

BEREKET FİDE TOHUMCULUK ÜRETİM İTHALAT İHRACAT VE TİCARET LİMİTED ŞİRKETİ

&

**KVKK YÖNERGELERİ**

2020

İçindekiler[[1]](#footnote-1)

[Kişisel Verilere İlişkin Yönerge 4](#_Toc56167386)

[Amaç ve Politika 5](#_Toc56167387)

[BİRİNCİ BÖLÜM 5](#_Toc56167388)

[Bilgi Güvenliği Politikası 5](#_Toc56167389)

[1. Tanım 5](#_Toc56167390)

[2. Kapsam 6](#_Toc56167391)

[3. Amaç 6](#_Toc56167392)

[4. Şifreleme 8](#_Toc56167393)

[5. Genel Bilgiler 9](#_Toc56167394)

[6. Kimlik Doğrulama ve Yetkilendirme 12](#_Toc56167395)

[İKİNCİ BÖLÜM 13](#_Toc56167396)

[Kişisel Verilerin Güvenliği 13](#_Toc56167397)

[1. Kişisel Veri Tanımı 13](#_Toc56167398)

[2. Genel Kurallar 13](#_Toc56167399)

[3. Kişinin Verisinin Kaderine Hâkim Olma Hakkı 14](#_Toc56167400)

[4. Verilerin Hukuka Uygunluğu İlkesi 14](#_Toc56167401)

[5. Bilgi Edinme Hakkı 14](#_Toc56167402)

[6. Veri Güvenliği 14](#_Toc56167403)

[7. Güncelleme 15](#_Toc56167404)

[Kişisel Veri Saklama, Silme, İmha ve Aktarılma Yönergesi 16](#_Toc56167405)

[1. Kişisel Veri Saklama, Silme, İmha ve Aktarma Yönergesi Hazırlanma Amacı 17](#_Toc56167406)

[2. Kişisel Veri Saklama ve İmha Yönergesi Hazırlanması ve Değişiklikler 17](#_Toc56167407)

[3. Tanımlar 17](#_Toc56167408)

[4. Kişisel Verilerin Kaydedildiği Ortamlar 18](#_Toc56167409)

[5. Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Hukuki, Teknik ve Diğer Sebepler 18](#_Toc56167410)

[6. Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesi ve Erişilmesinin Önlenmesi İçin Alınmış Teknik ve İdari Tedbirler 19](#_Toc56167411)

[7. Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Teknik ve İdari Tedbirler 20](#_Toc56167412)

[8. Kişisel Verileri Saklama ve İmha Süreçlerinde Yer Alanların Unvanları, Birimleri ve Görev Tanımları 20](#_Toc56167413)

[9. Periyodik İmha Süreleri 21](#_Toc56167414)

[10. Saklama ve İmha Süreleri 21](#_Toc56167415)

[11. Güncelleme 21](#_Toc56167416)

[Kişisel Verileri Koruma Komitesinin Görevlerine İlişkin Yönerge 25](#_Toc56167417)

[1. Amaç 26](#_Toc56167418)

[2. Görevleri 26](#_Toc56167419)

[3. Başvuruları Cevaplama 27](#_Toc56167420)

[4. Mevzuatı Takip ve Öneride Bulunma 27](#_Toc56167421)

[5. Geçmişe Yönelik Verilerin Hukuka Uygunluğunu Kontrol 27](#_Toc56167422)

[6. Yönergeleri Uygulama Görevi 27](#_Toc56167423)

[7. Güncelleme 27](#_Toc56167424)

[Veri Sahibi Başvuruları Yönetim Yönergesi 28](#_Toc56167425)

[1. AMAÇ 29](#_Toc56167426)

[2. TANIMLAR 29](#_Toc56167427)

[3. İRTİBAT KİŞİSİ ve KVKK KOMİTESİNİN GÖREVLERİ 29](#_Toc56167428)

[4. VERİ SAHİBİ BAŞVURUSUNUN GEÇERLİLİK ŞARTLARI 29](#_Toc56167429)

[5. BAŞVURUNUN ALINMASI 31](#_Toc56167430)

[6. BAŞVURU İNCELEME SÜRESİ 31](#_Toc56167431)

[7. BAŞVURULARIN SONUÇLANDIRILMASI 31](#_Toc56167432)

[8. ÜCRET 32](#_Toc56167433)

[Kişisel Verilere İlişkin Acil Durumlar Yönergesi 33](#_Toc56167434)

[1. Amaç 34](#_Toc56167435)

[2. Acil Eylem Planı 34](#_Toc56167436)

[3. Acil Durumun Sisteme Müdahale Suretiyle Ortaya Çıkması 34](#_Toc56167437)

[4. Sisteme Fiziki Müdahale 34](#_Toc56167438)

[5. Verilerin Dışarıya Sızması 34](#_Toc56167439)

[6. Komitenin Toplantıya Çağırma Yetkisi 34](#_Toc56167440)

[7. Kamuoyu Bilgilendirmeleri 35](#_Toc56167441)

[Komite için Genel Kurul Kararı 36](#_Toc56167442)

[Yönergeler için Genel Kurul Kararı 37](#_Toc56167443)

# Kişisel Verilere İlişkin Yönerge

Ortaklar Kararı ile yürürlüğe girer. KVKK Kitapçığına eklenir.

Versiyon 1.0

…/…/2020

## Amaç ve Politika

Bu Yönergenin amacı, **Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi**’de (Bundan sonra kısaca"Bereket Fide" veya "Şirket" olarak anılacaktır.) veri güvenliğinin ve kişisel verilerin korunmasıdır. Yönerge, Ortaklar Kararı ile yürürlüğe girer. Yönergenin uygulanması ise Ortaklar Kararı ile oluşturulan Kişisel Verileri Koruma Komitesi tarafından takip edilir.

Ortaklar re’sen ya da Komite’nin önerisi ile Yönergeyi yenileyebilir, Yönergede değişikliklere gidebilir.

Bereket Fide bu Yönerge ile kişisel verilerin elde edilmesi, işlenmesi, aktarılması ve silinme/yok edilmesine ilişkin her aşamada hukuka uygun bir şekilde hareket edilmesini amaçlamaktadır. Şirket, hukuk kuralları ile düzenlenmeyen hususlarda ise kişi yararını ön plana çıkarmayı amaçlar ve boşlukları doldururken bu yönde kararlar verir.

## BİRİNCİ BÖLÜM

## Bilgi Güvenliği Politikası

## Tanım

Bilgi güvenliği, Şirketteki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

a. Gizlilik

b. Bütünlük

c. Kullanılabilirlik

### a. Gizlilik

Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

### b. Bütünlük

Bütünlük, bilginin, kasten veya ihmal ile yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı, içeriğinin korunarak bozulmamış olma halidir.

### c. Kullanılabilirlik

Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim, kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesine göre, her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

## Kapsam

Bu politika, Şirket bilgi işlem altyapısını kullanmakta olan tüm birimleri kapsamaktadır.

## Amaç

Şirket yönetimi, şirketin iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak için bilgi işlem hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziki ve dijital bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

### E-Posta Kullanma Kuralları

a. Şirketin çalışanlara verdiği kurumsal e-posta, kullanıcının şahsi sosyal medya (facebook, twitter, instagram vb.) hesapları, şahsi hesaplar, kişisel kullanım amacıyla üyelikler için kesinlikle kullanılamaz.

b. Kötü amaçlı, spam, sahte vs. nitelikteki zararlı e-postalara yanıt yazılmamalı, bu maillere iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

d. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, bu şekilde gelen e-postalar herhangi bir işlem yapılmaksızın derhal silinmelidir.

e. Çalışanlar, e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

f. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu durumu engellemek için önem arz eden e-postaları şifreleme yoluyla göndermelidirler.

g. Şirket çalışanları kurumsal e-postaların firma dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

h. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Bu durum bilgi işlem departmanına derhal bildirilmelidir.

i. Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren bilgi işlem departmanı ile temasa geçip onlara durumu haber vermekle yükümlüdürler.

j. Şirketten ayrılan personel, kurumsal e-posta sistemini kullanmaya devam edemez. E-posta adresine sahip kullanıcının birim değiştirme, işten ayrılma gibi herhangi bir sebeple şirketten ayırılması durumunda e-posta sisteminde gerekli değişiklikler insan kaynakları departmanı tarafından Bilgi İşlem Birimine en kısa zamanda bildirilir.

