edilmiş (satın alma, üretme, ortaklık kurma) elektronik bilgi sistemleri ekipmanı ve bunlarla ilgili hizmet kaynaklarının verimli bir şekilde kullanılmasını sağlamak, kişisel çıkar veya kötü amaçlar için değerlendirilmesini önlemek,
4. Veri Sorumlusu bünyesinde kullanılan her türlü elektronik bilgi sistemleri ekipmanı ve bunlarla ilgili hizmet kaynaklarının yasal ve lisanslı olmasını sağlamak,

5. Veri Sorumlusu'nun kurumsal kimliğini ve yapısını korumak, kurumsal yapısının gelişmesini desteklemek,
6. Yasa ve yönetmeliklere uyumlu olarak bilgi güvenliği süreçlerini yürütmektir.

1. **Tanımlar**

- *Bilgi Sistemleri* : Verilerin/bilgilerin üzerinde tutulduğu, kaydedildiği, işlendiği, iletildiği, saklandığı elektronik, manyetik, yazılı ve diğer ortamlar ile ekipmanları, sistemleri, kişisel bilgisayarları (PC), sunucuları (server), dizüstü bilgisayarları (laptop, notebook); akıllı telefon, tablet, aktif cihaz, disket, kartuş, CD, DVD, BD medyaları, yedekleme birimleri, telli/telsiz iletişim cihazlarını, router, hub, switch ve modemleri; ağ bağlantılarını ve sistemlerini, faks, yazıcı (printer), fotokopi cihazı gibi ve ayrıca sistemlerle bağlantılı ve bunlara ait tüm yazılım, program, uygulama ve benzerlerini ifade eder.
- *Bilgi Sistemleri Direktörlüğü (BSD)* : Veri Sorumlusu'na destek sunan ve bilgi teknolojileri alanında hizmet veren Veri Sorumlusu iç birimini ifade eder.
- *Bilgi Sistemleri Güvenliği (BSG)* : Veri Sorumlusu'na destek sunan, Bilgi Sistemleri Direktörlüğü'ne bağlı çalışan bilgi sistemleri güvenliğinden sorumlu olan alt birimi ifade eder.
- *Gizli/Değerli Bilgi* : Veri Sorumlusu'nun mülkiyetinde olan ve ticari, maddi, manevi değer taşıyan veya her türlü potansiyel ticari değer taşıyacak veya rekabet unsuru olabilecek bilgileri; Veri Sorumlusu'na özgü yöntemlere, çalışma biçimine, iş hacmine, hazırlanmış veya hazırlanmakta olan projelere ait bilgileri, ticari sırları, her türlü bilgi sistemlerine ait lisansları, altyapı, bilgi / veri toplama, saklama, iletim, erişim yöntemleri de dahil olmak üzere teknik bilgi, bilgi sistemlerindeki güvenlik açıklarını, özel gizli veya güvenlik sistemlerine ait her türlü teknik veya gizli bilgiyi, yazılımları, programları ve kaynak kodlarını, şifreleri, özel yetki parametrelerini, elektronik posta (e-posta) adreslerini, şirket telefon numaralarını, finansal bilgileri, yeni iş veya hizmet fikirlerini, satış stratejilerini, çözümleri, müşteri liste ve portföylerini, endüstriyel tasarımları, marka / ürün adlarını, kayıt, evrak, resim, çizim, şema, sınai mülkiyet ve telif hakkı kapsamındaki bilgileri, logo, amblem, slogan, elektronik veya diğer ortamlarda üretilen ve kullanılan her çeşit ürün, ekipman vb. bilgileri ifade eder.
- *Hizmet Masası* : Veri Sorumlusu çalışanlarına, bilgi sistemleri kullanımıyla ilgili destek sunan, soru ve sorunların çözümü için ilk başvuruyu kabul eden BSD birimini ifade eder.
- *Kanun :* 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder. Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları belirleyen ve 24/3/2016 tarihinde kabul edilerek, 7/4/2016 tarihinde yürürlüğe giren kanundur.
- *Kişisel Veri* : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Kişilerin adı, soyadı, doğum tarihi ve doğum yeri, kişinin fiziki, ailevi, ekonomik ve sair özelliklerine ilişkin bilgiler, isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası gibi veriler kişisel veridir.