### b. İnternet Kullanım Politikası

a. Hiçbir kullanıcı Şirketin tavsiye ettiği veri paylaşım yöntemi dışındaki bir veri paylaşım kanalını kullanamaz. (Örneğin; Bittorent, iMesh, eDonkey, Aimster vb. peer-to-peer bağlantı yollarını içeren programlar kullanılamaz.)

b. Bilgisayarlar arası ağ üzerinden resmi ve iş görüşmeleri haricinde mesajlaşma ve sohbet programları gibi sohbet programları kullanılarak kişisel veri toplanamaz.

c. Hiçbir kullanıcı özel amaçlı olarak internet üzerinden Multimedia Streaming (Video, müzik ve iletişim vb. için) yapamayacaktır.

d. İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) ve bilgisayarlarda saklamak yasaktır.

e. İnternet üzerinden Bilgi İşlem Birimi tarafından onaylanmamış yazılımlar indirilemez ve firma sistemleri üzerine bu yazılımlar kurulamaz, kullanılamaz.

f. Şirket ağlarından ve bilgisayarlarından bilgisayar ve internet ağına zarar verebilecek internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

g. Bilgi İşlem Birimi, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.

h. Şirket ağları ve bilgisayarları üzerinden hiçbir şekil ve surette herhangi bir siyasi içerik ya da propaganda yapılamaz.

ı. Şirket dışında-sahada- internet kullanımı gerçekleştiren çalışanlar, şirket bilgisayarların güvenli olmayan ağlar üzerinden internet girişi gerçekleştirmemelidir.

i. Güvenli-güvensiz hiçbir ağdan, Şirket tarafından tahsis edilmiş bilgisayar, telefon gibi araçlar üzerinden şahsi banka hesapları için işlem gerçekleştirilmemelidir.

### c. Genel Kullanım Politikası

a. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3. şahısların bilgilere erişimi engellenmelidir.

b. Şirket verilerini içeren bir bilgisayarın veya taşıyıcının çalınması, kaybolması vs. durumlar en kısa sürede Bilgi İşlem Birimi’ne bildirilmelidir.

c. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek Şirkete veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret veya siyasi içerikli mail, kullanıcı bilgileri vs.) kişi sorumludur.

d. Şirketin bilgisayarlarını kullanarak yasadışı olaylara karışılmamalıdır.

e. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişilmemelidir.

f. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.

j. Şirket bilgileri üçüncü kişilere hiçbir şekilde iletilmemelidir.

g. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

h. Herhangi bir cihaz, yazılım ve veri iş dışında izinsiz olarak şirket dışına çıkarılmamalıdır.

i. Şirketin kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD’leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

j. Personel, kendilerine tahsis edilen ve şirket çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliğinden sorumludur.

k. Bilgi İşlem Birimi kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir, gereken teknik veya idari tedbirleri uygulayabilir.

l. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

m. Bilgisayarlar üzerinde resmî belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

n. Şirkette Bilgi İşlem Birimi bilgisi olmadan Ağ Sisteminde (Web Hosting, E-Posta Servisi vb.) sunucu niteliğinde olan bilgisayar ve cihaz bulundurulmamalıdır.

o. Bilgi İşlem Biriminin bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

p. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisanssız yazılımı bilgisayarında barındıran personel bu durumdan kendisi sorumludur.

r. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde mutlaka şifre kullanım kurallarına göre hareket edilmelidir.

s. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

### d. Acil Durum Politikası

a. Şirketimizde loglama yapılmaktadır. Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.

b. Şirket faaliyetlerinin devamlılığını sağlamak esastır. Acil durumlarda için bu esasa yönelik teknik tedbirler planlanmıştır.

c. Acil durumlar için gerekli araç-gereç ihtiyaçları tespit edilerek, yedekleme ve bakım planlanmıştır.

### e. Antivirüs Politikası

a. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem Birimine haber verilmelidir.

b. Zararlı programları (Örneğin, virüsler, solucanlar, truva atı, e-posta bombaları vb.) Şirket bünyesinde oluşturmak ve dağıtmak yasaktır.

c. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını kuramaz.

## Şifreleme

Şifreleme, bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır.  Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar aşağıda belirtilmiştir.

## Genel Bilgiler

### Şifre Kullanma Kuralları

a. Kullanılan şifrelerin tamamı kolayca kırılamayacak güce sahip olmalıdır.

b. Şifreler (E-posta, internet, PC vs.) en az altı ayda bir değiştirilmelidir.

c. Şifreler e-posta iletilerine veya herhangi bir elektronik forma yazılmamalı ve eklenmemeli, başkası ile paylaşılmamalı, fiziki ya da elektronik ortamlara yazılmamalıdır.

d. Herhangi bir kişiye telefonda şifre verilmemelidir.

e. Şifreler, işten uzakta olunan zamanlarda dahi iş arkadaşlarıyla paylaşılmamalıdır.

f. Kullanıcı, şifresini 3. kişilerle paylaşmamalı, kağıtlara ya da elektronik ortamlara yazmamalıdır.

g. Şifre 5 defa üst üste yanlış girildiğinde bilgisayar kilitlenmektedir.

j. Çoklu giriş yapılan bilgisayarlara giren personellere uyarılar yapılmaktadır.

k. Mutlaka ekran kilidi kullanılmalı ve ekran kilidi kısa aralıklara ayarlanmalıdır.

### Genel Şifre Oluşturma Kuralları

a. Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

b. Şifre, küçük ve büyük karakterlerle (a-z, A-Z), rakam ve sembollere (0-9, !’^+%&/()=?\_;\* gibi) sahip olmalıdır.

c. En az sekiz karakter olmalıdır.

d. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıdan şifresini değiştirmesi talep edilecektir.

### Şifre Koruma Standartları

a. Şirket bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalıdır. (Örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde).

b. Değişik sistemler için farklı şifreleme kullanılmalıdır.  Örneğin, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanılmalıdır.

**Aşağıda yapılmayacaklar listelenmiştir:**

* Herhangi bir kişiye telefonda şifre vermek.
* E-posta mesajlarında şifre belirtmek.
* Üst yöneticinizle şifreleri paylaşmak. (Mecbur kalındığında değiştirilmelidir.)
* Başkaları önünde şifreler hakkında konuşmak.
* Aile isimlerini şifre olarak kullanmak.
* Herhangi bir form üzerinde şifre belirtmek.
* Şifreleri aile bireyleri ile paylaşmak.
* Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek. (Mecbur kalındığında değiştirilmelidir.)

Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini araması söylenmelidir.

Uygulamalarda ve browserlardaki “şifre hatırlama” özellikleri seçilmemelidir. (Örnek: Chrome, Internet Explorer vs.)

### Uygulama Geliştirme Standartları

Uygulama geliştiricileri programlarında aşağıda belirtilen güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

1. Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

2. Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

3. Kural yönetim sistemi desteklenmelidir. (Örnek; bir kullanıcı diğer bir kimsenin şifresini bilmeden fonksiyonlarına devam edebilmelidir.)

### Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

Şirketin bilgisayar ağına uzaktan erişimi tek yönlü şifreleme algoritması veya güçlü şifrelerle yapılmalıdır.

### Sunucu Güvenliği

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

#### Sahip Olma ve Sorumluluklar

Şirket bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur.

Sunucu konfigürasyonları sadece bu grup tarafından yapılacaktır.

a. Bütün sunucular ve mobil cihazlar ilgili şirketin cihaz envanterinde kayıtlı olmalıdır. Envanter en az aşağıdaki bilgileri içermelidir:

* Sunucuların yeri ve sorumlu kişi.
* Donanım ve İşletim Sistemi.
* Ana görevi ve üzerinde çalışan uygulamalar.
* İşletim Sistemi versiyonları.

b. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

c. Şirkette izin verilen bilgi işlem sistemleri haricinde yabancı bir mobil cihaz ya da veri taşıyıcı takılamaz, kullanılamaz.

#### Genel Konfigürasyon Kuralları

a.  İşletim sistemi konfigürasyonları bilgi işlem biriminin talimatlarına göre yapılacaktır.

b.  Kullanılmayan servisler ve uygulamalar kapatılacaktır.

d. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

e. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırılmamalı, gereksiz servisler açılmamalıdır.

f.  Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

g.   Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

h.   Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

#### Gözlemleme

a. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:

* Bütün güvenlikle ilgili loglar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.
* Günlük tape backupları en az 1 ay saklanmalıdır.
* Logların haftalık tape backupı en az 1 ay tutulmalıdır.
* Aylık full backuplar en az 6 ay tutulmalıdır.
* Logloma kayıtları bina dışında olmalıdır.

b. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikli ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

* Port tarama atakları.
* Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
* Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

#### Uygunluk

a. Denetimler yetkili organizasyonlar tarafından şirket bünyesinde atanan Sorumlu tarafından altı ayda bir yapılacaktır.

b. Denetimler Bilgi İşlem Birimi tarafından yönetilecektir.

c. Denetimlerde organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

#### İşletim

a.   Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

b.   Sunucuların yazılım ve donanım bakımları yılda bir yetkili uzmanlar tarafından yapılmalıdır.

c.  Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

## Kimlik Doğrulama ve Yetkilendirme

Bilgi sistemlerinde Kimlik Doğrulama ve Yetkilendirme, konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır:

a. Şirket sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

b. Şirket sistemlerine erişmesi gereken kurum dışı kullanıcılara yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.

c.   Şirket bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenmelidir.

d.   Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.

e.   Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.

f.  Kullanıcılar şirket adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.

h.  Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

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

i.   Kullanıcılara erişim hakları yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için yaptırım uygulanmalıdır.

j.   Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

l. Dışarıdan şirket wi-fi ağına bağlanacak kimselerin mutlaka kimlik tespiti yapılmalıdır. Toplantı odaları için tahsis edilen wi-fi şifre kullanımları da toplantıya katılanların kimliği ile eşleştirilmelidir.

### a. Yetkilendirmeler

Şirket içerisinde online olarak kullanılan elektronik sistemlerin tamamı üzerinde yetkilendirmeler bulunmaktadır. Her programdaki her veri, her çalışan tarafından görüntülenememektedir.

1. Şirket içerisinde Bereket Fide için hazırlanan ve kullanılan online sistemler üzerindeki her veri her çalışan tarafından görüntülenmemektedir.
2. Bereket Fide sipariş defteri içerisindeki bilgiler sadece şirket müdürü ve satış-pazarlama, teslimat, finans departmanları tarafından görüntülenmektedir.
3. Muhasebe programı üzerindeki bilgileri görmeye sadece şirket müdürü ile Muhasebe departmanı yetkilidir. İlgili veriler şirket müdürü ve muhasebe biriminin gerek görmesi halinde, Şirket dışında çalışılan muhasebe bürosu ve danışman Mali Müşavir ile paylaşılabilecektir.
4. Özlük dosyaları sadece insan kaynakları departmanı ve şirket müdürü tarafından görüntülenmektedir.

## İKİNCİ BÖLÜM

## Kişisel Verilerin Güvenliği

## Kişisel Veri Tanımı

6698 Sayılı Kişisel Verilerin Korunması Kanunu’na göre kişisel veri, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. Örneğin, kişinin adı, soyadı, doğum tarihi, doğum yeri, banka hesap bilgileri, kimlik bilgileri ve telefon numarası vb.

Kişisel verilerin mahremiyeti hususunda uyulması gereken temel kurallar şunlardır.

## Genel Kurallar

Bütün kişisel ve kurumsal bilgilerin güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

a.  Şirkette kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin nitelikli verilere erişmesi mümkün olmamalıdır.

b.  Kişisel veriler, kişiye aittir. Yetkilendirilmiş çalışanlar ancak görevleri ile ilgili kişisel verilere erişebilmelidirler.  Ancak şirket bünyesinde atanmış bulunan ilgili sorumlunun yazılı onayı ile diğer yetki dışındaki kişiler verilere erişebilirler.

c.  Bayi, üretici, müşterinin rızası olmadan hiçbir çalışan sözle de olsa müşteri bilgilerini iş ilişkisi dışında üçüncü şahıslara, kişilere ve kurumlara iletemez.

d.  Bayi, üretici veya müşterinin talebi halinde bilgilerine ilişkin bir kopya ilgili kişiye teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir ilgili kişi kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.

e.  Bayi, üretici, çalışan ya da iş sebebiyle elde edilmiş kişisel verilerin izlenmemesi için gerekli tedbirler alınmalıdır. (Kişisel veri içeren hiçbir kayıt gelişi güzel ortada bırakılmamalı, bilgisayar ekranı başkalarınca okunabilecek şekilde bırakılmamalıdır).

f.  Sosyal medya üzerinden yapılan paylaşımlarda ilgili kişinin fotoğrafının paylaşılması sadece ilgili kişiden açık rıza alınması halinde mümkündür.

g. Telefon ile konuşurken kişisel verilere üçüncü şahısların vakıf olmasına engel olunmalıdır.

h.  Bütün kişisel veriler fiziksel olarak korunmuş mekanlarda saklanmalıdır.

ı.  Şirketin elektronik kayıtlarına internet ortamından erişim mümkün olmamalıdır.

i. Çalışanlara, kişisel verilere korunmasına yönelik ilişkin eğitim verilmekte, kişisel verilere ilişkin periyodik bilgilendirmeler gönderilmektedir.

j. Bayi, üretici, müşteri, çalışan verilerin korunması için idari ve teknik önlemler alınmıştır.

## Kişinin Verisinin Kaderine Hâkim Olma Hakkı

Veri sahibi, kendi verisi ile ilgili olarak verisinin nasıl işlendiğini bilme, bilgi talep etme, gerektiğinde güncelleme ve nihayet silinmesini talep etme hakkına sahiptir. Şirket, kullanıcılardan ya da müşterilerden gelecek bu talepleri karşılamak zorundadır.

## Verilerin Hukuka Uygunluğu İlkesi

Şirkette bulunan veya şirkete intikal eden ya da şirketten çıkan bütün veriler ve verilerle ilgili her türlü işlem, hukuka ve kişilik haklarına uygun yapılmalıdır. Şirketin bütün çalışanları, şirket müşterilerinin verilerinin gizliliğine saygı göstermek zorundadır.

## Bilgi Edinme Hakkı

Şirket müşterileri, kendi verilerinin nerede ve nasıl kullanıldığını bilme hakkına sahiptir. Bu hakkı kolaylaştıran ve mümkün kılan önlemler şirket tarafından alınır.

## Veri Güvenliği

Veri Güvenliğine ilişkin tüm idari ve teknik önlemler Bereket Fide tarafından alınmıştır. Bilgi Güvenliği Politikası içerisinde önlem ve yetkilendirmelere ilişkin tüm bilgiler mevcuttur.

## Güncelleme

İşbu Yönerge’de yapılan değişiklikler aşağıdaki tabloda gösterilmektedir.

|  |  |
| --- | --- |
| Yönerge Güncelleme Tarihi | Değişiklikler |
|  |  |
|  |  |

# Kişisel Veri Saklama, Silme, İmha ve Aktarılma Yönergesi

Ortaklar Kararı ile yürürlüğe girer. KVKK Kitapçığına eklenir.

Versiyon 1.0

…/…/2020

## Kişisel Veri Saklama, Silme, İmha ve Aktarma Yönergesi Hazırlanma Amacı

Bu Yönergenin amacı, **Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi** ’de (Bundan sonra kısaca"Bereket Fide" veya "Şirket" olarak anılacaktır.) kişisel verilerin güncellenmesi, aktarılması, anonimleştirilmesi, silinmesi ve yok edilmesine ilişkin düzenlemelerin yapılmasıdır. Yönerge, Ortaklar kararı ile yürürlüğe girer. Yönergenin uygulanması ise Ortakların aldığı Karar’ın kararı ile atanan Kişisel Verileri Koruma Komitesi tarafından takip edilir.

## Kişisel Veri Saklama ve İmha Yönergesi Hazırlanması ve Değişiklikler

Politika, Bereket Fide Ortaklar Kararı ile yürürlüğe girer. Yönerge’nin uygulanması ise Ortaklar’ın kararı ile atanan Kişisel Verileri Koruma Komitesi tarafından takip edilir. ORtaklar, re’sen ya da sorumlunun önerisi ile Yönerge yenileyebilir, Yönerge‘de değişikliklere gidebilir.

## Tanımlar

Bu Kişisel Veri Saklama ve İmha Yönergesi’nin uygulanmasında:

|  |  |
| --- | --- |
| Kısaltma | Tanım |
| Kanun: | 6698 sayılı Kişisel Verilerin Korunması Kanunu’nu, |
| Kişisel Verileri Koruma Komitesi/Sorumlusu: | Bereket Fide bünyesinde Ortakların kararı ile oluşturulan ve kişisel verilerin korunması ve işlenmesine ilişkin şirket içi işleyişten sorumlu Kişisel Verileri Koruma Komitesi ya da Komite’nin seçtiği üyesini, |
| Kişisel Verilerin Anonim Hale Getirilmesi: | Kişisel verilerin, başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini, |
| Kişisel Verilerin İmha Edilmesi: | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini, |
| Kişisel Verilerin Silinmesi: | Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini, |
| Kişisel Verilerin Yok Edilmesi: | Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini, |
| Politika: | Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi Kişisel Veri Saklama ve İmha Politikasını, |
| Şirket: | Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi ’yi, ("Bereket Fide" veya "Şirket") |
| Ortaklar Kurulu | Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi Ortaklar Kurulu’u, |
| Yönetmelik: | 28 Ekim 2017 tarihli Resmî Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale getirilmesi Hakkında Yönetmelik’i ifade eder. |

## Kişisel Verilerin Kaydedildiği Ortamlar

Şirket, Kanun’a uygun olarak gerçekleştirmekte olduğu veri işleme faaliyetleri kapsamında elde ettiği özel nitelikli kişisel veriler de dahil olmak üzere tüm kişisel verileri, işleme amacının gerektirdiği ölçü ile sınırlı olmak kaydıyla muhafaza etmektedir. Bu kapsamda, elde edilen kişisel veriler Şirket tarafından fiziki ve elektronik ortamlarda saklanmaktadır.

## Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Hukuki, Teknik ve Diğer Sebepler

Kanun’da yer alan veri işleme şartlarına uygun olarak doğrudan veya dolaylı biçimde elde edilen kişisel veriler, Şirket tarafından ilgili mevzuatın öngördüğü veya işleme amacının gerektirdiği süre boyunca hukuka ve dürüstlük kurallarına uygun olarak muhafaza edilmektedir.

Şirket, ticari faaliyetlerine ilişkin kişisel veri içeren bilgi ve belgeleri, 6102 sayılı Türk Ticaret Kanunu ve 4857 sayılı İş Kanunu ve ilgili diğer mevzuattan doğan hukuki yükümlülüklerinin yerine getirilmesi ve Kanun’da yer alan veri işleme şartlarından biri olan haklarının tesisi, kullanılması veya korunması kapsamında, işin gereği ve zamanaşımı süreleri boyunca saklamaktadır. Şirket, kendisine yapılmış olan iş başvurularını, başvuru sahiplerinin silme talebine kadar şirket sistemlerinde tutmakta ve her halde 1 sene sonra sistemlerinde silmektedir. Zaman zaman personel ihtiyacı sistemde kayıtlı bulunan başvurular arasından karşılanmaktadır.

Ayrıca, Şirket elde ettiği kişisel verileri Kanun’un 5. ve 6. maddelerinde yer alan işleme şartlarının gerçekleştirilmesi amacıyla sınırlı olarak da saklayabilmektedir.

Kişisel veriler, Kanun’un 4. maddesinde yer alan genel ilkelere uygun olarak saklanmasını gerektiren sebeplerin ortadan kalkması halinde silinmelidir. Ayrıca, veri sahibinin açık rızasına dayalı olarak yürütülen saklama faaliyetleri, rızanın veri sahibi tarafından geri alınması halinde de derhal sonlandırılmakta ve ilgili kişisel veriler silinmelidir. Veri sahibinin Kanun’un 11. maddesinde yer alan hakları kapsamında verilerinin silinmesi talebini Şirkete iletmiş olduğu durumlarda, Şirket içi yetkilendirilmiş kişilerce talep değerlendirilmekte ve Kanun’da belirtilen veri işleme şartlarının tamamının ortadan kalkması halinde kişisel veriler imha edilmektedir.

## Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesi ve Erişilmesinin Önlenmesi İçin Alınmış Teknik ve İdari Tedbirler

Bereket Fide, kişisel verilerin hukuka uygun işlenmesi ve güvenliğinin sağlanması amacıyla her türlü teknik ve idari tedbiri almakta; bu tedbirlere uyulması amacıyla Şirket personeline eğitimler vermekte ve periyodik aralıklarla denetim yapmaktadır.

Şirket, bünyesinde yer alan her bir departmanın gerçekleştirdiği kişisel veri işleme süreçlerini analiz etmekte, mevcut ve eklenen süreçlerde hukuka uygunluğun temini için gerekli aksiyonları almaktadır.

Şirkette veri toplamaya ilişkin bütün aşamalar tek tek gözden geçirilmekte, verilerin hukuka uygun bir şekilde elde edilmesi için çalışmalar yapılmaktadır. İş başvuruları alınırken bunlara ilişkin onay metinleri de alınmakta, Şirket [info@bereketfide.com.tr](mailto:info@bereketfide.com.tr) mailine gelenlere ise e-posta ile dönülerek başvuruları ile ilgili onay süreci tamamlanmaktadır.

Şirket çalışanları, işleri kapsamında öğrendikleri kişisel verileri herhangi bir üçüncü kişi ve/veya kuruma açıklamama konusunda bilgilendirilmektedir. Çalışan ile Bereket Fide arasındaki hizmet sözleşmelerine bu doğrultuda gizlilik kayıtları eklenmekte; çalışanlardan bu sır saklama yükümlülüklerinin görevden ayrılmalarının akabinde de devam edeceği yönünde taahhüt alınmaktadır.