- *özel Nitelikli Kişisel Veri* : Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkümiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.
- *Sistem Cihazları* : Sadece yetkili çalışanın müdahale ve yetkili erişiminde/kullanımda bulunabileceği, sistem odaları veya sistem odalarının olmadığı yerlerde belirlenmiş bir alanda/bölgede bulunması gereken, şirketlerin tüm bilgi sistemlerinin, veri iletişim kanallarının kesintisiz çalışmasını sağlayan, altyapısını destekleyen, kritik öneme sahip; tüm türlü bilgi sistemlerini, elektrik ve enerji üretim ve destek cihazları, UPS, jeneratör vb. tüm bu sistemlere ait ekipman, donanım, yazılım, program ve uygulamaları ifade eder.
- *Sistem Erişim Bağlantıları/Oturumları* : Bilgi sistemleri aracılığıyla, etki alanı, ağ alanları ve sistemleri, sunucu sistemlerine belli parametreler, kullanıcı adı/şifresi veya benzeri her türlü yetkili erişim ekipmanlarını kullanarak bağlantı sağlanması, oturum açılması, erişim yapılması vb. (domain/network login/logon, AS400 sign on vb.) eylemleri/durumları ifade eder.
- *üçüncü Şahıslar* : Veri Sorumlusu dışındaki tüm resmi veya resmi olmayan kurum, şirket, kuruluş, örgüt, kişi veya kişiler.
- *Veri/Bilgi* : Kişisel bilgisayar , sunucu , dizüstü bilgisayar, akıllı telefon, tablet, el bilgisayarları, aktif cihazlar, disket, kartuş, CD, DVD, BD medyalar, yedekleme birimleri, telli/telsiz iletişim cihazları, router, hub, switch, modem, ağ bağlantıları ve sistemleri vb. her türlü elektronik/manyetik ortamlar, sistemler ve ekipmanlar ve bunlara ait yazılım, program, uygulamalar vb. üzerinde işlenen, tutulan, kaydedilen, iletilen, saklanan tüm veri ve bilgiler ile; faks, yazıcı, fotokopi, el yazısı vb. ile üretilmiş dosya, yazı, çıktı, doküman, evrak vb. yerlerde tutulan, kaydedilen, iletilen, saklanan tüm veri ve bilgileri ifade eder.
- *Veri İletişim Kanalları* : Her türlü genel amaçlı veri/bilgi veya gizli/değerli bilgiye erişilmesi veya tüm bu verilerin/bilgilerin bulunduğu ortamdan başka ortamlara çeşitli yollardan (telli/telsiz iletişim, Internet, telefon, GSM, e-posta, ağ üzerinden kopyalama, yedekleme cihazları üzerine taşıma, CD, DVD, BD vb. medyalar ile, faks, modem, fotokopi, yazıcı vb.) iletimi, kopyalanması, taşınmasına olanak veren bilgi sistemlerini ifade eder.
- *Veri Sorumlusu* : VOLCAR OTOMOBİL VE YEDEK PARçA SANAYİ VE TİC.A.Ş. ve ortaklık pay oranlarına bağlı kalınmaksızın var olan ve ileride kurulacak bağlı şirketler, iştirakleri ve bunların ortaklık kurduğu ve kuracağı tüm şirketleri ifade eder. Aynı zamanda, kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
- *Veri Sorumlusu İrtibat Kişisi* : Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.

1. **Kapsam**

Bu politika, Veri Sorumlusu bünyesinde çalışan (bordrolu, sözleşmeli, stajyer, diğer özel anlaşmalara bağlı vb.), her türlü yetki, unvan, amaçla görev yapan tüm çalışanları kapsamaktadır. Tüm Veri Sorumlusu çalışanları bu politikada belirtilen standart ve kuralları okumak, bilmek ve uymakla yükümlüdür.

1. **Yetki ve Sorumluluklar**
    1. *Veri Sorumlusu Yöneticilerinin Sorumlulukları*
        1. Belirlenmiş olan politika ve standartların önemini kendi birimindeki çalışanlara aktarmak, kurumsal ve yasal gereksinimler kapsamında düzenli olarak gözden geçirmek ile sorumludur.
        2. Politika ve standartları, kendi birimindeki çalışanların anlamasına ve politikalara uyumun sağlanmasında yardımcı olmalıdır.
        3. Kendi birimindeki çalışanlarda güvenlik bilincinin oluşması ve yerleşmesine yardımcı olmalıdır.
2. *Veri Sorumlusu çalışanlarının Sorumlulukları*
    1. Bilgi sistemleri işlemlerini belirlenen kurallar ve standartlar doğrultusunda, gerektiğinde BSD bünyesinde görev yapan Hizmet Masası birimlerinden destek alarak gerçekleştirmek ile yükümlüdür.
    2. İlgili güvenlik standartları ve politikalarına aykırı davranışları gözlemlediklerinde en kısa sürede Hizmet Masası veya BSG birimlerine bildirir.

1. *BSG Birimi Sorumlulukları*

Bilgi sistemleri güvenlik

1. *BSD İlgili Birimlerinin Sorumlulukları*

İlgili güvenlik standartlarını ve teknik düzenlemelerini bilmek ve uygulamakla yükümlüdür. Belirlenmiş olan politika ve standartlara göre Veri Sorumlusu çalışanlarına destek verir.

1. **Kurallar ve Uygulama**
    1. Kurum içinde elektronik veya diğer ortamlardaki veriler/bilgiler Veri Sorumlusu'nun mülkiyetindedir ve tüm yasal hakları Veri Sorumlusu'na aittir.
    2. Veri Sorumlusu bünyesindeki her türlü bilgi sistemleri, veri iletişim kanalları, verileri/bilgileri vb. yalnızca iş amaçlı kullanılmak zorundadır.
    3. Veri Sorumlusu çalışanları, her türlü bilgi sistemleri, veri iletişim kanalları, veri ve bilgilerin kullanımları sırasında, fiziksel koruma, erişim denetimi, yedekleme, güvenlik ve gizlilik ilkelerine azami önem göstermek ve uymak zorundadırlar.

özellikle kaybolma ve hırsızlık risklerine açık olan taşınabilir cihazlar gözetimsiz bırakılmamalı ve güvenliği sağlanmalıdır.

4. Veri Sorumlusu'na ait gizli/değerli bilginin ve her türlü kişisel verilerin gizliliğinin sağlanması esastır. Tüm bu değerli bilgi ve kişisel verilerin veri iletişim kanalları yoluyla Veri Sorumlusu dışına çıkartılması ve üçüncü şahıslara, her ne şekilde ve her ne amaçlı olursa olsun iletilmesi, kullandırılması yasaktır. Ayrıca kurumsal süreçlerde kullanılan özel nitelikli kişisel veriler ve kişisel veriler elektronik veya fiziksel kopya olsun çalışanın evinde, dizüstü bilgisayarlarda veya diğer kişisel taşınabilir cihazlarda ve işyeri dışındaki diğer sahalarda tutulamaz. Verilerin/bilgilerin kurum dışına çıkartılması gereken özel durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan **"Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası"** uygulanacaktır.

5. Veri Sorumlusu çalışanları, Veri Sorumlusu mülkiyetinde olmayan bilgi sistemlerini bina, ofis, şirket vb. içine sokamaz, kullanamaz. Gerektiği özel durumlarda yalnızca BSD bilgisi ve onayı ile yetkili çalışan gözetiminde giriş yapılabilir.

6. Sistem odalarına ve bu odaların olmadığı yerlerdeki sistem cihazlarına yalnızca Veri Sorumlusu BSD bünyesindeki yetkili çalışan giriş yapabilir. Bu çalışan dışındaki kişilerin sistem odalarına girmesi veya sistem cihazlarına erişmesi gerektiği durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" uygulanacaktır.

7. üçüncü şahısların Veri Sorumlusu bilgi sistemleri ve bu sistemler üzerindeki her türlü bilgiyi veri iletişim kanallarıyla kullanması gerektiği durumlarda, konuyla ilgili Veri Sorumlusu bünyesinde yayımlanmış olan "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikası" uygulanacaktır.

8. çalışma saatleri sonunda masaüstünde herhangi bir doküman bırakılamaz, gizli/değerli, kişisel ve kurumsal veri içeren belgeler, özel proje dosyaları ofis masalarının parçası olan kilitli çekmecelerde ve dolaplarda tutulmalıdır. Aynı şekilde şifre ve kullanıcı adı yazılı küçük kağıtlar çalışma masası üzerinde veya çevresinde kesinlikle bırakılamaz.

9. Veri Sorumlusu çalışanları kullanmakta oldukları bilgi sistemlerine veri iletişim kanallarıyla kendi istekleri ve bilgileri dışında erişilmesine olanak tanımamalıdır. Bilgi sistemlerinde çalışmaları bittiğinde, mutlaka şifre denetimli ekran koruyucularını çalıştırmalı veya sistemden erişim bağlantı / oturumlarını kapatarak (logout/logoff vb.) çıkmalıdırlar.