Ayrıca, Şirketin Kanun’un 8. ve 9. maddesine uygun olarak kişisel veri aktarımı gerçekleştirdiği üçüncü kişi ve/veya kurumlar ile arasındaki sözleşmelere, alıcı grubunun kişisel verilerin güvenliğini sağlama hususunda her türlü tedbiri alacağı yönünde hükümler eklenmektedir.

Bereket Fide, sistemlerinde yer alan kişisel verilerin güvenliğinin sağlanması amacıyla teknolojik imkanlar ve maliyetler çerçevesinde her türlü teknik tedbiri almaktadır. Örneğin, güvenlik duvarı kullanımı, güvenlik yazılımlarının bütün cihazlara kurulumu ve güçlü şifre uygulaması gibi. Kişisel verilere hukuka aykırı erişimin ve kişisel verilerin ifşasının önlenmesi amacıyla Şirket yazılımlarında şifreleme sistemleri kullanılmakta; çalışanların verilere erişimi iş kapsamları ile sınırlandırılmaktadır.

Bunun yanı sıra, Şirket hukuka uygunluğun temini kapsamında çeşitli politika ve yönergeler yürürlüğe koymuştur. Bu politika ve yönergeler, değişen mevzuata ve ortaya çıkan ihtiyaçlara uygun olarak güncellenmektedir. (Kişisel Veri Yönergesi, Kişisel Verilerin Silinmesine ve Yok Edilmesine İlişkin Yönerge ve Komitenin Çalışma Esaslarına İlişkin Yönerge)

Ayrıca;

* **Bilgisayar Ortamındaki Ortak Dosyalarda Bulunan Kişisel Verilerin Temizlenmesi:** İşe yaramayan dosya ve resimler silinmiş, işe yarayacağı düşünülen ya da belirtilen dosya ve resimler sadece IT’nin erişimde olan klasörlere eklenmiştir.
* **Erişim Yetkileri Güncellenmesi:** Ortak sistemlerdeki erişim yetkileri kısıtlanarak çalışanların sadece işleriyle ilgili dosyalara erişimi şeklinde yetkilendirme sağlanmıştır. Yeni erişim yetkisi genel müdür onayı sonrasında verilecek şekilde düzenlenmiştir.
* **Tüm İK Formlarının Güncellenmesi:** İşbaşında ya da çalışırken aldığımız formların tümü değerlendirilerek gereksiz kişisel veriler çıkartılmıştır.
* **Raporlarımızın Güncellenmesi:** Bayi, müşteri, çalışan, komisyoncuların kişisel verilerinin bulunduğu tüm raporlarımız taranmış ve kişisel veri içeren raporlar değerlendirilerek gereksiz kullanılan kişisel veriler temizlenmiştir.
* **KVKK Komitesi:** KVKK komitesi kuruldu.
* **Eğitim Verilmesi:** Departman sorumlusu çalışanlara KVKK hakkında eğitim verilmiş ve sorumlulukları anlatılmıştır. Ayrıca eğitimin zorunlu eğitimlere dahil edilmesi ve yeni çalışanlar için yılda bir kez tekrarlanması kararı alınmıştır.
* **Muvafakatname:** Çalışanlardan gizlilik taahhüdü, araç takip aydınlatma metni, araç takip-yakıt aydınlatma metni, gerekli açık rıza metinleri onay imzaları alındı ve aydınlatma metinleri yayınlanmıştır. İşe girişte imzalatılacak formlar arasına eklenmiştir.
* Ticari işlemleri için aydınlatma metinleri hazırlanmış ve sözleşmelere eklenmiştir.
* **Politikalar:** Gizlilik Politikası, Özel Nitelikli Kişisel Veri Politikası, Çerez Politikası, KVKK Politikası, Bilgi Güvenliği Politikası hazırlanmıştır.
* **E-posta Uyarısı ve Site Güncellemesi:**Maillere otomatik eklenecek e-posta uyarıları hazırlanmış ve mail imzalarına eklenmiştir. KVKK ile ilgili sitemize gerekli metinler eklenmiştir.

## Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Teknik ve İdari Tedbirler

Şirket, Kurul tarafından aksine bir karar alınmadıkça, Yönetmelik gereği kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçmeye yetkilidir. Veri sahibinin talebi halinde, uygun yöntemi gerekçesini açıklayarak seçer.

Bereket Fide, kişisel verilerin hukuka uygun olarak silinmesi, yok edilmesi veya anonim hale getirilmesi için her türlü teknik ve idari tedbiri almaktadır. Şirket’in sahip olduğu teknolojik imkanlar ve uygulama maliyetleri göz önünde bulundurularak en uygun yöntemler kullanılmaktadır.

İmha süreçleri, Şirket bünyesinde kişisel veri işleme süreçlerinin hukuka uygunluğunu sağlamak üzere oluşturulan birim tarafından denetlenmektedir. Periyodik imha süreçleri, bu birim bünyesindeki en az iki kişi tarafından birlikte gerçekleştirilmekte, imha edilen kişisel verilerin herhangi bir kopyasının alınmadığı hususunda bu kişilerden yazılı taahhüt alınmaktadır. Görevliler ayrıca Komite tarafından belirlenecektir.

Şirkette bulunan ve kişisel verileri taşıyan cihazlar, artık kullanılmaz duruma gelmişse ve dışarıya satılma ya da bırakılma durumu olacaksa cihaz içindeki veriler yok edilmekte, bu mümkün değilse cihaz yok edilmektedir.

## Kişisel Verileri Saklama ve İmha Süreçlerinde Yer Alanların Unvanları, Birimleri ve Görev Tanımları

Kişisel verilerin saklanması ve imha edilmesine ilişkin süreçler, Şirket bünyesinde kurulan ve kişisel verilerin hukuka uygun işlenmesini temin etmekle görevli olan birim tarafından gerçekleştirilir.

Bereket Fide, Kişisel Veri Koruma Komitesi, Şirket Kişisel Veri Koruma Komitesi’nin görevi; Şirket’in kişisel verilerin işlenmesi süreçlerinde Kanun’a, Yönetmelik’e, diğer ikincil mevzuata, Şirket politika ve yönergelerine uygunluğunu temin etmek; veri sahiplerinden gelen talepleri değerlendirmek ve sonuçlandırmak; kişisel verilerin imhası süreçlerine fiilen katılmak, bu kapsamda gerekli her türlü tedbiri almak ve denetim yapmaktır.

## Periyodik İmha Süreleri

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

Periyodik imhanın gerçekleşeceği zaman aralığı 1 yıldır. Ancak, imha edilmesi gereken kişisel verinin saklama süresi 1 yıldan daha az ise, ilgili kişisel verinin imhası bakımından bu süre uygulanır.

## Saklama ve İmha Süreleri

Şirket’in işlemekte olduğu kişisel veriler bakımından saklama ve imha süreleri aşağıdaki tabloda gösterilmiştir. Saklama sürelerinin hukuki dayanaklarına ilişkin mevzuat hükümlerine işbu Yönerge’nin ekinde yer verilmiştir.