10. BSD bilgisi ve onayı olmadan, bilgi sistemlerine veri iletişim kanallarıyla ne amaçlı olursa olsun, herhangi bir yazılım, donanım veya sistem kopyalanamaz, kurulamaz. Veri Sorumlusu çalışanları, BSD tarafından hazır olarak kendilerine teslim edilmiş hiçbir kişisel bilgisayarda yazılım, donanım veya sistem ayarlarında değişiklik yapamaz. Değişiklik gerektiği durumlarda her türlü ayar değişikliğini yalnızca, o sistemlerin yetkilisi olan BSD Kullanıcı Destek ekipleri yapacaktır.

11. Veri Sorumlusu bünyesindeki bilgi sistemlerinde kullanılan tüm yazılımlar lisanslı ve yasaldır; bu sistemlerin ürün standartlarını BSD belirler. Veri Sorumlusu çalışanları bilgisayar programlarını da kapsayan 5846 sayılı Fikir ve Sanat Eserleri Kanunu'na aykırı hareket edemezler.

12. Kişisel bilgisayar veya sunucu sistemlerde virüs koruma (anti-virus) programı kurulu ve sürekli etkin durumda olacaktır. Veri Sorumlusu çalışanları, kullandıkları bilgisayarlarda virüs koruma programının kurulu olmadığını, programın çalışmadığını veya bilgisayara zararlı bulaştığını fark ederlerse, mutlaka en kısa sürede Hizmet Masası birimlerine haber vermelidirler.

13. Kullanıcı kimliği ya da şifreler kişiye özeldir ve kimseyle paylaşılmamalıdır. Kullanıcı kimliği ya da şifrenin herhangi yetki dışı kullanım dahil tüm kullanımından ve meydana gelebilecek suiistimal olaylarının yaratabileceği kurum zararlarından çalışanlarımız sorumludur. Kullanıcı kimliğinin ya da şifrenin güvenliğinden kuşku duyulan durumlarda şifreler değiştirilmeli ve derhal Hizmet Masası birimiyle temasa geçilmelidir. Veri Sorumlusu çalışanları, bilgi sistemlerindeki tüm kullanıcı adı, şifre, yetki sistemleri vb. kullanımlarında, BSD'nin Veri Sorumlusu bünyesinde yayımladığı "Şifre Seçimi Ve Kullanımında Uyulması Gereken Güvenlik Standartları" dokümanını okumalı ve söz konusu dokümanda belirtilen tüm kurallara uyacak şekilde şifre seçmeli ve kullanmalıdırlar.

14. Gizli/değerli veriler ile kişisel veriler ağ aracılığı ile güvensiz (şifrelenmemiş) olarak paylaşılamaz ve iletilemez. Veri Sorumlusu çalışanları bu amaca yönelik veri ve bilgi şifrelemede kullanılacak uygun yöntem ve politika için Hizmet Masası birimimizden destek alabileceklerdir. Aynı şekilde gizli/değerli veriler ile kişisel verilerin şirket içerisinde başka bir çalışan ile paylaşılmasının gerektiği durumlarda, iç yazışma zarfları "Kişiye özel" olarak sadece ilgilisine gönderilmelidir.

15. Veri Sorumlusu bünyesinde kurum tarafından verilen internet hizmeti dışında, alternatif internet hizmeti kullanılamaz. Veri Sorumlusu çalışanları, yetkili Internet erişimi veya Internet üzerinden şirket içi ve dışı her türlü diğer erişim gereksinimlerinde konuyla ilgili Veri Sorumlusu genelinde yayımlanmış olan BSG politika ve standartlarına göre istekte bulunacaklardır.

16. İnternet, yalnızca şirket mevzuatı, işleri ile ilgili araştırma/geliştirme, bilgi toplama, ihtiyaçlar ve amaçlar kapsamında, ilgili yasal, resmi, kurumsal web sitelerine erişim yapmak için kullanılmalıdır. Kurum cihazları güvenlik açısından gerekli görüldüğünde BSG uzmanları tarafından merkezi olarak kontrol edilebilecektir.

17. Veri Sorumlusu çalışanları, şirket e-posta sistemlerini, adreslerini ve e-posta kutularını yalnızca iş amaçlı kullanabilir. Şirket e-posta adreslerini kullanılarak, çalışanlarımıza veya üçüncü şahıslara, kişiliği zedeleyici, müstehcen içerikli, hakaret, tehdit, küfür, siyasi mesaj, slogan, propaganda vb. içeren e-posta iletilemez; şirket e-posta sistem ve adresleri kurumsal şirket politikalarını, kurallarını veya ülke yasalarını ihlal edecek kanundışı işlemlerde kullanılamaz.

18. Veri Sorumlusu çalışanları, tanımadıkları adreslerden gelen, ek dosyası, konusu veya içeriği kuşkulu veya belirsiz olan e-postaları kesinlikle açmamalı, herhangi başka bir adrese iletmemeli, en kısa sürede Hizmet Masası birimlerine haber vermelidir. Benzer şekilde, Veri Sorumlusu çalışanları, herhangi bir kaynaktan (e-posta, medya, Internet veya başka yolla) bir virüs ihbar, haber ve uyarısı alırsa, bu bilgiyi herhangi bir üçüncü şahsa veya iş arkadaşına kesinlikle aktarmayıp Hizmet Masasına iletmelidir.

19. İş amaçlı her türlü liste servisi (sosyal medya, mailing list, newsgroup) ya da benzeri ortak elektronik posta sistemleri ve dağıtım gruplarına üyeliklerde, Hizmet Masası birimleri aracılığıyla BSD'den onay alınması gerekmektedir.

20. Veri Sorumlusu çalışanlarının yapmış olduğu bütün Internet erişimleri ve e-posta kullanımları, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği Veri Sorumlusu içindeki bilgi güvenliği kontrol sistemlerinde kayıtlanıp takip altında bulundurulmaktadır.

21. Veri Sorumlusu'na ait veriyi korumak amacıyla, kurumsal kaynaklara şirket dışından veri iletişim kanallarıyla bağlanarak çalışan için ek güvenlik önlemleri alınması gerekecektir. Bu durumlarda çalışanın kullandığı bilgi sistemlerine (kişisel bilgisayar, akıllı telefon, tablet vb.) BSD uzmanları tarafından uygulanacak kontroller (iyileştirme, düzenleme, şifreleme ve zararlı kod önleme) kurumsal kaynaklara erişim süresince çalışır durumda tutulmalıdır.

22. Kullanıcıların Veri Sorumlusu kurumsal sistem kaynaklarına erişim yetkileri iş gereksinimlerine göre düzenlenmektedir. Veri Sorumlusu çalışanları kendilerinde ya da çalışma arkadaşlarında gördükleri yetki aşımı ya da paylaşımı gibi uygunsuzlukları en kısa zamanda Hizmet Masası birimine bildirmekle yükümlüdürler.

23. Ortak paylaşım alanları, elektronik posta sistemleri kişisel verilerin arşiv depolamasına uygun değildir. Veri Sorumlusu suç veya kanunsuz olması muhtemel olarak görülen her türlü veri, sistem ve malzemeyi kendi bilgi sistemlerinden çıkarma hakkını ve bununla ilgili resmi işlem başlatma hakkını saklı tutar.

24. Veri Sorumlusu bünyesinde bilgi sistemleri ve ekipmanları ile iş kapsamı dışında bulut depolama ve mesajlaşma hizmetlerinin (Dropbox, Gdrive, Onedrive, Whatsapp, Hangouts, Box, vb.) kullanılması yasaktır. Bu tür gereksinimler için iş öncelikleri gözetilerek kurumsal uygulamaların belirlenmesi ve hizmete alınması BSD birimlerinin sorumluluğundadır.

25. 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. Bu nedenle çalışanlarımız Veri Sorumlusu idari ve iş birimleri tarafından kendisinden talep edilmeyen kişisel verilerini, özel nitelikli kişisel verilerini kurum kaynaklarında saklamamalı ve kullanmamalıdır. İşle ilgili olmayan ve şahsi/özel kullanım amaçlı tüm kişisel veriler (veri sorumlusu tarafından gereğince aydınlatılan ve açık rıza

alınanlar hariç olmak üzere), veri sorumlusu tarafından tahsis edilen e-posta kutularında, anlık mesajlaşma yazılımlarında, ofis belgelerinde, taşınabilir bilgisayarlarda ve ortak paylaşım alanlarında bulundurulmamalıdır. Ayrıca çalışanlar, işledikleri bütün kişisel verilerin güvenli şekilde tutulmasını temin etmekle yükümlüdürler. Kişisel Veriler, kazaen veya başka bir şekilde de olsa herhangi yetkisiz bir üçüncü kişiyle sözlü, yazılı veya başka şekilde paylaşılamaz, ifşa edilemez. Kişisel verileri yetkisiz olarak paylaşılması gibi maddede belirtilen prensiplere aykırı durumların derhal Veri Sorumlusu İrtibat Kişisi'ne bildirilmesi gerekmektedir.