## Güncelleme

İşbu Yönerge’de yapılan değişiklikler aşağıdaki tabloda gösterilmektedir.

|  |  |
| --- | --- |
| Yönerge Güncelleme Tarihi | Değişiklikler |
|  |  |
|  |  |

ZAMANAŞIMI SÜRELERİ

6102 sayılı Türk Ticaret Kanunu, 5237 sayılı Türk Ceza Kanunu, 6098 sayılı Türk Borçlar Kanunu çerçevesinde göz önünde bulundurulması gereken zamanaşımı süreleri aşağıdaki şekilde değerlendirilmelidir.

|  |  |  |
| --- | --- | --- |
| VERİ KATEGORİSİ | SAKLAMA VE İMHA SÜRESİ | HUKUKİ DAYANAK |
| Şirket çalışanlarına ilişkin kişisel veriler | Hizmet ilişkisinin devamı + 15 yıl süresince saklanır. | 6098 sayılı Türk Borçlar Kanunu, 4857 sayılı İş Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat. |
| Şirketin mal ve/veya hizmet almakta olduğu tedarikçilere ve tedarikçi temsilcilerine ilişkin kişisel veriler | Ticari ilişkinin devam ettiği sürece saklanır. Ticari ilişkinin olmayacağının düşünüldüğü, uzun yıllar ticari ilişkinin kurulmadığı hallerde yasal zamanaşımı Süresi 10 yıl + 1 yıl süre ile saklanır. Bu sürenin sonunda silinir. | 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat. |
| Kapalı Devre Görüntüleme Sistemleri vasıtasıyla elde edilen kamera kayıtları | Adli bir vakıanın yaşanmamış ve resmi kurumlarca talep edilmemiş olması halinde bir ay sonunda silinir. | 6698 sayılı Kişisel Verilerin Korunması Kanunu’na uygun olarak veri sorumlusu Şirketin meşru menfaatleri kapsamında bir ay makul süre ile saklanmaktadır. |
| Araç-benzin takip sistemi kayıtları | Adli bir vakıanın yaşanmamış ve resmi kurumlarca talep edilmemiş olması halinde 2 yıl sonunda silinir. | 6698 sayılı Kişisel Verilerin Korunması Kanunu’na uygun olarak veri sorumlusu Şirketin meşru menfaatleri kapsamında 2 yıl makul süre ile saklanmaktadır. |
| Şirket içinde unutulan ve kişisel veri içeren eşyalar | Sahibine ulaşılamamış ise, 6 ay süre ile muhafaza edilir. Süre bitiminde bir tutanak ile yok edilir. | 6698 sayılı Kişisel Verilerin Korunması Kanunu’na uygun olarak veri sorumlusu Şirketin meşru menfaatleri kapsamında 6 aylık makul süre ile saklanmaktadır. |
| İş Başvuruları-Özgeçmişler | Başvurular, başvuru sahibinin silme talebine kadar sistemde saklanır ve her halde 1 yıl sonunda veya onay sahibinin talebi ile derhal yok edilir. | Başvuru sahibinin ve Şirketin meşru menfaati ve başvurusu kapsamında saklanmaktadır. |
| İşten ayrılan eski çalışanlara ait veriler | Olası iş davaları, özellikle de meslek hastalıklarına dayanan davalar nedeniyle 15 yıl saklanır. | İş Kanunu nedeniyle saklanır. |
| Dava süreci devam eden dosyalar | Yukarıdaki zamanaşımı ve imha süreçlerinden biri ile ilgili dava süreci devam ediyor ise -imha süreci gelmiş olsa bile- bu halde dava sürecinin bitimi ve mahkeme kararının kesinleşmesine kadar veriler saklanır. İmha kesinleşme tarihinden veya sürecin icra vb. işlemlerle devamı halinden itibaren 1 yıl sonra gerçekleştirilir. | 6098 Sayılı Borçlar Kanunu ve zamanaşımı sürelerinin düzenlendiği ilgili diğer mevzuat. |

# Kişisel Verileri Koruma Komitesinin Görevlerine İlişkin Yönerge

Ortaklar Kurul Kararı ile yürürlüğe girer. KVKK Kitapçığına eklenir.

Versiyon 1.0

…/…/2020

## Amaç

Bu Yönergenin amacı, şirket bünyesinde oluşturulan kişisel verileri ve veri güvenliğini korumak için atanan Komitenin görevlerini ve yetkilerini belirlemektir.

Yönerge, Ortaklar kararı ile yürürlüğe girer, gerektiğinde güncellenir.

## Görevleri

a. Komite, Şirket içinde bulunan kişisel verilerin hukuka uygun toplanması, korunması ve aktarılması, silinmesi, yok edilmesi ile ilgili bütün tedbirleri almakla görevlidir.

b. Komite, Şirket içinde bulunan bütün görevlileri, kişisel verilerin korunması konusunda uyarır, uyarılara rağmen kişisel verilerle ilgili verilen görevleri yerine getirmeyen kişilerle ilgili Müdüre bildirimde bulunur.

c. Komite, Şirket içinde bulunan bütün müşterilere ilişkin verilerin korunması için gerekli uyarıları hazırlar ve personelde bilincin oluşmasına yardımcı olur.

aa. Üreticilerden, bayilerden, müşterilerden, iş ortaklarından ve çalışanlardan gerekenden fazla bilgi talep edilemez.

bb. Çalışanlardan sağlık verileri ancak onların iş güvenliğinin sağlanması için alınabilir ve bu konuda onlardan onay alınır.

d. Komite, kişisel verilerle ilgili kendisine gelen bütün talepleri değerlendirir. Yapılan başvuru, Sorumlu tarafından 30 gün içinde cevaplanır.

aa. Çalışanlardan/İş ortaklarından/müşterilerden kişisel verilere ilişkin verilerin silinmesine ilişkin talepler, sözleşmeye ilişkin zamanaşımı sürelerine göre belirlenir.

bb. İş başvurusu yapanların başvuru aşamasında kalanların CV’lerinin silme talepleri ise karşılanır ve sistemden silinir.

cc. Çalışanların/Müşterilerin kişisel verilerinin güncelleme talepleri hemen karşılanır sistemdeki bilgiler de güncellenir.

e.Komite, kişisel verilerle ilgili başvuruların değerlendirilmesi ve VERBİS ile ilgili güncellemelerde irtibat kişisine yardımcı olacaktır. İrtibat kişisinin bulunmadığı zamanlarda ilgili düzenlemelerde Komite, irtibat kişisine destek verecektir.

f. Çalışan ve bayilere, müşterilere ait veriler hakkında yakınları bile olsa üçüncü kişilere bilgi verilmez.

g. Çalışan ve müşteri bilgileri dışarıdan gelen sorgulamalara (telefon, şahsen sorgulama vb.) karşı korunur.

h. Resmî kurumlardan gelen bilgi ve belge talepleri mevzuata uygunluğu veya mahkeme kararına dayanması halinde ivedilikle karşılanır.

i. Şirkette kişisel verilerin korunmasına ilişkin teknik ve idari tedbirler, yılda **bir** kontrol edilir ve kontrolün sonuçları, Ortaklara raporlanır. Bu raporda ayrıca alınması gereken ilave tedbirler de yönetime bildirilir.

j. Komite, Yönerge’ye aykırı hareket etmesi ve görevlerini ihmal etmesi halinde doğacak zararlardan sorumlu olacağının farkındadır.

k. Komite, kişisel verilerle ilgili ortaya çıkabilecek olan sorunları çözme ve kendisine gelen talepleri karşılamakla görevlendirilmiştir.

## Başvuruları Cevaplama

Komite, ilgili kişinin kişisel verilerine ilişkin soru ve taleplerini mümkün olan en kısa sürede ve olması gerektiği gibi cevaplamakla yükümlüdür.

## Mevzuatı Takip ve Öneride Bulunma

Komite, kişisel verilerle ilgili mevzuattaki gelişmeleri ve işletmeye düşen yükümlülükleri belirler ve bunları da Müdür’e raporlar.

## Geçmişe Yönelik Verilerin Hukuka Uygunluğunu Kontrol

Komite, şirketin kurulmasından bugüne kadar, şirkette bulunan bütün verilerin hukuka uygunluğunu kontrol etmekle görevlidir. Bunlardan şirket için önemsiz hale gelenleri ve işlenme amacı bitenleri silmekle görevlidir.