26. Her çalışan, kurumla ilişiğinin kesilmesi durumunda; Veri Sorumlusu'na ait her türlü gizli/değerli bilgi, veri/bilgi ve bunların tutulduğu veya kayıtlı, yazılı olduğu tüm bilgi sistemlerini işten ayrıldığı yazılı tarihi takiben en fazla 1 iş günü içinde Veri Sorumlusu'na geri teslim etmek zorundadır. İşten çıkartılan veya kendi isteğiyle işten ayrılan her çalışan, Veri Sorumlusu ile ilişiği kesildiği tarihten itibaren süresiz olarak işbu Politika'nın 5.1. ve 5.4. maddelerine uymakla yükümlüdür.

Araştırma İçin

Kriz Müdahale Prosedürü

1. Amaç

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) 12. Maddesinin 5. fıkrasına göre ARKAS TURİZM SEYAHAT ACENTASI A.Ş. (Şirket) işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildirmekle yükümlüdür.

İşbu Kriz Müdahale Prosedürü (Prosedür), kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde diğer bir deyişle, kişisel veri ihlali olması durumunda oluşacak krize nasıl müdahale edileceği ve atılacak adımların neler olduğu konusunda çalışanları bilgilendirmek amacıyla hazırlanmıştır.

2. Sorumluluk

Prosedür'ün uygulanmasından tüm çalışanlar sorumludur. Prosedür'e aykırı hareket eden çalışanlar "Disiplin Yönetmeliği" hükümlerine tabi olacaktır.

3. Sorumluluk

Kişisel veri ihlali, kişisel verilerin kanuna aykırı bir şekilde elde edilmesi, hukuka aykırı bir şekilde kişisel verilere yetkisiz erişim sağlanması, kişisel verilerin yanlışlıkla/kasten yetkisiz kişilere açıklanması, kişisel verilerin hukuka aykırı bir şekilde silinmesi, değiştirilmesi veya bütünlüğünün bozulması gibi durumlarda ortaya çıkmaktadır.

Aşağıda yer alan durumlar genel olarak kişisel veri ihlali olarak değerlendirilir:

- Kişisel veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi,
- Gizli bilgilerin hukuka aykırı şekilde ifşası,
- Kişisel veri ve/veya gizli bilgi içeren e-postaların yanlışlıkla şirket dışında ilgisiz kişilere iletilmesi, gönderimi,
- IT ekipmanlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle kişisel verilere hukuka aykırı erişim sağlanması.

Yukarıda belirtilen veya benzer durumlarda bu Prosedür'de belirtilen şekilde hareket edilmelidir.

4. Kriz Müdahale Ekibi

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıdaki departmanlardan belirlenen katılımcıların dahil edileceği bir Kriz Müdahale Ekibi (Ekip) oluşturulur:

- Veri Sorumlusu İrtibat Kişisi [1]
- Veri Sorumlusu Üst Yöneticisi (Genel Müdür)
- İhlalin Meydana Geldiği Departmanın Yöneticisi
- KVK Danışma Grubu
- KVK Konusunda Veri Sorumlusu'nun Yetkilendirdiği Üst Yöneticiler (KVK Üst Yöneticiler)

Şirketlerimiz nezdinde kurulmuş olan Kriz Müdahale Ekibi üyelerinin kimler olduğu işbu Prosedür'ün ekinde yer almaktadır (EK-2 / Kriz Müdahale Ekibi)

5. Kriz Müdahale Süreci

Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24.01.2019 Tarih ve 2019/10 Sayılı Kararı (Karar) uyarınca, Şirket'in kişisel veri ihlalini öğrendiği tarihten itibaren **gecikmeksizin ve en geç 72 saat içinde** Kurul'a bildirmesi ve veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de **makul olan en kısa süre içerisinde** ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirket'in kendi internet sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılması gerekmektedir.

Söz konusu yükümlülüklerin yerine getirilebilmesi için, bir veri ihlali durumunda öncelikle şirket içerisinde belirli adımlar takip edilmelidir:

- Krize ilişkin ön değerlendirme,
- Engelleme ve kurtarma çalışmalarının yürütülmesi,
- Risklerin değerlendirilmesi,

- Bildirim,
- Değerlendirme ve İyileştirme.

- *Krize İlişkin Ön Değerlendirme*

Şirket nezdinde gerçek veya potansiyel bir veri ihlalinin söz konusu olması halinde, ilgili tüm çalışanlar Veri Sorumlusu İrtibat Kişisi'ne derhal ve gecikmeksizin durumu bildirmekle yükümlüdür. Bu kapsamda ilgili çalışan aşağıdaki hususları içerir bir rapor hazırlayarak, veri ihlalini Veri Sorumlusu İrtibat Kişisi'ne bildirir.

- Kişisel veri ihlalinin gerçekleşme tarihi ve saati,
- Kişisel veri ihlalinin tespiti tarihi ve saati,
- Kişisel veri ihlali olayına ilişkin açıklamalar,
- Eğer biliniyorsa kişisel veri ihlalinden etkilenen kişi ve kayıt sayısı,
- Kişisel veri ihlalinin tespit edildiği tarihte varsa atılan adımlara, alınan önlemlere ilişkin açıklamalar,
- Raporu hazırlayan çalışanın/çalışanların adı soyadı, iletişim bilgileri ve rapor tarihi.

Veri Sorumlusu İrtibat Kişisi, rapor kapsamında belirtilen hususları dikkate alarak bir ön değerlendirme yapar. Bu değerlendirmeyi yaparken, gerçekten bir veri ihlalinin söz konusu olup olmadığını, ihlalin kapsamını, oluşabilecek etkilerini de göz önünde bulundurarak, Ekip ile birlikte veri ihlalinin araştırılması için kapsamlı bir soruşturma başlatır.

- *Engelleme ve Kurtarma Çalışmalarının Yürütülmesi*

Veri ihlalinin Şirket ve ilgili kişiler üzerindeki etkilerinin azaltılabilmesi için engelleme ve kurtarma çalışmaları ekibin gözetiminde yürütülür. Bu kapsamda öncelikle veri ihlalinden haberdar edilmesi gereken departmanlar tespit edilir ve bu kişilere ihlalin kontrol edilebilmesi, mümkünse engellenebilmesi ve zararların azaltılabilmesi için atılması gereken adımlara ilişkin rehberlik edilir.

Akabinde veri ihlalinden etkilenecek kişilerin ve kayıtların neler olduğu tespit edilmeye çalışılır ve varsa bu kişilerin iletişim bilgileri de belirlenir. Eş zamanlı olarak, veri ihlali nedeniyle haberdar edilmesi gereken başka kurum ya da kuruluşlar olup olmadığı değerlendirilir.[2]

- *Risklerin Değerlendirilmesi*

Kişisel veri ihlalleri, ihlalden etkilenen kişiler üzerinde kimlik hırsızlığı, hakların kısıtlanması dolandırıcılık, finansal kayıp, itibar kaybı, kişisel verilerin güvenliğinin kaybı, ayrımcılık gibi birçok olumsuz etki oluşturabilir. Bu nedenle kişisel veri ihlalinin olası sonuçlarının Şirket ve ihlalden etkilenen kişiler üzerinde ne gibi etkiler oluşturabileceğinin dikkatli bir şekilde değerlendirilmesi ve risklerin ortaya koyulması çok önemlidir.

Ekip tarafından riskler değerlendirilirken, ihlalden etkilenen kişisel verilerin niteliği, hassasiyeti ve hacmi ile etkilenen bireylerin sayısı ve kişi gruplarının kimler olduğu, veri ihlalinin Şirket'in faaliyetleri ile itibarına olan etkisi, veri ihlalinin etkisinin azaltılmasında alınan önlemler ve ihlalin olası sonuçları ayrı ayrı ele alınmalıdır. Bunların sonucuna göre veri ihlali "düşük düzeyde, orta düzeyde veya yüksek düzeyde risk" olarak nitelendirilir:

- **Düşük düzeyde risk:** İhlal ilgili kişiler üzerinde olumsuz herhangi bir etkiye neden olmamakta ya da bu etki ihmal edilebilir düzeyde kalmaktadır.
- **Orta düzeyde risk:** İhlal ilgili kişiler üzerinde olumsuz etkilere neden olabilir fakat bu etki büyük değildir.
- **Yüksek düzeyde risk:** İhlal etkilenen kişiler üzerinde ciddi düzeyde olumsuz etkilere neden olmaktadır.[3]

Orta ve özellikle yüksek düzeyde risk olarak tanımlanan veri ihlallerine ilişkin Veri Sorumlusu Üst Yönetimi'ne Ekip tarafından bilgi verilir.

- *Bildirim*

Veri ihlalinin gerek hukuki yükümlülük kapsamında gerekse veri ihlaline ilişkin tedbir alınması, ihlalin olası etkilerinin azaltılması gibi amaçlarla Şirket dışında üçüncü kişilere bildirilmesi gerekmektedir.