1. Şirket aracı verilmiş olan çalışanların verilerinin son iki yıla kadar olanları tutulmuş, kalanlar silinmiştir.
2. Kamera kayıtlarının son iki aya kadar olan kayıtlar tutulmuş, diğer kayıtlar silinmiştir.
3. Çalışan özlük dosyaları son 15 yıla ait çalışan kayıtları tutulmuş, öncesine dair kayıtlar silinmiştir.
4. Ticari ilişkinin devam ettiği bayi, üretici, çiftçi bilgileri tutulmuş, son 10 yılda ticari iş/işlem yapılmayan şahıs/şirketlerin verileri silinmiştir.

## Yönergeleri Uygulama Görevi

Komite, gerek resmî kurumlar gerekse Ortaklar tarafından çıkarılan bütün kanun, yönetmelik, tebliğ ve yönergeleri uygulamakla görevlidir.

## Güncelleme

İşbu Yönerge’de yapılan değişiklikler aşağıdaki tabloda gösterilmektedir.

|  |  |
| --- | --- |
| Yönerge Güncelleme Tarihi | Değişiklikler |
|  |  |
|  |  |

# Veri Sahibi Başvuruları Yönetim Yönergesi

Ortaklar Kararı ile yürürlüğe girer. KVKK Kitapçığına eklenir.

Versiyon 1.0

…/…/2020

## AMAÇ

İşbu Veri Sahibi Başvuruları Yönetim Yönergesi’nin amacı, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında veri sorumlusu bünyesindeki irtibat kişinin görevleri ile veri sahibi başvurularında izlenecek yöntemlerin ortaya konulmasıdır.

## TANIMLAR

**Veri sahibi :** Kişisel verisi işlenen gerçek kişi.

**İrtibat Kişisi :** Şirket’in 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kişisel Verileri Koruma Kurumu ile kurulacak iletişim için Şirket tarafından Veri Sorumluları Sicili’ne kayıt esnasında bildirilen gerçek kişidir.

**Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

**Şirket : Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi**

**Kanun :** 6698 Sayılı Kişisel Verilerin Korunması Kanunu

## İRTİBAT KİŞİSİ ve KVKK KOMİTESİNİN GÖREVLERİ

İrtibat kişisi bilgileri, Veri Sorumluları Sicili’ne kayıt esnasında işlenir. İrtibat kişisi Şirket’i Kanun ve ikincil mevzuat hükümlerine göre temsile yetkili değildir.

İrtibat kişisi ve KVKK Komitesi,

* + Veri sahiplerinin Şirket’e yönelteceği taleplerin cevaplandırılması konusunda iletişimi ve Kişisel Verileri Koruma Kurumu ile Şirket arasındaki iletişimi sağlar.
  + Veri sahibi tarafından herhangi bir başvuru gerçekleştirilmesi durumunda, başvuru ve verilen cevabı Bereket Fide Kişisel Verileri Koruma Komitesi’ne bildirir.
  + Veri Sorumluları Sicili üzerindeki verilerin güncelliğini kontrol eder ve gerektiğinde değişiklikleri gerçekleştirir.

## VERİ SAHİBİ BAŞVURUSUNUN GEÇERLİLİK ŞARTLARI

### Başvuru Hakkına Sahip Olan Kişiler

Bütün gerçek kişiler, Kanun’un 11. maddesinde sıralanan taleplerine ilişkin olarak *(başvurularını Türkçe yapmak kaydıyla)* Şirket’e başvuru hakkına sahiptir.

### Başvuru Usulü

Veri sahipleri aşağıdaki yöntemlerden birini kullanarak Türkçe başvuru yapmak zorundadır. Bu yöntemler dışında *(örneğin, sözlü olarak)* yapılan başvuruları Şirket’in değerlendirme zorunluluğu yoktur.

* Yazılı olarak
* Kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da veri sahibi tarafından Şirket’e daha önce bildirilen ve Şirket’in sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle
* Başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla

### Başvuruda Bulunması Gereken Bilgiler

Veri sahibi, başvurusunda aşağıdaki bilgilerin tamamını iletmek zorundadır.

* Ad, soyadı ve başvuru yazılı ise imza,
* Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası,
* Tebligata esas yerleşim yeri veya iş yeri adresi,
* Varsa bildirime esas elektronik posta adresi, telefon ve faks numarası,
* Talep konusu

Konuya ilişkin diğer bilgi ve belgeler başvuruya eklenir.

### Başvuruda Yer Alabilecek Talepler

Veri sahibi başvurusunda yer alabilecek talepler şunlardır:

* Kişisel veri işlenip işlenmediğini öğrenme
* Kişisel verileri işlenmişse buna ilişkin bilgi talep etme
* Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme
* Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme
* Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme
* İşlenmesini gerektiren bütün sebeplerin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme
* Kişisel verilerin düzeltilme ve imha edilme işlemlerinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme
* İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme
* Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

## BAŞVURUNUN ALINMASI

Yukarıda yer alan geçerlilik şartlarını taşıyan başvurular, Şirket’in belirlediği irtibat kişisi tarafından alınır. Başvurunun irtibat kişisi dışındaki bir çalışana ya da üçüncü kişiye iletilmesi durumunda başvuru, ilgili çalışan/üçüncü kişi tarafından gecikmeksizin irtibat kişisine iletilmelidir.

Şirket bünyesinde kişisel verilerin korumasına ilişkin bir kişi ya da birimin görevlendirilmiş olması durumunda başvuru doğrudan görevlendirilen kişiye/birime yönlendirilir. Süreç kapsamında diğer gerekli işlemleri söz konusu kişi/birim gerçekleştirir.

Şirket bünyesinde kişisel verilerin korunmasına ilişkin bir görevlendirme yapılmamışsa irtibat kişisi başvuru dilekçesinde açıklık bulunmaması durumunda aşağıdaki konulara ilişkin olarak veri sahibinden ilave bilgi talep edebilir:

**Şirket’le Olan İlişkiniz :** ⃝ Ziyaretçi ⃝ İş Ortağı ⃝ Çalışan ⃝ Diğer

⃝ Çalışan Adayı ⃝ Müşteri/Müşteri Çalışanı ⃝ Tedarikçi/Tedarikçi Çalışanı

**Şirket’le Olan İlişkiniz Sona Erdi mi? :**

İrtibat kişisi, Şirket ile ilişkisini belirlediği veri sahibinin başvurusu yönlendirmek üzere Kişisel Veri İşleme Envanteri’nden ilgili departmanı tespit eder ve başvuruyu yönlendirir.

## BAŞVURU İNCELEME SÜRESİ

Veri sahibi başvuruları talebin niteliğine göre en kısa sürede ve **en geç 30 (otuz) gün içinde** sonuçlandırılır. Bu süre;

* Yazılı başvurularda evrakın veri sorumlusu Şirket’e tebliğ edildiği tarihten,
* Diğer yöntemlerle yapılan başvurularda ise; başvurunun veri sorumlusu Şirket’e ulaştığı tarihten itibaren hesaplanır.

## BAŞVURULARIN SONUÇLANDIRILMASI

Şirket, veri sahibi başvurularını etkin, hukuka ve dürüstlük kurallarına uygun olarak değerlendirir; başvuruyu kabul eder ya da gerekçesini açıklayarak reddeder.

Şirket, cevabını veri sahibine yazılı olarak veya elektronik ortamda bildirir. Şirket’in cevap yazısında aşağıdaki hususların yer alması zorunludur:

* Veri sorumlusu veya temsilcisine ait bilgiler
* Başvuru sahibinin; adı ve soyadı, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası
* Talep konusu
* Şirket’in başvuruya ilişkin açıklamaları

Veri sahibinin talebinin kabul edilmesi hâlinde, Şirket talebin gereği en kısa sürede yerine getirir ve veri sahibine bilgi verir.

## ÜCRET

Şirket, veri sahibi başvurularını kural olarak ücretsiz sonuçlandırır. Ancak veri sahibi başvurusuna yazılı olarak cevap verilecekse 10 (on) sayfanın üzerindeki her sayfa için 1 (bir) Türk Lirası işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde Şirket tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

Başvurunun Şirket’in hatasından kaynaklanması halinde alınan ücret ilgiliye iade edilir.

# Kişisel Verilere İlişkin Acil Durumlar Yönergesi

**Acil durum hallerinin çıkartılması ve kriz yönetimine ilişkin çalışmanın yapılmasının ardından çıkartılır.**

Ortaklar Kararı ile yürürlüğe girer. KVKK Kitapçığına eklenir.

Versiyon 1.0

…/…/2020

## Amaç

Bu Yönergenin amacı, **Bereket Fide Tohumculuk Üretim İthalat İhracat ve Ticaret Limited Şirketi**’nde işlenen kişisel verilerle ilgili acil hallerde yapılması gerekenlere ilişkin kuralların ve usullerin belirlenmesidir. Acil durumlar, şirket içinde bulunan kişisel verilerin saldırıya uğraması, sistemlerin hacklenmesi, içeriden dışarıya bilgi sızdırıldığına ilişkin ciddi endişelerin mevcut olmasıdır.

Yönerge, Ortaklar Kurulu tarafından alınan karar ile yürürlüğe girer.

## Acil Eylem Planı

Şirket içinde bulunan kişisel verilerin korunması ve veri güvenliği konusunda görev yapacak sorumlu, yukarıda tanımlanan acil hallerden biri ile karşılaşıldığında derhal bütün sisteme müdahale yetkisine sahiptir. Bu konuda gerek şirket içinde gerekse şirket dışında bulunan resmi ya da yetkin kişi ya da kuruluşlarla iş birliği yapabilir.

## Acil Durumun Sisteme Müdahale Suretiyle Ortaya Çıkması

Şirket bilgi işlem sistemlerine dışarıdan ya da içeriden bir müdahale ile karşılaşıldığında Sorumlu her türlü gerekli tedbiri alabilir. Gerektiğinde sistemin kapatılması da dahil yetki kısıtlamalarına gidebilir. Sorumlu, karşılaşılan durumu ve aldığı ve sonrasında alınması gereken önlemleri derhal şirketteki bütün ilgilileri toplayarak bilgi verir.

Dışarıdan ya da içeriden sisteme müdahale eden kişilerin kimlik tespiti için gerekli işlemleri ve aksiyonları alır. Söz konusu kişilerin eylemleri hakkında derhal şirketin hukuk birimini haberdar eder.

## Sisteme Fiziki Müdahale

Bilgi işlem sistemlerine fiziki müdahalenin ve yetkisiz girişlerin engellenmesi için gerekli her türlü tedbiri alır. Bu konuda sisteme yetkisiz erişimleri engelleyecek her türlü idari ve teknik tedbirler alınıp uyarılar yapılır. Şirket içinden ya da dışından bilgi işlem sistemlerine yetkisiz erişimin tespiti halinde şirket güvenliği ya da kolluk güçlerine derhal haber verilir. Söz konusu kişi eğer şirket çalışanı ise hakkında soruşturma açılır.

## Verilerin Dışarıya Sızması

Verilerin dışarıya sızdığına ilişkin bir duyum alınır ise bu husus, derhal KVK Komitesi’ne iletilir ve gerekli her türlü tedbir Komite’nin bilgisi ile alınır. Gerektiği hallerde şirket sistemleri derhal sızma testine tabi tutulur.

Verilerin dışarıya sızdığı tespit edilirse, söz konusu verilerin ne şekilde ve nasıl çıktığı belirlenir. Eğer kişileri ihlal edecek bir sızma söz konusu ise bu halde derhal yetkili merci ve makamlar durumdan haberdar edilir.

## Komitenin Toplantıya Çağırma Yetkisi

Komitenin, ihlalin ve acil durumun niteliğine göre gerekli her türlü önlemi almaya yetkilidir.

## Kamuoyu Bilgilendirmeleri

Kamuoyundan ya da verisi ihlal edilenlerden gelecek şikâyet ve başvurularda bir şirket dili geliştirilir ve şirketin en az imaj kaybı ve en az zarar görerek acil durumdan çıkması için gerekli önlemleri alır. Veri ihlali halinde dahi Sorumlu, ihlalin ve zararın boyutlarını şirket içinde dahi olsa kimse ile paylaşmaz ve bunun bir şirket sırrı olduğu bilinciyle hareket eder.

8. Bu Yönergeyi, KVKK Komitesi yürütür.

# Komite için Ortaklar Kurulu Kararı

**Şirket İçinde Kişisel Verileri Koruma Kurulunun/Komitesinin Kurulmasına İlişkin Ortaklar Kurulu Kararı**

**KARAR**

Ortaklar Kurulu ………. Tarihinde yaptığı toplantısında aşağıdaki kararları almıştır.

* 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat kapsamında şirket içinde kişisel verilerin korunması ile ilgili bir Komitenin atanmasına ve ortakların bu konudaki görev ve yetkilerini bu komiteye devretmesine oy birliği ile karar verilmiştir.
* Kişisel Verileri Koruma Komitesi’ne aşağıdaki listede ismi yazılı üç kişinin atanmasına karar verilmiştir.

1. Remzi Büyükkalkan

2. Aylin Gül

3. Payende Akar

# Yönergeler için Ortaklar Kurulu Kararı

**KARAR**

Genel Kurul ………. Tarihinde yaptığı toplantısında aşağıdaki kararları almıştır.

6698 sayılı Kanun ve ilgili mevzuat kapsamında şirket içinde kişisel verilerin korunması ile ilgili aşağıda listelenen yönergelerin yürürlüğe girmesine oy birliği ile karar verilmiştir.

1. Kişisel Verilere İlişkin Yönerge
2. Kişisel Veri Saklama, Silme, İmha ve Aktarılma Yönergesi
3. Kişisel Verileri Koruma Sorumlusunun/ Komitesinin Görevlerine İlişkin Yönerge
4. Veri Sahibi Başvuruları Yönetim Yönergesi
5. Kişisel Verilere İlişkin Acil Durumlar Yönergesi

|  |  |  |
| --- | --- | --- |
| YÖNERGELER | | |
| Yönergelere İlişkin Kontrol Soruları | Yönergelerin içinde geçen teknik donanımın şirkete uygunluğu IT tarafından incelendi mi, hangileri gerçeği yansıtmıyor belirlendi mi?  Yönergelerin yürürlüğe girebilmesi için YK Kararı alındı mı?  Veri Silme Kişisi belirlenerek Yönerge’de ilgili kısma eklendi mi?  Her yıl mart ayında güncelleme ihtiyacı gözden geçiriliyor mu?  Güncellemeler Politikalara işlendi mi?  Takibi KVK Komitesi ve YK tarafından yapılıyor mu?  Komite üyeleri ile görevleri ve yapılacaklarla ilgili bilgilendirme toplantısı yapıldı mı? |  |

1. Tüm belgelerde yazılanların uygulama ile örtüşmesi gerekmektedir. Dolayısı ile belgeler dikkatli bir şekilde okunmalı, uygulama ile örtüşmeyen kısımlar varsa danışman avukatın görüşü alınarak silinmeli ya da revize edilmelidir. Aksi durum, hukuka aykırı veri koruması gerçekleştirildiği anlamı taşır. [↑](#footnote-ref-1)