- *Kurul'a bildirim*

Veri Sorumlusu İrtibat Kişisi, öncelikle **kişisel veri ihlalinden haberdar olduğu andan itibaren gecikmeksizin ve en geç 72 saat içerisinde** Kurul'a bu durumu bildirmekle yükümlüdür. Bu nedenle, Şirket içerisinde tüm çalışanların herhangi bir veri ihlali durumunu vakit kaybetmeksizin Veri Sorumlusu İrtibat Kişisi'ne bildirmesi, Şirket'in herhangi bir yaptırımla karşı karşıya kalmaması için önem arz etmektedir.

Kurul'a yapılacak bildirimde Kişisel Verileri Koruma Kurumu'nun (Kurum) internet sitesinde yayınlanmış olan Kişisel Veri İhlali Başvuru Formu[4] kullanılır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir.

Haklı bir gerekçe ile 72 saat içerisinde Kurul'a bildirim yapılamaması durumunda, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurul'a açıklanır.

- *İhlalden Etkilenen Kişilere Bildirim*

Şirket, kişisel veri ihlalinden etkilen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa uygun yöntemlerle (örneğin internet sitesi üzerinden duruma ilişkin bir duyuru yayınlanması) bildirim yapmalıdır. Söz konusu bildirimler, Ekibin desteğiyle Veri Sorumlusu İrtibat Kişisi tarafından gerçekleştirilir.

Veri sorumlusu tarafından ilgili kişiye yapılan veri ihlali bildiriminde yer alması gereken asgari unsurlara ilişkin, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı uyarınca Şirket tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak aşağıdaki unsurları içermesi gerekir:

- İhlalinin ne zaman gerçekleştiği,
- Kişisel veri kategorileri bazında (kişisel veri/özel nitelikli kişisel veri ayrımı yapılarak) hangi kişisel verilerin ihlalden etkilendiği,
- Kişisel veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun internet sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi.

- *Diğer Bildirimler*

Şirket'in hukuken yapması zorunlu olan bildirimlerin yanı sıra, veri ihlalinin niteliği, büyüklüğü, ihlalin suç teşkil edip etmediği gibi hususlar göz önünde bulundurularak üçüncü kişilere de bildirim yapılması gerekebilir. Bu kişiler, diğer veri sorumluları ya da veri işleyenler, dış danışmanlar, adli makamlar, bankalar olabilir. Ekip, böyle bir gereklilik olup olmadığını ayrıca değerlendirir ve gerekli ise bildirimleri yapar.

- Değerlendirme ve İyileştirme

Şirket tarafından kişisel veri ihlallerine ilişkin tüm bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurul'un incelemesine hazır halde bulundurulması gerekmektedir. Veri Sorumlusu İrtibat Kişisi ve Ekip, veri ihlaline ilişkin atılan adımların uygun olup olmadığını ve olası bir veri ihlalinde geliştirilebilecek/ iyileştirilebilecek hususların neler olabileceğini belirlemek adına bir değerlendirme yapar. Bu kapsamda Ekip, aşağıdaki unsurları içerir bir değerlendirme ve iyileştirme raporu hazırlar.

- Olası kişisel veri ihlallerinin etkilerini azaltmak için hangi adımların atılması gerektiği
- Kişisel veri ihlali nedeniyle herhangi bir politika, prosedür ya da raporlamada iyileştirme gerekip gerekmediği
- Kişisel veri ihlalinin tekrarlanmasını önleyebilmek için ek bir idari ve/veya teknik tedbir alınmasının gerekli olup olmadığı,
- İhlalin tekrarlanmasını önleyecek bir personel farkındalık eğitimi gerekliliği,
- İhlallere maruz kalmayı ve maliyet etkilerini azaltmak için kaynaklara/altyapıya ek yatırım yapılmasının gerekli olup olmadığı

6. İlgili Politika Ve Prosedürler

Bu Prosedür, Şirket nezdinde kişisel verilerin korunması ve işlemesine ilişkin yürürlüğe konmuş tüm politika ve prosedürler ile birlikte ele alınmalıdır.

7. Güncelleme

Bu Prosedür kurumsal ya da yasal kaynaklı içeriklerindeki değişiklik gereksinimlerine bakılmaksızın yılda bir kez gözden geçirilerek kayıt altına alınır. Prosedür güncellenmemiş olsa bile, mevzuatta meydana gelen değişiklikler derhal uygulanacaktır.